Annual ADFSL Conference on Digital Forensics, Security and Law

2018
Proceedings

May 18th, 10:40 AM - 11:15 AM

Knowledge Expiration in Security Awareness Training

Tianjian Zhang
tj.zhang@okstate.edu

KNOWLEDGE EXPIRATION IN SECURITY AWARENESS TRAINING

Tianjian (TJ) Zhang
Oklahoma State University
Management Science and Information Systems, Spears School of Business
Stillwater, OK 74078
tj.zhang@okstate.edu

ABSTRACT

This study evaluates the effectiveness of security education, training, and awareness (SETA) programs though the examination of the knowledge expiration process. The prevalence of security threats has led companies to invest more in information security. However, it is questionable how much a single training session could contribute to information security. We examine the knowledge types in a typical training program and measure the "shelf lives" of the knowledge. We find that technical knowledge decays faster than application knowledge, and both types of knowledge evaporate within a month following the training. This paper will contribute to the information security literature by revealing the ineffectiveness of single training sessions in the long run and suggest remedies to ensure consistent security policy compliance.

Keywords: cyber attack, security, awareness, knowledge, training, forgetting curve

1. INTRODUCTION

Information security is a pressing issue for businesses. Securities and Exchange Commission (SEC) Co-Directors of Enforcement Stephanie Avakian and Steven Peikin warned, "The greatest threat to our markets right now is the cyber threat." With virtually every company turning digital, at least 57 per cent of them had a recent significant cybersecurity incident [1]. Even tech giants are not immune to security breaches. In April 2017, Google and Facebook fell for a phishing attack, where unsuspected employees wired a total $100 million to a scammer that posed as a business partner [2].

This is merely one example where having a strong IT infrastructure is not enough to prevent cyberattacks in today's environment. Oftentimes, humans are the weakest link. Studies have shown that employees from within the organizations are the leading threats to IS security [3, 4], and non-malicious insiders such as careless or unaware employees are the major security vulnerability [1, 3].

Therefore, it is of utmost importance to build a "human firewall" through training programs [5]. Employees should learn early on the dos and don'ts in the digital world. For example, never click on suspicious links in their emails. However, sceptics of security trainings might question the usefulness of such training programs. After all, some employees are only trained through a quick slide show when they entered the company. We argue that the ineffectiveness of training is because the training is not carried out properly.

We first conduct a controlled experiment to show that training is, in fact, effective in reducing phishing succumbence rate. Next, we examine the knowledge expiration process after security trainings. We posit that the long-term ineffectiveness of training is partly due to the short "shelf lives" of training knowledge. If training knowledge decays quickly, employees are effectively untrained after a period of time.

There are few empirical studies on the effectiveness of the training [5]. In view of this deficiency, we utilize theories from learning and forgetting to understand the training effectiveness in the long run. In doing so, we will empirically determine the "expiration date" of current training programs.

In measuring the training outcomes, we will focus on actual compliance behaviors. The fundamental role of awareness in information security is long established [6, 7, 8], but there is a lack of empirical evidence to demonstrate that increased awareness level would affect compliance behavior. Intention to comply is often measured in lieu of actual compliance. An empirical evaluation of the training outcomes would potentially fill this gap.

From a practical standpoint, an assessment of SETA programs will enable more effective training designs, and potentially prevent the severe financial losses due to security breaches [9, 10]. It is estimated that cyberattacks cost businesses $400 billion a year [11]. The world could lose $90 trillion by 2030 if cybersecurity measures fall short [12]. In some industries, data breaches will also incur government fines on top of financial losses. In 2016, a hospital was fined $5.5 million [13] for compromising patient information, which violated the Health Insurance Portability and Accountability Act (HIPAA).

Furthermore, improved training programs will provide guidelines for companies to spend their ever-increasing cybersecurity investments more effectively. In 2015, Bank of America, Citi Bank, J.P. Morgan, and Wells Fargo spent a total of $1.5 billion on cybersecurity [14]. The cumulative 2015-2020 cybersecurity market size for US financial industries alone is forecasted to exceed $77 billion, making it the largest non-government cybersecurity market [15].

