2017

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

Gamifying Security Awareness: A New Prototype

A Capstone
Presented to
the Graduate School of
The University of North Carolina Wilmington

In Partial Fulfillment
of the Requirements for the Degree
Masters of Science in Computer Science and Information Systems
Computer Science

---

by
John Russell Cole
May 2017

Proposed to:
Dr. Toni Pence, Committee Chair
Dr. Jeffrey Cummings
Dr. Elizabeth Baker

Abstract

Data breaches within an organization have many causes. Social engineering attacks, ransomware applications and harmful spam email messages are data breach catalysts that are the result of human error. Human error is the leading cause of data breach and is also one of the more difficult factors for an organization to prevent. Many users are unable to see how their role is impacted by organizational security policy, and therefor see no benefit to abide the policy. When employees use company devices to perform personal tasks, or use personal devices to perform business tasks, lines of ownership can be blurred and important organizational data assets can be put at risk.

This project and accompanying research paper will explore the gamification of a security training and awareness program. I set out to design and implement a prototype application that would make the process of training employees in security awareness fun and interactive. By developing role-based game modules to teach secure behavior to all organizational users, incentivizing secure behavior with real rewards that matter to participants and applying the training throughout the year, it will be possible to reinvent security awareness and prevent future data breaches.

To aid in the iterative development of the application, I created usability studies to gauge user experience regarding the functionality, appearance and navigation of the application. I conducted the usability study at the Wilmington Information Technology Expo, or WITX, with fellow students and with co-workers. I found that users rated the appearance of the application with an average score of 2.68 out of 10, where 1 leaned towards positive responses and 10 leaned toward negative responses. Users rated the functionality of the application with an average score of 2.89. And finally, users rated their experience with navigation within the application with an average score of 3.04.

Table of Contents

Chapter 1

Introduction

A data breach occurs when confidential information is lost or released into an un-trusted environment. Data breaches continue to be issues for organizations and often lead to the theft of private customer information (like health or banking information), and can cause problems for all company stakeholders. The problem that I aimed to address with this project is that human error is still the highest ranking cause of data breaches. It may seem like an easy factor to control, but for many companies, enforcing a strict security policy can be difficult. For other companies, employee training programs aren't considered a priority, but merely a required checkbox on an auditor's form that must be addressed annually.

The prototype that I created to address this issue integrates elements of gamification and incentivization into a security training and awareness program. Applying principles of gamification to a process involves engaging users in problem solving activities and rewarding positive behavior. I gamified the process of security training and awareness by creating a training module that emulates a video game, rewarding users with points for playing and employing secure behavior, allowing users to redeem those points for real incentives and encouraging competition between employees with elements of social networking. This program should be administered throughout the year to ensure that security awareness remains in the users' daily activities. The program should be adaptive to each organization to ensure that employees will actually value and be interested in pursuing them as rewards. Not every organization has the same values; some organizations might collectively be more interested in monetary rewards, while others might be interested in earning extra vacation time. It will be important to discover these values for each organization and implement the training program

to cater to those values. To make the process of employee training fun, I incorporated elements like trophies that provide points when you earn them and illustrate a user's mastery of a given topic, easter eggs that are like small treats hidden in the game that can be humorous and provide some talking points around the office, and a leaderboard that ranks employees based on point totals and encourages competition to earn more points.

By ensuring that employees understand how their roles are affected by organizational security policy and illustrating the importance of security training and awareness to organizational executives, it might be possible to reduce the number of data breaches that occur to organizations through the process of gamification.

Chapter 2

Background Research

2.1 Data Breaches on the Rise

According to IBM and the Ponemon Institute's recent release of the 2015 Cost of Data Breach Study: Global Analysis, the average total cost of a data breach for the 350 companies participating in the research study increased from $3.52 million to $3.79 million between 2014 and 2015[LLC, 2015]. The study goes on to state that the average cost paid for each lost or stolen data record containing sensitive and confidential information increased from $145 to $154. The study goes into further detail regarding the costs and the root causes of a data breach. Cybersecurity threats are cited throughout the study as primary causes of data breach and loss. However, when the article addresses the factors that influence the cost of a data breach, either those that accelerate the cost or mitigate the threat and lower the potential cost of a breach, employee training topped the list of factors that decrease the per capita cost of data breach. Along with the extensive use of encryption and an on-site incident response team, employee training is identified as being able to reduce the cost of a data breach by $8 per record, taking the average cost per record from $154 to $146 [LLC, 2015]. According to the 2016 Shred-it Security Tracker information security survey conducted by Ipsos, 78% of small business owners in the U.S. and 51% of senior executive C-Suite respondents only conduct training on information security procedures one or fewer times per year. In addition, 28% of small business owners report that they have never trained their employees on security procedures[It, 2016].

A more recent study released by the Ponemon Institute entitled 2016 Cost of Data Breach

Study: United States, indicates that companies in the United States on average have both a higher cost per stolen record at $221 and a higher average cost of data breach at $7.01 million [LLC, 2016]. The data also indicates that there was a 7% increase in the total cost of breach and a 2% increase in cost per stolen record. It is clear that the cost of data breaches as a trend are on the rise, but the 2016 Ponemon study also indicates that many companies are taking measures to mitigate threats through various means. Improvements in data governance programs will reduce the cost of a data breach. Incident response plans, appointment of a chief information security officer (CISO), employee training and awareness programs and a business continuity management strategy continue to result in cost savings. Employee training reduced the average cost per record by $15.4, shown in figure 2.1 [LLC, 2016].