While industries are spending more on cybersecurity in general [1, 10, 16], it is not clear how much investment went into SETA programs, considering that 47 percent of the organizations still did not have any security training program as of 2016 [16]. Companies would be more willing to invest in SETA programs if we could show the improved security as a result of such programs.

Unfortunately, simply having a program may not be enough. Learning effects tend to decay overtime as modeled by the forgetting curve [17]. For the 53 percent of the organizations that do conduct security trainings [16], the training may range from voluntary review of a short slide show to more extensive online and face-to-face trainings covering a wide range of topics with a test at the end. There is little public information on the form and lasting effect of these programs. In light of the theoretical and practical gaps, we investigate the effectiveness of existing SETA programs, and propose measures to prolong the positive effects of training. The research questions are as follows. (1) Does SETA program help prevent security breaches? (2) How long does the learning effect last? (3) What are the measures to prolong the learning effect?

The rest of the article is organized as follows. §2 discusses the learning effect of the SETA programs. §3 studies knowledge decay. §4 discusses potential retraining mechanisms to ensure a consistent high level of security policy compliance rate. Since our experiments are conducted in the context of phishing, we will review literature on phishing §5. §6 will layout the two pilot studies. §7 concludes with

limitations and future research plans. This paper will contribute to the information security literature by revealing the ineffectiveness of single training sessions in the long run and suggest remedies to ensure consistent security policy compliance.

2. LEARNING

Information systems security management is a knowledge-intensive activity [18]. Employees usually acquire basic information security knowledge through SETA programs. Learning theory suggests that trainings (learning-before-doing) are effective in increasing trainees' knowledge level [19]. In this study, we will not go into details of the learning process in training. However, due to the reciprocity of learning and forgetting, we briefly review the literature on learning.

A large body of literature on learning focused on workers' learning behavior in manufacturing environment [e.g., 20, 21, 22]. The learning curve was applied in other areas such as education [23], economics [24], and management [25]. Notably, Kim et al. [26] applied the learning curve towards IT support services. To our knowledge, there is no theory of learning in the context of SETA programs.

As demonstrated in Kim et al. [26], learning can occur even in the volatile environment of IT support services. In IS security, there are also rapid evolution of different security threats. While the traditional Nigeria prince phishing emails may still trick some people, new tricks are constantly emerging. Some spear phishing emails are now sent from hacked email accounts familiar to the recipients, making it more difficult to identify the security threats.

However, unlike IT support services, where employees were learning-by-doing, the learning-before-doing SETA programs have a relative stable format. This raises question whether a preset SETA program is sufficient in coping with the changing IS security environment. We will discuss more of that in retraining in §4.

SETA programs generally involve more than one type of knowledge. For instance, part of the program may teach employees what a VPN is and why it is important, while another part of the program may teach them how to install relevant software on their computer and mobile devices. It is of value to assess any differential effect of different types of knowledge, so that organizations can adjust their programs accordingly based on their goals.

Knowledge was traditionally classified into two categories, content knowledge and knowledge regarding learning how to learn [27]. For IS studies, Kim et al. [26] divided IT knowledge into two subsets: (1) application-level knowledge that everybody possesses to use IT for practical purposes and (2) technical-level knowledge that goes beyond the simple usage of IT. We are interested to know which of the two types of knowledge would last longer following a SETA program.

As Dutton and Thomas pointed out, the learning rate should not be treated as a constant [28]. Learning curves may depend on an individual's task proficiency [29]. For now, we will focus on the fact that training will increase trainees' security knowledge.

Hypothesis 1: After a SETA program, trainees' information security knowledge will increase compared to the pre-training level.

Admittedly, there is an obvious gap between gaining knowledge and applying the knowledge to prevent security breach in the work environment. We attempt to address the issue through a controlled experiment to show that SETA program is effective in reducing phishing succumbence rate; however, even as knowledge level increases following training, and such increase help prevent security breaches, it is not clear how long the positive effect is going to last.

3. FORGETTING

With the learning effect of SETA programs in mind, the next step is to investigate how long these effects could last. We suspect that employees are prone to quickly forget security knowledge they obtained during one single training session. If any positive learning effect quickly wears off, employees are essentially untrained after the learning effects "expire." Hence, decay in knowledge will likely negatively affect security policy compliance over the long run.