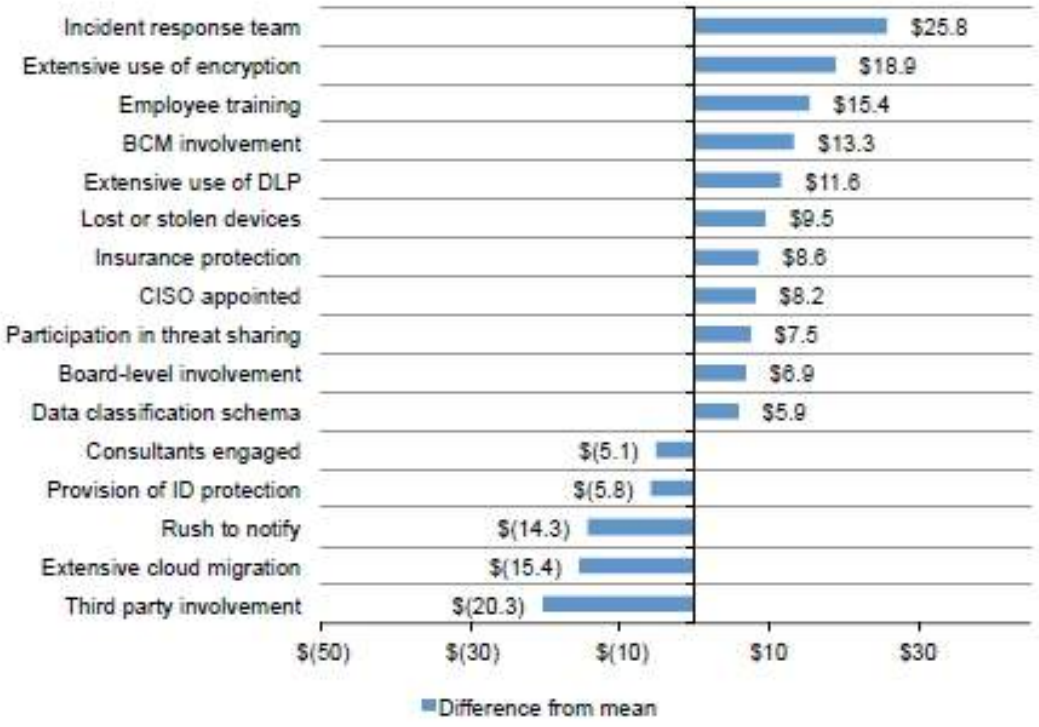


Figure 2.1: Employee Training reduced the average cost per record by $15.4. 2016 Cost of Data Breach Study: United States. Ponemon Institute

However, in that same study there is a different set of data that addresses the methods that companies participating in the survey took to respond to and remediate a data breach. According to this data, since 2010, implementation of employee training and awareness programs as a response to a data breach has decreased by 15%, shown in Figure 2.2 [LLC, 2016].

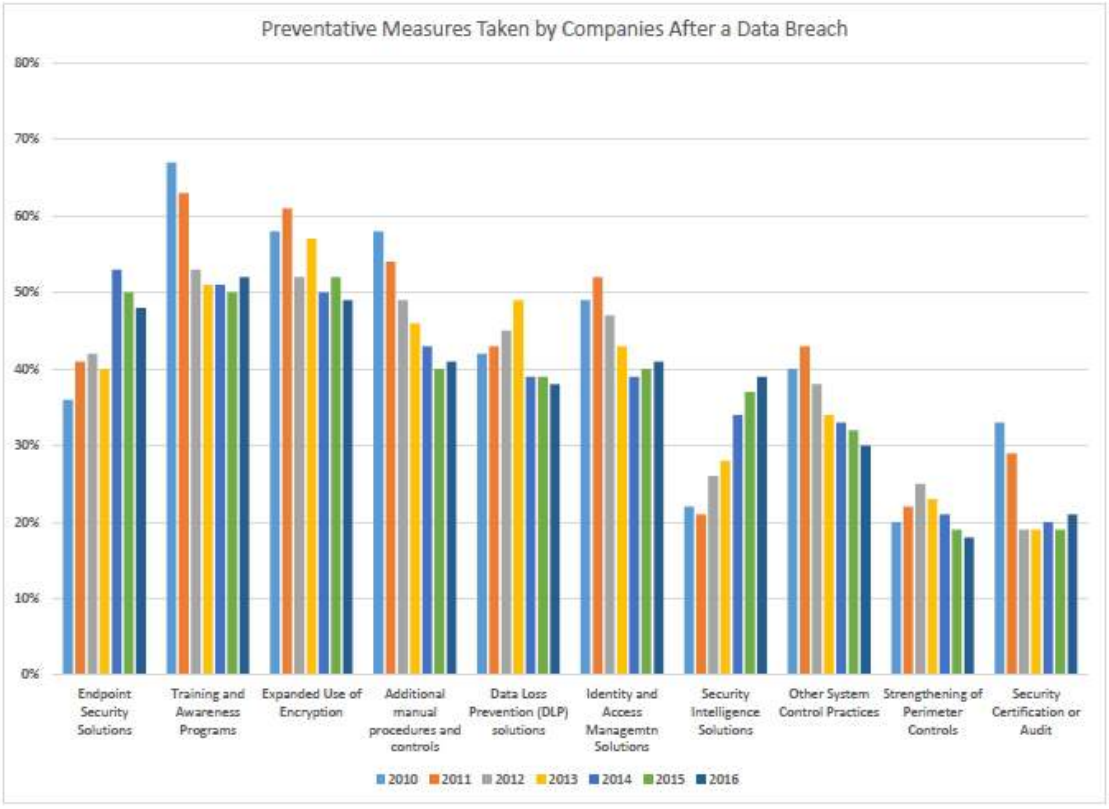


Figure 2.2: Employee Training programs implemented after breach decreased by 15%. 2016 Cost of Data Breach Study: United States. Ponemon Institute

According to Jones, during the same period when organizations are having a difficult time mitigating risk of breaches and developing appropriate countermeasures, employees are seeing more of the technology they use at the work place come into their homes and personal lives [Jones, 2010]. This is a threat to confidentiality because in some cases, the user is performing work related tasks on a non-work machine and non-work related tasks on a work machine. "The security requirements of the user for personal information, if they are considered at all, are normally far lower than those which are required to properly protect an organization's information." Besides the occasional news story surrounding a high profile data breach, home users don't have an understanding of information security requirements to effectively evaluate risks. And if users are giving the same level of consideration to personal assets and resources as they are company assets it could potentially lead to a data breach.

Based on these reports, it is clear that there is serious potential to mitigate controllable

security threats by implementing security education and training of end users. A meaningful training curriculum that is administered more than once a year could be the solution to the prevention of future instances of data loss or make a big difference in the speed of discovery and response.

2.2 Information Security Education, Training and Awareness

Building an effective security awareness program requires inclusion of education and training [Siponen, 2000]. Education can increase motivation of users and answer the question "why?", while training can increase skills and improve a user's competence of organizational security policy and addresses the "how?". Siponen explains "Since the 'why' part is extremely important, employees should not be satisfied with answers such as 'you just have to do it', 'this is the rule', or 'this is our policy'. Their motivations and attitudes are not likely to be increased in this way."

In order to plan and implement a valuable information security training program, it is important to understand the elements that hinder security awareness. Shaw et al. conducted a study that consisted of testing the security awareness levels of 154 MIS freshman at a university in Taiwan. This research defines security awareness as the degree of understanding users have regarding the importance of information security and their responsibilities to exercise sufficient levels of information security control to protect the organization's data and networks [Shaw et al., 2009].

Shaw describes the three major barriers to security awareness as employee's general lack of security awareness, employee's computer skills, and organizational budgets. Budgetary concerns are a main reason why organizations are reluctant to focus on training. Certain methods of training like face-to-face or classroom training are very effective but can get expensive. Since it is difficult to measure its potential payoff, it is harder to justify the investment. Other methods of delivery for security training may be cheaper, but less effective. For example, distributing plaintext documents to train employees and users about organizational security policy may be the cheapest way to deliver training, but it is less effective and hard to enforce.

In addition to limitations of an organization's budget, certain risk prone behaviors that occur on company equipment and over the company network could also be potentially harmful behaviors, yet are often overlooked by IT and corporate management. Behavior like online shopping and using personal email on corporate devices are good examples of this. Shaw et al. lists some of the most common risk prone behaviors are related to using company resources for non-work related

tasks and sharing corporate computing resources with non-employees [Shaw et al., 2009]. These behaviors can be further compounded by the adoption of corporate bring your own device (BYOD) policies. Using company resources with your device can blur the lines of ownership. It is important for an organization to be clear with its employees regarding the correct use of personal devices when used in conjunction with corporate intellectual property.

2.2.1 Motivation

Safety researchers have repeatedly challenged the presumption that simply telling people the relevant facts will allow people to optimize their behavior and manage risk. According to Stewart, the trouble for users is not just in finding the authoritative source, but also what the incoming information actually means and what to do with it [Stewart, 2009]. They give an analogy of a crisis related to the measles, mumps and rubella (MMR) vaccine that occurred in the UK. "A lack of understanding for the underlying science and how immunization works may have lead to opinions being given more weight than facts"[Stewart, 2009]. They suggest that even though there was an abundance of information available from authoritative sources, those who were at risk were not optimally instructed. Compare this case with information security, where those operating the technology don't have the best understanding of how the systems function. Stewart suggests that borrowing concepts from safety communications research is a good strategy to better develop information security awareness and communication. A "mental model" is a method of recording a set of perceptions that exist for a given audience which can then be compared to mental models of other audiences. They are often used as a systematic approach to risk communications. See figure 2.3 for an example. Experts compare models from different audiences and evaluate the differences in perception and are able to tailor communication for different groups, with the aim to change the behavior of users regarding certain risks.

In addition to presenting new training material on a regular basis, Peltier continues to state that it's important that the employee be able to relate to the material presented. If you are able to convince the user that using identification badges protects employees by ensuring that only authorized employees are allowed on company grounds, they will be more likely carry out this security process. He also suggests that segmenting the audience into different levels of training based on five metrics: current level of computer usage, what an audience really wants to learn, how receptive the audience is to the security program, how to gain acceptance and who could be a