Before attempting to devise any counter-measures to the potential knowledge decay, we need to have to a full understanding of the knowledge decay process. In particular, we will empirically determine the "expiration date" of training programs, and whether different knowledge types have different decay trajectory.

The natural means to model the forgetting process is through forgetting curves. Forgetting curve was first proposed by the well-known psychologist Hermann Ebbinghaus in 1885 [30]. Ebbinghaus memorized a series of nonsense syllables and tested his memory at various periods ranging from 20 minutes to 31 days. This simple experiment showed an exponential decay in memory.

The simplest form of forgetting curves is a decreasing linear function, where the dependent variable is the level of memory retention, and the independent variable is the time. Linear functions are best used to model drop in short intervals of time, but not for longer intervals. There are four basic forms of forgetting curve for longer periods, power function, hyperbola function, exponential function, and logarithmic function. Other variations of function are mostly based on these basic forms, which are all decreasing and convex. In other words, the initial decline is sharper than the latter decline.

Hypothesis 2: Following a SETA program, trainees' information security knowledge will decrease over a period of time.

Similar to learning curves, forgetting curves have been applied in different disciplines such as education [31], economics [22], and management [32]. However, application of forgetting curves in Information Systems (IS) has been limited. In one of the few instances, i.e., software development, the knowledge of methodology was found to be more easily forgotten than the knowledge of domain or technology [33].

Notably, learning process does not determine the forgetting curve. Forgetting rate is shown to be independent from learning rate [34]. Forgetting rate is determined by several factors such as the original level of learning [35], and type of the task. Procedural tasks [36] and cognitive tasks [37] are more prone to forgetting, while forgetting in continuous controls, such as bicycle riding, are negligible [38]. We are more interested to see whether the different knowledge types have different forgetting rates. Since ordinary employees are not tech-savvy, and everyday use of technology do not require deep knowledge, we posit that technical knowledge will decrease faster than application knowledge.

Hypothesis 3: After a SETA program, trainees' technical-level knowledge will decrease faster than application-level knowledge.

It is tempting to simply assume SETA programs should consist of a larger proportion of the type of knowledge that is more effective, but in evaluating training effectiveness in the long run, we should also take into account the forgetting rate. For instance, one type of knowledge may be effective in the short run but easily forgotten, while another type may be less effective in the short run but has a lower forgetting rate. Therefore, decision on the proportion of the two types of knowledge in a

SETA program will likely involve some intricacy.

In understanding the forgetting process, estimating the average forgetting rate is practically difficult. One could only measure a subject's knowledge level a few times at most in an experimental setting. As an alternative, we will quantify in our second pilot study how long it takes before security knowledge drop to the pre-training level, (i.e., the "expiration date" of the training program.) Shorter "expiration date" means faster knowledge decay, which is equivalent to a higher average forgetting rate.

4. RETRAINING

Knowledge decay call for measures to prolong the positive effects of training. One natural response is retraining. While it seems extremely costly to retrain employees every month, retraining need not be repeated indefinitely thanks to a reduction of the forgetting rate following each retraining [30, 39, 40]. In fact, the retraining time to achieve the peak performance level is likely to be less than half of the original training time [36].

It is suggested that repeatedly training employees will reinforce the learning effect and ultimately maintain the knowledge at a higher level [40, 41]. Each retraining will alter the next forgetting curve, making it flatter (i.e., lowering the average forgetting rate.) Ultimately, the forgetting curve would be so flat, that the forgetting rate is close to zero. Hence, loss of knowledge can eventually be neglected.

In designing retraining programs, one needs to consider the moderating roles on repetitive training. In advertising, ease of message processing was identified as a moderator for the repetition effect [42]. In the context of SETA program, training format may be one moderator.

It is noteworthy that repetitive training is not equivalent to massed repetition. The spacing effect suggests learning is more effective when studying is spread out over time [43]. Advertising literature has pointed out the ineffectiveness of repeating the same advertisement in a short interval [44]. To avoid cramming in recurring SETA sessions, retraining may be alternated based on different contents.

As mentioned in §2, the volatile IT environment also motivates repeated training. A change in the content of training is somewhat beyond the scope of this paper. However, it is conceivable that retraining planned around a short "shelf life" is unlikely to involve much additional new material. If new materials are required, alternating the new and old material in recurring training might effectively boost the spacing effect.

In short, retraining is an effective measure to mitigate the short "shelf lives" of training knowledge. It is noteworthy that retraining need not be carried out indefinitely. After a few retraining sessions, training knowledge will be maintained at a relatively high level.

5. PHISHING

As mentioned in §2, some may question whether increase in knowledge can be reflected in the reduction of security breaches. To address the issue, we will test the effectiveness of a SETA in terms of phishing prevention. We will briefly review the literature on phishing.

Phishing is among the top threats in cybersecurity [1]. As pointed out in the introduction, even tech giants with relatively advanced security mechanisms can become victims of phishing attacks.

As a result, more companies start to lay emphases on phishing in SETA programs. According to the latest Ernst & Young cybersecurity survey, 79 per cent of the surveyed organizations perform self-phishing within the company [1]. Due to the nature of

social engineering, phishing attacks can often be avoided by teaching employees the basic knowledge of identifying "red flags" in emails and reminding them to be constantly vigilant for such cues. In simulating real attacks, companies are able to test the knowledge of the employees, and the effectiveness of their training.

Phishing is studied extensively in prior literature. Wright et al. (2014) addressed the differential effects of different influencing techniques in phishing based on persuasion and motivation theory [45]. They found that individuals were more vulnerable to techniques offering a high level of self-determination. Interestingly, they also found males were significantly less likely to respond to phishing emails than females. However, other studies found no significant difference between genders [46]. Also, individuals aged between 18 and 25 are most susceptible to phishing attacks [46].

In terms of anti-phishing training methods, Kumaraguru et al. (2007) found that users learn more effectively when the training materials are presented after users fall for the attack, and users retain and transfer more knowledge in such training [47]. This may well explain why almost 80 per cent of the companies are performing self-phishing [1].

In a more specific study, Kumaraguru et al. (2009) focused on a specific kind of training module called PhishGuru, where users were trained right after clicking on the link in an artificial phishing email. It was revealed that such training allows users retain knowledge longer than usual, and repetitive trainings are effective in preventing phishing attacks [48].

For our purpose, we will focus on a generic phishing attempt to show that phishing succumbence rate falls as a result of training.

6. PILOT STUDIES

We conducted two pilot studies. The first pilot study measured the effectiveness of training in preventing phishing attacks. Pilot study 2 measured the decay of training knowledge over a period of time. Together, the two pilot studies demonstrate the short-term effectiveness and long-term ineffectiveness of training.

6.1 Pilot Study 1

In an attempt to learn if training programs can help mitigate phishing attacks on employees (i.e., everyday computer users), we conducted a pilot study. The study took place in a large university in the midwestern United States. Three groups of students (n>100 each) were evaluated for the ability to identify and not react to phishing attacks.

We believe college students are appropriate respondents for this study, because like everyone else, they face consequences if they succumb to an attack. A freshman college student is rather similar to a new employee in the security training context. They are both new to the organization, which is usually when security trainings take place. Also, their priorities are not IS security. Students tend to worry more about their coursework, and employees mainly focus on their job performance. Like companies, universities also experience data breaches from time to time. College students, being the majority population on campus, need to receive proper security awareness training.

All three groups of students received a pre-test on their ability to identify phishing emails. The first group was a control group with no follow-up trainings. After the pre-test, the second group was given a short (5 minute) recurring training sessions once a week for the next six weeks. The third groups received the same type of recurring training twice a week for six weeks.

In the training, the respondents reviewed various emails and determined whether they were phishing attacks. Afterward, their instructor went over the emails with the students and explained what made them phishing attacks or not.

After all training sessions were finished, the researcher waited a week before sending an artificial phishing email to all respondents in the study. The prevailing thought is that more training will better prepare the respondents to identify and not succumb to phishing attacks.

The results show 20% of people in the control group succumbed to phishing attacks. The number dropped to 10% for treatment groups, suggesting the positive effective of the phishing training. However, there is no significant difference between the two treatment groups, which was somewhat surprising.