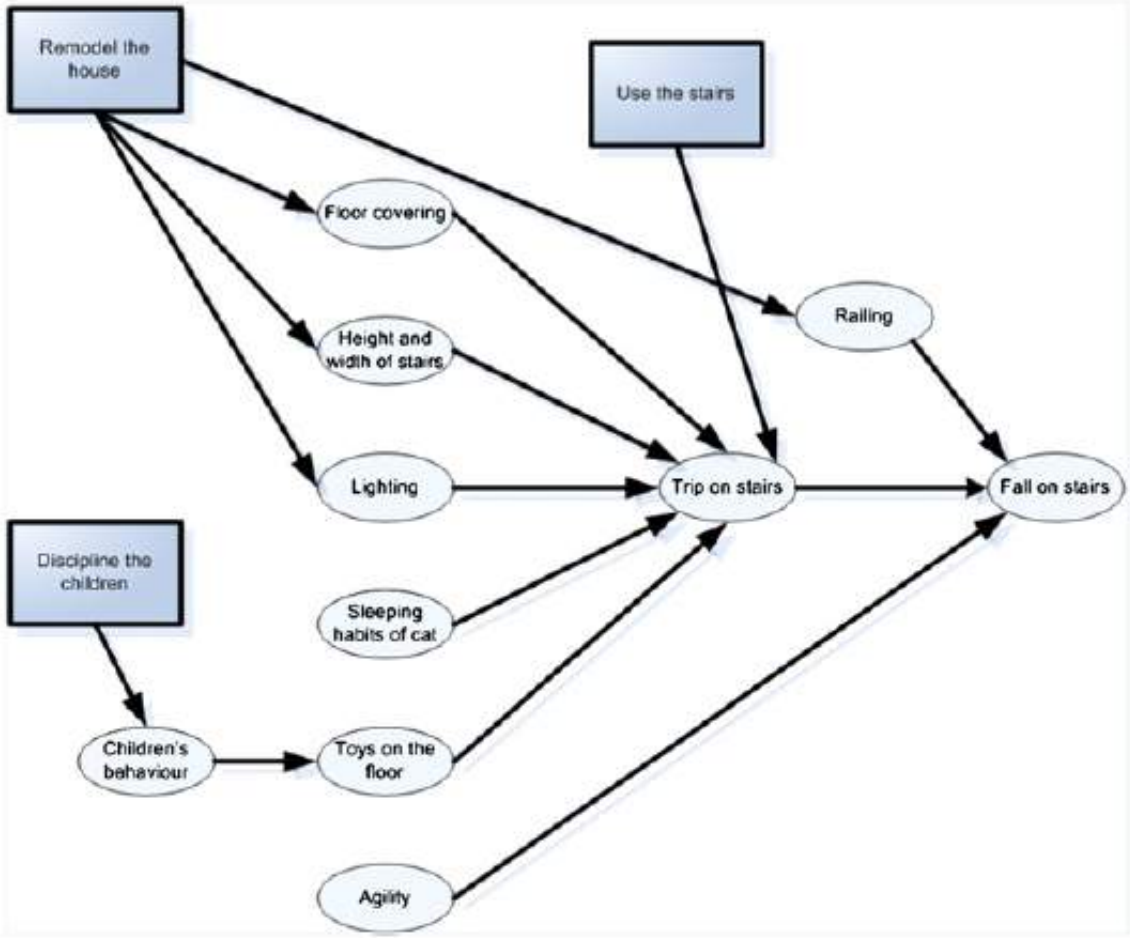


Figure 2.3: Example of a mental model, suggested by Stewart. This model shows potential actions one might take to address the risk of falling down the stairs. Compare this to actions one can take to avoid security risks.

possible ally. If the program designers practice effective listening, they will be able to cater their program to different knowledge levels and scale modules to best serve the users. It's also effective to put information into the program that the user is interested in. For example, Peltier suggests using news shows like "Dateline", "48 Hours" or other news stories that could reinforce the current issue. Showing clips from news stories focusing on a similar organization getting hacked will spark a conversation between employees about current policies and practices.

Siponen gives some practical approaches to motivation: Logic, morals and ethics, rationality, emotions, sanctions/pressure, feeling of security and well-being [Siponen, 2000]. With these principles, security guidelines and policies will be explained better and the user will be able to relate

better to the issues provided in security awareness training.

At its core, information security training and awareness programs are designed to prevent users from violating an organization's security policy. Hu et al. addresses the behavioral reasoning behind a person's decision to violate organizational policy. "We submit that when an individual is presented with an opportunity to commit policy violations, his or her behavior depends on the rational calculus of the costs and the benefits" [Hu et al., 2011]. Hu goes on to explain that there are three independent forces that control the determination of that cost-benefit evaluation. Individual propensity (which Hu defines as the degree of low self-control), an individual's moral beliefs (defined as the individual's judgment about right and wrong) and the perceived deterrence related to the misconduct (defined as the perceived certainty, severity and celerity of sanctions against the behavior). See figure 2.4.

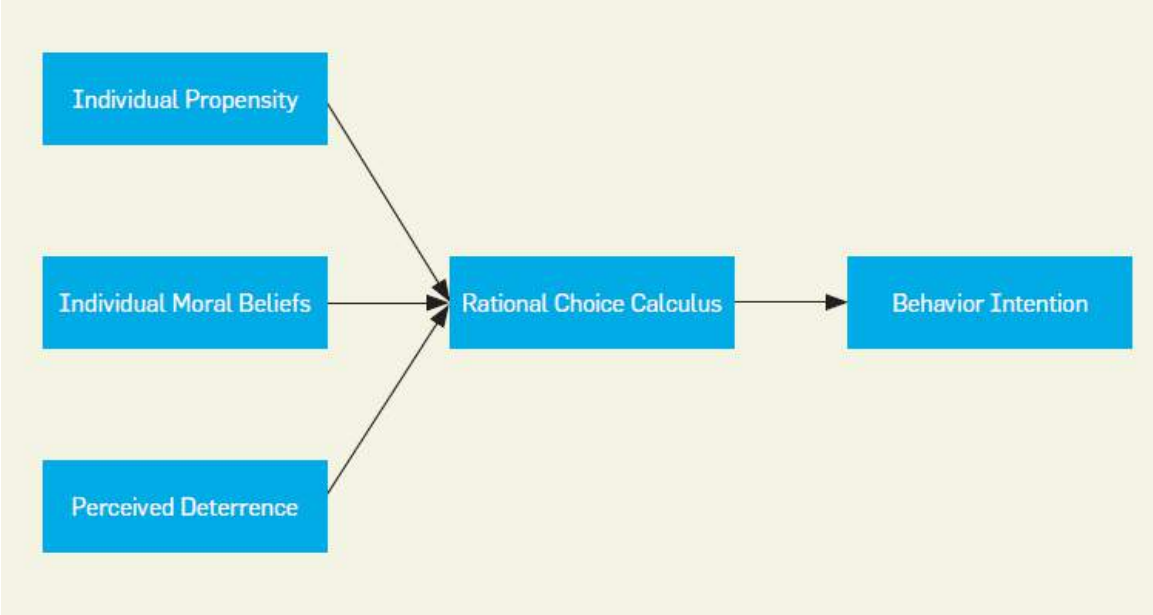


Figure 2.4: This model illustrates the three factors that Hu states help people calculate the cost-benefit analysis when making decisions

Hu et al. tested their theory by surveying five large Chinese organizations with three scenario-based questions that aimed to gauge the users likelihood to violate a given security related policy. The questions asked the participants about unauthorized access to payroll data, unauthorized access to and transfer of product designs and stealing and selling confidential price and cost data to competitors. The results of the survey indicated that when an individual is contemplating

whether to commit policy violations, the perceived benefits trump the perceived risks in the participant's decision making process. Based on the evaluation of the certainty, severity and celerity of the punishment of the misconduct, the results of the survey also indicated that deterrence has no significant impact on an individual's intention to commit policy violations [Hu et al., 2011]. They compare these results to those found in a study that surveyed criminals; 60% of criminals claimed that they did not think about any possibly negative legal consequences when making their decision to act, just the possible positive outcome of the crime. There are other ways to consider these results besides that deterrence is an ineffective way to manage employee behavior. For example, lowering the perceived benefit of violating policy and vetting candidates for employment based on answers to questions regarding morality and self control.