We believe the unexpected results could have occurred for a number of reasons. First, the respondents were given their phishing attack either the week before finals exams or the week of finals exams. This is a very high-stress, high-tempo time period at a university, and the students may have been overwhelmed by all the end-of-term email traffic and failed to correctly identify the bogus email. Second, the phishing email may have been too authentic looking. The email appeared to be from the university bursar's office informing the students that a two-thousand-dollar payment is due in their bursar account and requested that they click on the link and follow the instructions. It is possible that students were very worried about the accounts and responded to the attack. The researcher who developed the email was very familiar with the university bursar emails and developed a very authentic looking email. Typical phishing emails are developed by those outside the organization and the perpetrator has very little information about the organization, its processes, and other internal indicators.

While not perfect, this pilot study proved to be informative. We have shown a positive training effect in preventing phishing attacks. To understand the mechanisms behind an effective training program, we intend to conduct similar training in a future study, and conduct follow-up interviews to ask students why they avoided or failed to identify the phishing attack.

6.2 Pilot Study 2

Pilot study 2 was designed to estimate the "expiration date" of a typical training program that involves both application and technical knowledge. Similar to pilot study 1, the sample was drawn from three different sections of an introductory information system management course in a large mid-western university in the United States. Each section had approximately 150 students.

IS security knowledge levels were measured by SETA quiz results. Each quiz had a total of twenty questions, half of which tested technical knowledge, the other half tested application knowledge. A week before the training, participants took an in-class quiz (pre-test) on security topics to set the baseline of participants' security knowledge. A week after the pretest, an in-class training module was presented by the course instructor. Immediately after the training, participants took another in class quiz (post-test 1). The pretest and posttest 1 used the same quiz.

Depending on which of the three class sections the students were in, participants then took a third in-class quiz (post-test 2) 15, 30 or 45 days after post-test 1. Since the study is largely exploratory, the choice of the intervals was based on authors' experience. Post-test 2 used slightly different questions, but all quizzes are on the same topic, and at the same level of difficulty. We avoided too many repeated tests on one group to minimize the distortion of learning effect in retesting. The three test scores are paired by student ID.

Summary statistics show a sharp increase in test scores from pre-test to post-test 1 and a sharp decrease from post-test 1 to post-test 2 (figure 1). ANOVA on pre-test results of all three groups suggests equal group means (p=0.6966). Within each group, repeated measures ANOVA on the three test results show that at least two of them are not equal (p<0.001). Pairwise t-tests will determine which two (three) are not equal.

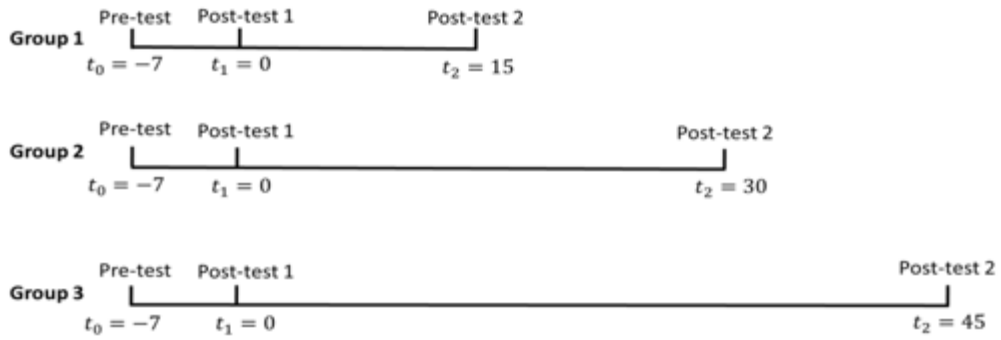

Figure 1. Pilot Study 2 Design

Table 1
Overall Test Score Change

	Pre-test	Post-test 1	Post-test 2
Group 1	12.55	14.71	12.85
Group 2	12.50	14.11	12.78
Group 3	12.48	14.51	12.95

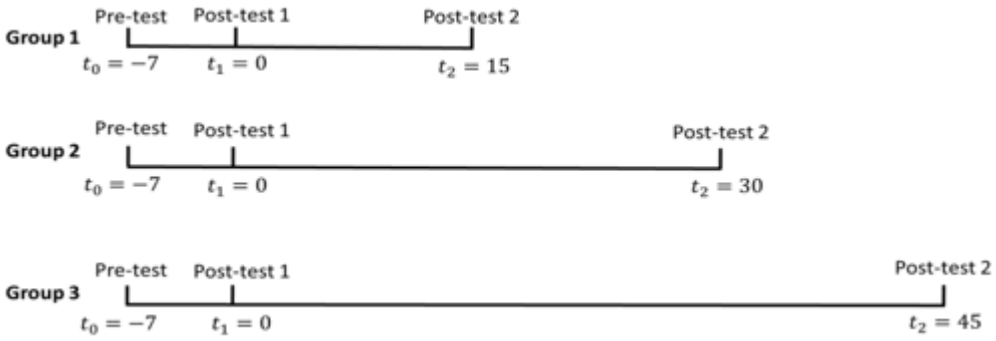

Figure 1. Pilot Study 2 Design

Figure 2. Overall Test Score Change

Figure 3. Technical Knowledge Score Change

Figure 4. Application Knowledge Score Change

Table 2.
Paired t-test for Pre-test and Post-test 2

$H_a: y_0 < y_2$	n	p-value		
		Overall	Technical	Application
Group 1	122	0.0849	0.3881	0.0383
Group 2	112	0.1579	0.4805	0.1101
Group 3	74	0.0026	0.4044	0.0001

y_i $(i = 0,1,2)$ stand for the test score at the pre- or post- tests 1 or 2.

Pairwise comparison by paired t-test showed a significant increase in overall test scores from pre-test to post-test 1 in all three groups ($p<0.001$), thus confirming the positive learning effect. Also, paired t-test showed a significant decrease in test scores from post-test 1 to post-test 2 ($p<0.001$) confirming the knowledge decay as predicted by forgetting curves. The results also hold for technical and application knowledge (figure 3, 4).

A similar pattern can be observed for participants scoring 80% or higher right after the training (post-test 1), which means any positive learning effect soon wears off. While government regulations such as HIPAA require employees in certain industries to be trained and reach a certain threshold, the knowledge decay pattern shown here suggest such seemingly demanding regulations may lose effect before long.

In order to devise meaningful retraining programs, we need to quantify the "expiration date" of each type of knowledge. To do that, we compare pre-test and post-test 2 scores (table 2) to see how long it took for the training effect to wear off. Intuitively, "expiration date" for a training program is when the post-test 2 scores equal the pre-test scores.

For technical knowledge, the post-test 2 score is statistically the same as the pre-test score for all three groups (table 2). Since the forgetting curve is a decreasing function, this means the learning effect of technical knowledge most likely wore off within 15 days following the training program.

For application knowledge, result for group 1 shows that post-test 2 score is still significantly higher than the pre-test score at 0.05 level (table 2), meaning there is still room for further decline. For group 2, post-test 2 score is statistically the same as the pre-test score. However, we cannot abruptly conclude that training expired at 30 days. It could happen some point before that. We conclude that the "shelf life" for application knowledge is somewhere between 15 and 30 days.

The abnormal results for group 3 are possibly due to the dramatic shrink in sample size. We believe those remained in class towards the end of the semester were probably more motivated students, who took the training more seriously in the first place. Hence, the group 3 sample at post-test 2 is biased. Although there is significant decrease from post-test 1 to post-test 2, the decay was not large enough to reduce them to their original knowledge level.

We found different "expiration dates" for different types of knowledge. Technical knowledge seems extremely short-lived (less than 15 days), while application knowledge has

a relative longer life (between 15 to 30 days). It is safe to conclude any positive learning effect of a SETA program evaporates within a month.

7. CONCLUSION, LIMITATION AND FUTURE STUDIES

Pilot study 1 has shown the positive effect of training in preventing phishing attacks. The "casualty rate" fell from 20% to 10% after the training. As a follow-up, we plan to conduct interviews on why students succumbed or avoided phishing traps. Furthermore, we have planned another study to determine what types of training would be more effective in preventing phishing attacks. We expect to see a differential learning effect on technical and application knowledge as discussed in §2.