According to Mitnick et al., an organization's workforce must be trained, be aware and be conscientious of security policy in order to properly protect company assets [Mitnick and Simon, 2011].He suggests that having an ongoing security awareness program and that allocating 40% of the organization's security budget towards security training and awareness. A cornerstone of the training program should be getting every employee of the organization involved. One tactic Mitnick suggests is demonstrating that sometimes there is no line between company data and their personally identifiable information (PII) and that because the company stores information about each employee, like phone number, address and social security number, it's in the best interest of everyone in the organization to practice good security behaviors and protect organizational information.

2.2.2 Training Curriculum Design

Puhakainen et al. set out to empirically design a theory-based information security training and awareness program based on universal constructive instructional theory and the elaboration likelihood model. Their goal was to improve employee compliance with information security policies and procedures. The researchers explain that the elaboration likelihood model demonstrates how predictable, long-lasting behavioral changes can be achieved through cognitive processing [Puhakainen and Siponen, 2010]. The universal constructive instructional theory provides a framework for designing instruction that is customized for a certain learning subject and target group. See figure 2.5. These two models compliment each other in that UCIT constitutes the framework for the training curriculum, while ELM allows the training method to be evaluated through systematic cognitive processing of information.

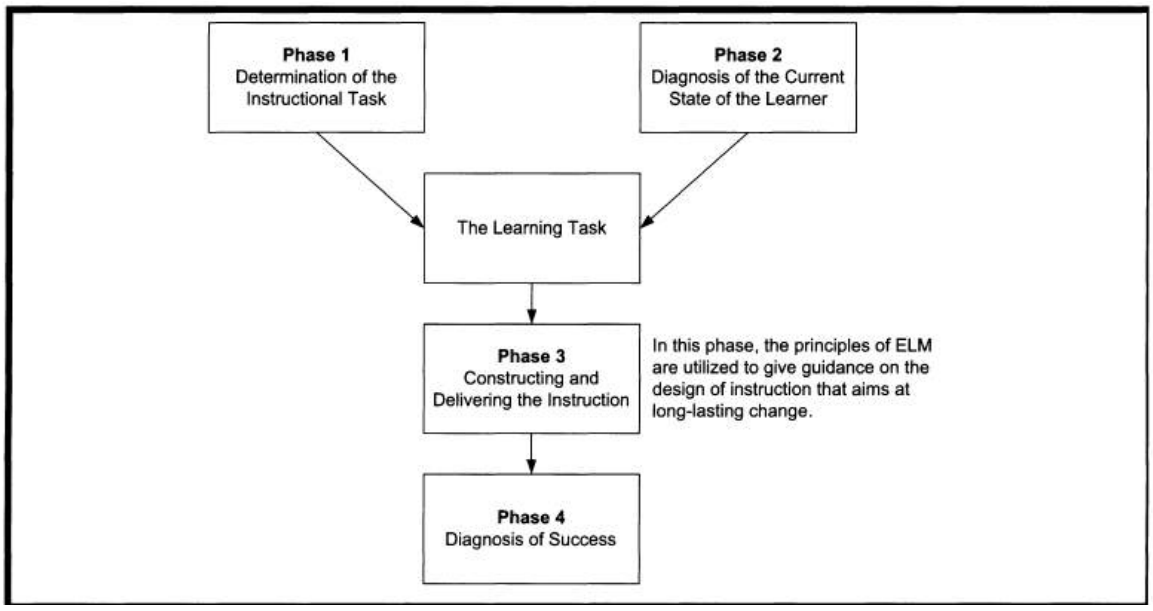


Figure 2.5: This model illustrates the four phases of instruction within the Universal Constructive Instructional Theory

The two models meet the requirements set forth by the researchers. One being that the training program is able to explain why and how the training is successful. It's important that the educators evaluating the plan understand the theory of how the program helps the people participating learn. In the case of information security training and awareness, it's important that the training explain how people learn, and also what learning principles are expected to change the user's behavior. Understanding these things will allow the training to be scaled for different groups. The second requirement basically states that there must be guidelines for how the training is to be delivered successfully in practice, so that the practitioners can implement it successfully. One requirement regards the design of the training, the other regards the cognitive evaluation of the methods.

The methods used to collect research data included interviews, a survey and participatory observation. Basically Puhakainen et al. wanted to gauge if employees had the knowledge and skills to comply with the current security policy while gathering information about employee attitudes and habits. Using the information collected in this phase of the study, the researchers began designing the training program, focusing on how the learner was to efficiently acquire the knowledge. They ultimately came up with three training sessions, each with multiple parts, targeting different types of users. For example, the first session had real examples of emails sent by the sales team that

violated the organization's security policy. Another session focused on teaching non-technical users the importance of encrypting confidential information and password protecting it.

After delivering the training, the results of the study were positive. Users were speaking positively of information security related issues as well as admitting that after the training was conducted they thought more often about the consequences of sending unencrypted information over email. The results showed that it is useful to use information security policy compliance training methods and ideas that enable learner's systematic cognitive processing of information [Puhakainen and Siponen, 2010]. In addition, it is just as important to be able to provide learning tasks that are personally relatable.

Security is often obfuscated by complex network design and a myriad of technical tools and terms and this is often a good excuse for employees to think they have no role in information security. Mitnick states that a good plan will make employees feel like they are on the "front lines" and their efforts are absolutely necessary to the security of the organization as a whole [Mitnick and Simon, 2011]. He goes on to suggest that modularizing the awareness program for different functional departments across the organization. Even thought there is no "one-size-fits-all" solution for all companies, there are certain groups that are widely adopted among many companies. Managers, IT personnel, computer users, non-technical personnel, administrative assistants, receptionists and security guards are the groups that Mitnick suggests using. Utilizing training methods that deter social engineering attacks is important for security guard, administrative assistant and receptionist personnel. Social engineering is generally defined as a hacker's clever manipulation of the natural human tendency to trust [Granger, 2001]. The hacker's objective is to talk to system users to and find out information that will help in granting their unauthorized access to the system. Because the human element is often the weakest link in the information security chain, attackers will often focus on users who have access to critical resources but don't fully understand how best to protect them.

Mitnick stresses that users who are not necessarily considered computer users by the organization cannot be overlooked when designing the security training and awareness program. Anyone who has access to office buildings or protected areas can be deceived into allowing allowing a threat to occur, and even though they may have only been responsible for allowing a physical intrusion, they could potentially be at fault for a computer intrusion as well. Because of this it's important to consider all of your users when designing the training and awareness program and cater different

elements to different types of users.

In order to propose a new information security training and awareness program, it's important to attain the correct levels of approval and funding. Attaining management's approval for any project should always be a priority. Desman describes a situation in his book "Building an Information Security Awareness Program," where he had an idea to use electronic signs to actively warn people of virus threats should they enter the network [Desman, 2001]. He had set the gears into motion and begun to recruit the electricians, building services and network engineers to work on his project when he got word that the "top guy in the company" shut down his project due to misuse of company resources. He suggests the following approach to avoid this problem in the future: "Once you have identified areas of concern that will require the concerted efforts of more than one person, it is wise to go to your immediate management with an outline of what you want to do, how much it will likely cost, and what the benefits to the company will be." Being able to defend your project by identifying all areas of the business that could be potentially effected by the proposed change. Both changes to an internal flow or becoming the recipients of some new service could potentially change day-to-day operations and being able to speak to all potential outcomes will illustrate your understanding of the scope and impact of the project. Being able to take this information, coupled with the approval of your immediate manager, to the executive level leaders of your company will aid the approval and acceptance of you project. Mitnick supports Desman's claim and makes the argument that information security training and awareness programs require substantial support from management. "Employees must see that senior management is fully committed to the program. That commitment must be real, not just a rubber-stamped 'We give our blessings' memo. And the program must be back up with sufficient resources to develop, communicate, test it, and to measure success" [Mitnick and Simon, 2011]. It needs to be clear to employees that management believes in the awareness program if it is to be successfully adopted and executed. Contextual information about the organization is necessary when deciding on what topics should be focused on in any curriculum. According to Furnell et al. the extent to which organizations are able to give focus to the issue is often influenced by practical considerations [Furnell et al., 2002]. They go on to say that the level of organizational protection must be proportionate with the value of the protected assets. They provide the example of putting finger print authentication scanners on workstations in a college lab that would represent a misuse of resources as the cost to install the scanners would outweigh the value of the data protected by those stations.

Organizations do not have only their own employees to consider when training around information security and awareness; often an organization employs contractors or third party entities and must grant them some level of access to critical systems and data. As the world saw in 2014, Target suffered a severe hack where the intrusion was traced back to credentials stolen from the companies contracted heating, ventilation and air conditioning, a third party vendor [Krebs, 2014]. According to Peltier, contract personnel should be made aware of the information security program goals and objectives, but they should included in the company's training and awareness program at high caution and discretion [Peltier, 2005]. If the contractor does not conduct their own security training program, it might be useful to hold separate training sessions targeted towards those users. And it's important to ensure that the contracts between the organization and the third party vendor explicitly states that all users must adhere to organizational security policy.

2.2.3 Effective Execution of Training and Awareness

"Any organization thinking of mitigating information security risks through purely technological countermeasures shall fail eventually" [Eminaaolu et al., 2009]. Eminagaoglu et al. state that every employee of an organization should be convinced to contribute and comply with security practices and rules for the organization to attain successful and effective management of information security. They carried out a case study with white-collar transportation employees in Turkey in response to several major security incidents that were mostly related to exploitation of access control on enterprise systems. The incidents resulted in loss and disclosure of critical employee data and were attributed to users selecting easy simple passwords, leaving their computer workstations unlocked while away from the desk, and by misusing administrative access rights by giving away passwords.

The project scope of the case study included a security training and awareness campaign for all white-collar employees in the enterprise. Password audits were performed on all of the active directory employee user accounts. Training sessions, workshops, puzzles and quizzes, posters, newsletters, web content and graphics were all used in the awareness program over the following year of the case study. The results of the study showed that weak password usage decreased among most users. In the initial password audit, 57.9% of user passwords were cracked within two hours. After six months, only 31.7% were cracked in that same amount of time, see figure 2.6. And after one year had passed since the inception of the training program, only 20% of employee passwords

1st Password audit results: (just before the project was initiated) Number of user accounts audited: 2846		% Broken (cracked) passwords
Number of passwords broken in less than 1 min	637	22.4%
Number of passwords broken within 15 min	1014	35.6%
Number of passwords broken within 2 h	1647	57.9%
Number of passwords broken within 24 h	2812	98.8%

Figure 2.6: Results from initial password audit. The positive outcomes of information security awareness training in companies: A case study

were cracked in two hours, see figure 2.7.

These results indicate that most employees improved their awareness during the course of the training and chose longer, safer and smarter passwords. Because of the implementation of the training program, most employees of the enterprise showed a tendency to comply with the information security policies.

Adoption and implementation of security training and awareness programs can be a hurdle for all organizations. However, Furnell et al. describes that, because staff capacity and financial resources can be specifically allocated for security awareness, larger organizations have an easier time executing training programs than smaller and medium sized enterprises (SME) [Furnell et al., 2002]. SME organizations' data and systems are no less valuable compared with larger companys' resources, but because of operational constraints that smaller companies usually experience, they can't have the same focus on security that they require. For example, lacking specific staff security professionals or having a non-expert bleed over into that role, lacking finances to bring in a third party consultant or to train the current staff, lacking understanding of or dismissing security related threats and inability or unwillingness to focus on information security because of business priorities are all examples of reasons why smaller companies might not be addressing security awareness in the right way.