Pilot study 2 has quantified the "shelf life" of technical and application knowledge. We have shown while both types are short-lived, technical knowledge decays faster than application knowledge. The short "shelf-life" should prompt the need for retraining.

We intend to conduct recurring training experiments to test the stabilization of knowledge. The ongoing studies on learning and forgetting need to be completed first to pinpoint the expiration point of the two types of knowledge and quantify the potential differential effectiveness. Based on those data, we would be able to decide the optimal knowledge composition of the training programs as well as retraining windows. Finally, we will test the effectiveness of the re-designed SETA program.

The two pilot studies have a few limitations. First, more control variables may need to be added in pilot study 1 in order to explain the lack of difference between the two treatment groups. Second, the in-class training in pilot study 2 has time limits as opposed to online trainings. It is possible a more thorough self-learning could postpone the expiry of the training. However, employees' willingness to engage in self-training is questionable given that IS security is not their main obligation. Third, there was a significant reduction in sample size for the third group in pilot study 2. These shortcomings will be addressed in the follow-up primary studies.

The pilot studies were meant to be exploratory. Future main studies will be refined to fully address the research questions raised in §1. This paper will add to security policy compliance literature showing that a full understanding of the knowledge expiration processes could improve the design of SETA programs, and ultimately enhance IS security policy compliance behavior.

REFERENCES

[1] Ernst&Young. (2016). "EY's Global Information Security Survey".

[2] Baraniuk, Chris. (2017). "Google and Facebook duped in huge 'scam'". BBC. Retrieved on Jan 30 from http://www.bbc.com/news/technology-39744007

[3] Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28(2), 203-236.*

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

[5] Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly, 757-778.*

[6] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34(3), 523-548.*

[7] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20(1), 79-98.*

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

[9] Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11(3), 431-448.*

[10] Richardson, R., & Director, C. S. I. (2011). CSI computer crime and security survey. *Computer security institute, 1, 1-30.*

[11] Gandel, Stephen. (2015). "Lloyd's CEO: Cyber attacks cost companies $400 billion every year". *Fortune*. Retrieved on Jan 30 from http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[12] Atlantic Council. (2015). "Atlantic Council / Zurich Insurance Report Finds the Global Benefits of Cyber Connectivity Expected to Outweigh Costs by $160 Trillion through 2030". Retrieved on Jan 30 from http://www.atlanticcouncil.org/news/press-releases/atlantic-council-zurich-insurance-report-finds-the-global-benefits-of-cyber-connectivity-expected-to-outweigh-costs-by-160-trillion-through-2030

[13] U.S. Department of Health & Human Services. (2017) "$5.5 million HIPAA settlement shines light on the importance of audit controls". Retrieved on Jan 30 from https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html

[14] Morgan, Steve. (2015). "J.P. Morgan, Bank of America, Citibank And Wells Fargo Spending $1.5 Billion To Battle Cyber Crime". *Forbes*. Retrieved on Jan 30 from https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#125ab80b116d

[15] Homeland Security Research Corp. (2015). "Premium Homeland Security and Public Safety Technology and Market Reports".

[16] PriceWaterhouseCoopers. (2016). "Key findings from the global state of information security survey".

[17] Rubin, D. C., & Wenzel, A. E. (1996). One hundred years of forgetting: A quantitative description of retention. *Psychological review, 103(4), 734.*

[18] Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security, 13(3), 189-202.*

[19] Carrillo, J. E., & Gaimon, C. (2000). Improving manufacturing performance through process change and knowledge creation. *Management Science, 46(2), 265-288.*

[20] Wright, T. P. (1936). Learning curve. *Journal of the Aeronautical Sciences, 3(1), 122-128.*

[21] Lapré, M. A., Mukherjee, A. S., & Van Wassenhove, L. N. (2000). Behind the learning curve: Linking learning activities to waste reduction. *Management Science, 46(5), 597-611.*

[22] Benkard, C. L. (2000). Learning and forgetting: The dynamics of aircraft production. American Economic Review, 90(4), 1034-1054.