2nd Password audit results: (6 months after the project began) Number of user accounts audited: 2911		
Number of passwords broken in less than 1 min	308	10.6%
Number of passwords broken within 15 min	715	24.6%
Number of passwords broken within 2 h	924	31.7%
Number of passwords broken within 24 h	2556	87.8%
3rd Password audit results: (12 months after the project began) Number of user accounts audited: 2924		
Number of passwords broken in less than 1 min	92	3.1%
Number of passwords broken within 15 min	203	6.9%
Number of passwords broken within 2 h	585	20.0%
Number of passwords broken within 24 h	1859	63.6%

Figure 2.7: Results from second password audit. The positive outcomes of information security awareness training in companies: A case study

Computer based training, or CBT is a good solution for smaller companies to train their employees on security related topics and be able to apply their new skills in a soft environment. [Furnell et al., 2002]. A security training tool that can enable the investigation of countermeasures within organizational policy and is coupled with scenario based training modules can be a cost effective method to increase security awareness in small and medium sized organizations.

Additionally, a security training program must continue to stay in front of user on a regular basis in order for it to remain successful [Peltier, 2005]. He states that programs fail because there is little to no follow up after the program is launched. Usually the response to the "big splash" program launch is to do nothing. When new programs are launched, and the old one is done away with, employees of the organization are conditioned to wait out the program and remain indifferent until it dies and something else replaces it. Peltier argues that if you are able to map out a strategy for your plan that is designed to keep the message in the users' mind and daily activities, they will be less likely to remain inactive and indifferent.

In addition to presenting new training material on a regular basis, Peltier continues to state that it's important that the employee be able to relate to the material presented. If you are able to convince the user that using identification badges protects employees by ensuring that only authorized employees are allowed on company grounds, they will be more likely carry out this security process. He also suggests that segmenting the audience into different levels of training based on five metrics: current level of computer usage, what an audience really wants to learn, how receptive the audience is to the security program, how to gain acceptance and who could be a possible ally. If the program designers practice effective listening, they will be able to cater their program to different knowledge levels and scale modules to best serve the users. It's also effective to put information into the program that the user is interested in. For example, Peltier suggests using news shows like "Dateline", "48 Hours" or other news stories that could reinforce the current issue. Showing clips from news stories focusing on a similar organization getting hacked will spark a conversation between employees about current policies and practices. Siponen gives some practical approaches to motivation: Logic, morals and ethics, rationality, emotions, sanctions/pressure, feeling of security and well-being [Siponen, 2000]. With these principles, security guidelines and policies will be explained better and the user will be able to relate better to the issues provided in security awareness training.

2.2.4 Interview with Mike Orr of IBM

Mike Orr, a Program Manager for Life Sciences Compliant Cloud Deployment for IBM and lecturer at the University of North Carolina Wilmington takes IBM's security training program yearly. IBM's cybersecurity and privacy training program was contracted out to the SANS institute who had produced digitally animated short films for topics like social engineering, phishing, proper use of social networks and how to use mobile devices securely among others. Videos averaged about three minutes in length and were followed by about four to six questions regarding content from the video. After successfully completing the quiz, documentation that is specific to IBM's security policy is delivered to the user.

As Orr took the learning it was apparent that the training was split into generalized info from SANS regarding best practices followed by IBM specific security policy. Besides the SANS logo embedded into the video, Orr noticed that the word supervisor was being used by the narrator and noted that IBM doesn't use that terminology. Besides this Orr had a lot of good things to say

about the training. “This is by far the most memorable training I’ve done for security,” remarked Orr. He said that he found the information regarding the process of off-boarding employees who had been let go was valuable and something that hadn’t occurred to him as being too important. The social networks and mobile modules also had a lot of good, up-to-date information that Orr found informative, although maybe not as useful to him personally. He was able to complete the training without getting a single question wrong. However, at one point he wanted to test the case of what happened if he answered incorrectly. He was disappointed that there was no specific feedback; the application just returned an incorrect message and highlighted the correct answer. There was no feedback on your answer and no chance to try again.

Although Orr stated that this was the most memorable security training he had ever received he still had some complaints. It was noticeable throughout the training that many of the graphics were reused throughout the videos and somewhat took away from the experience. In addition, there were some aspects of the module for Data Access and Data Security that didn’t apply to Orr’s role with IBM and there was a confusing question regarding access rights and restricting user privileges which Orr did not know the answer to. He wished there were more relevant information and questions related to his role in the company. In addition, Orr had some complaints about the IBM specific documentation that was delivered following each module. Each document had several links inside that led to IBM knowledge repositories. There was a document for incident response that had a scenario table that was split up into several pieces and organized poorly. Orr remarked that if there was a real incident, this documentation would not be useful. If there was a single and simple way to report incidents and discover next steps, it would be more useful than the current solution, according to Orr.

Orr explained that these training modules are coupled with phishing attacks. He was fooled by the attack because although he scanned the URL and saw that it was not from IBM, he believed it might still be credible because IBM utilizes contractors regularly. He also described role playing scenarios that he used to do for security awareness training where different IBM employees would act out certain security driven scenarios to help teach appropriate behavior. Orr found them to be useful but wasn’t sure of their effectiveness as far as delivery of information goes.

To conclude, Orr found the delivery of the content via digitally animated videos to be helpful, informative and progressive. However, when the IBM issue-specific documentation was presented in plain text with a multitude of links to IBM knowledge pages, he found that to be ineffective and

described those pages as an "information overload." If the pages had been more organized, perhaps graphical and led to a more organized knowledge landing page, they would have been more effective.

2.3 Gamification

Training employees is an important aspect of operations for organizations of all sizes. Traditional training methods often include videos portraying appropriate workplace behavior, electronic learning modules that test a user's understanding of training materials or even posters or newsletters that give information on organizational protocol. In a presentation at the RSA conference in 2014, Ira Winkler and Samantha Manke, the President and Executive Vice President of the security company Secure Mentem compared new training methods involving gamifying security training with traditional methods of training [Winkler and Manke, 2014]. They discuss the core principles of training gamification: clearly defined goals, rules, ongoing feedback, voluntary participation. They argue that it can't be considered a game if users are "forced" to take it.