[23] Hsu, L. H., Liu, C. C., & Ko, J. S. (2004). Education and experience improve the performance of transbronchial needle aspiration: a learning curve at a cancer center. *Chest, 125(2), 532-540.*

[24] Nembhard, D. A., & Uzumeri, M. V. (2000). Experiential learning and forgetting for manual and cognitive tasks. *International journal of industrial ergonomics, 25(4), 315-326.*

[25] Adler, P. S., & Clark, K. B. (1991). Behind the learning curve: A sketch of the learning process. *Management Science, 37(3), 267-281.*

[26] Kim, Y., Krishnan, R., & Argote, L. (2012). The learning curve of IT knowledge workers in a computing call center. *Information Systems Research, 23(3-part-2), 887-902.*

[27] Ellis, H. C. (1965). The transfer of learning.

[28] Dutton, J. M., & Thomas, A. (1984). Treating progress functions as a managerial opportunity. *Academy of management review, 9(2), 235-247.*

[29] Reagans, R., Argote, L., & Brooks, D. (2005). Individual experience and experience working together: Predicting learning rates from knowing who knows what and knowing how to work together. *Management science, 51(6), 869-881.*

[30] Ebbinghaus, H. (2013). Memory: A contribution to experimental psychology. *Annals of neurosciences, 20(4), 155.*

[31] Kerfoot, B. P., Fu, Y., Baker, H., Connelly, D., Ritchey, M. L., & Genega, E. M. (2010). Online spaced education generates transfer and improves long-term retention of diagnostic skills: a randomized controlled trial. *Journal of the American College of Surgeons, 211(3), 331-337.*

[32] Darr, E. D., Argote, L., & Epple, D. (1995). The acquisition, transfer, and depreciation of knowledge in service organizations: Productivity in franchises. *Management science, 41(11), 1750-1762.*

[33] Kang, K., & Hahn, J. (2009). Learning and forgetting curves in software development: Does type of knowledge matter?. *ICIS 2009 Proceedings, 194.*

[34] Brainerd, C. J. (1990). Issues and questions in the development of forgetting. *Monographs of the Society for Research in Child Development, 55(3-4), 100-109.*

[35] Johnson, M. K., & Hasher, L. (1987). Human learning and memory. *Annual review of psychology, 38(1), 631-668.*

[36] Schendel, J. D., & Hagman, J. D. (1982). On sustaining procedural skills over a prolonged retention interval. *Journal of Applied Psychology, 67(5), 605.*

[37] Arzi, Y., & Shtub, A. (1997). Learning and forgetting in mental and mechanical tasks: a comparative study. *IIE transactions, 29(9), 759-768.*

[38] Bailey, C. D. (1989). Forgetting and the learning curve: A laboratory study. *Management science, 35(3), 340-352.*

[39] Nembhard, D. A., & Uzumeri, M. V. (2000). An individual-based description of learning within an organization. IEEE *Transactions on Engineering Management, 47(3), 370-378.*

[40] Jaber, M. Y., Kher, H. V., & Davis, D. J. (2003). Countering forgetting through training and deployment. *International Journal of Production Economics, 85(1), 33-46.*

[41] Erev, I., & Roth, A. E. (1998). Predicting how people play games: Reinforcement learning in experimental games with unique, mixed strategy equilibria. *American economic review, 848-881.*

[42] Anand, P., & Sternthal, B. (1990). Ease of message processing as a moderator of repetition effects in advertising. *Journal of Marketing Research, 345-353.*

[43] Dempster, F. N. (1988). The spacing effect: A case study in the failure to apply the results of psychological research. *American Psychologist, 43(8), 627.*

[44] Janiszewski, C., Noel, H., & Sawyer, A. G. (2003). A meta-analysis of the spacing effect in verbal learning: Implications for research on advertising repetition and consumer memory. *Journal of consumer research, 30(1), 138-149.*

[45] Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research, 25(2), 385-400.*

[46] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 373-382). ACM.*

[47] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *In Proceedings of the 3rd symposium on Usable privacy and security (pp. 88-99). ACM.*

[48] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009, July). School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th*

Symposium on Usable Privacy and Security (p. 3). ACM.