2.3.1 Gamification Methods

According to Brian Burke, Research Vice President and analyst at Garner Research, "Gamification is most successful when you are engaging with employees to help them complete their own goals, not organizational goals. Shared goals are achieved as a consequence" [Marvin, 2015]. Burke also suggests that making the game more social, like letting employees check their points against each other through leaderboards adds positive reinforcement through incentivization.

The Infosec Institute argues that games in the workplace must be relatable and engaging. They describe an information security training game called "SecurityIQ AwareED", that uses interactive exercises that implements scenarios that employees have likely been in before [Institute, 2016]

The research of Gutzwiller et al. suggests that working in cyber and information security gives very little reward. In fact, the successful performance of your job often rewards you with more work. For example, thwarting an active attack will lead to other issues needing to be resolved and more vulnerabilities to be identified and patched [Gutzwiller et al., 2015]. In fact, they describe the negative performance metric "How did I fail this time?" as a significant source of input to many operator's day-to-day operations and work. They go on to cite that in terms of a cyber environment, the operational interfaces lend themselves to this negative interaction. After performing a task

or making a decision, there is little feedback from the interaction and all evidence of the event disappears. "Furthermore, analysts may feel disconnected from their job, and disconcerted that their prior decisions seem of no measurable value or impact. This psychological burden of joyless operation and resulting frustration is contributing to turnover and burnout" [Gutzwiller et al., 2015].

These researchers focus primarily on improving the experience of cybersecurity specialists by improving their day-to-day experience, but their conclusions translate to the defense of gamifying information security training for all employees of an organization. "Hedonomic design approaches suggest that once an interface facilitates safe, effective and usable performance, further design and experimentation should determine how to make these interactions pleasurable" [Gutzwiller et al., 2015].

As Mitnick states, information security is at a crossroads within the business world, as being one of the most important subjects that all users must be educated about, but also being one of the most inherently dull topics in business [Mitnick and Simon, 2011]. "The aim should be to make security information awareness and training an engaging an interactive experience." Methods that Mitnick suggests are demonstrating social engineering attacks through role playing, reviewing media coverage and reports, as well as case studies regarding recent attacks on other businesses and discussing what could have been done to mitigate those threats and showing informative and entertaining videos related to the organization's security policy.

Kalinauskas states that the purpose of a gamified platform is to create an engagement activity that can engage and involve the user in the content [Kalinauskas, 2014]. Badges, leaderboards, points and leveling up can help the game designer achieve some success in gamifying a learning experience, but the researcher also mentions that the reward of the game can't be based on a false sense of achievement and that it needs to create true value for the user and produce natural involvement. In some ways, this is an inherent benefit of gamification, because the potential of the medium comes from the ability to attract and engage users, tailoring content towards specific audiences with different skill sets and goals.

Kalinauskas continues to discuss "Flow Theory," which regards users being able to absorb knowledge at an increased rate during a challenging activity. A "Flow" for the purpose of the theory is defined as "a line between boredom and anxiety, when a subject is challenged enough to be interested" [Kalinauskas, 2014]. The game designers should aim to keep the user in the flow for as long as possible and increase the difficulty of each challenge as the user continues to play, be

successful and fail, learning as they go.

Information security has the ability to empower users and protect organizational assets. However, according to Jones many organizations view security as a barrier and only take it for the penalties that accompany negative behavior [Jones, 2010]. Jones explains that it would be a better approach to instead reward positive behavior by offering incentives to employees who perform positive security related tasks. The goal would be to attract attention to information security, create some buzz about good behavior and get employees involved, thus potentially changing their perspective of their organization's security policy and hopefully changing their behavior as a result.

2.3.2 Gamification Applied

According to Kingsley et al. using video games for educational purposes has been proven to not only enhance performance, but also motivation [Kingsley and Grabner-Hagen, 2015]. Those researchers primarily focused on gamification in the classroom, where instructors would gamify a concept by creating achievement badges, levels and experience points (XP) to indicate a student's level of comprehension and to add some incentives to keep learning. In the gamified learning module used in the study, students were able to self-regulate their learning experiences, choosing which subjects to do in their own time based on skill level, interest and time. As one student participating in the study claimed, "A fun way to learn, but it does not feel like learning [Kingsley and Grabner-Hagen, 2015] This lends itself to gamification of training in an organization because if users are able to dictate their own experience with the module, it is less likely to feel forced.

Kim goes into detail on several different gamified experiences and how they are able to influence changes in behavior [Kim, 2015]. The Fun Theory is a website that identifies and recognizes groups who have gamified some every-day experience and made it fun, thus making a step towards changing people's behavior for the better. One of the winners of the award are the Bottle Bank Arcade machine which lights up and makes sounds and awards points when people are able to put their glass bottle to be recycled in the right hole in a certain amount of time. About 100 people used the machine in one night, while only two people recycled at the nearest conventional recycling facility. Another winner was the Speed Camera Lottery, where drivers were alerted to the game and in a certain stretch of road, if you were caught by the machine while driving under the speed limit, you were entered into a lottery to win real money. The real money for the lottery came from citations taken from other drivers caught speeding by the same machine. During the three day

period of the experiment, almost 25,000 cars passed the machine and the average driving speed was fond to decrease 22%, from 32 kilometers per hour to 25 kilometers per hour.

Kim makes the point that the gamified applications and tools discussed in the article can add some fun to every-day activities, as well as encouraging users to be more socially responsible, safe, healthier and more productive. Kim discusses an application called EpicWin that lets you create a character and role play while making a to-do list. When you accomplish a task from your list, it lets you upgrade your character with different traits and watch them grow. Chore Wars is a similar application where users can gain experience points for doing chores in the office or at home. The game calls them "quests," and as you accomplish them, you're given the option to level up your in-game character or get real world rewards. These gamified experiences are designed to reduce procrastination and make dull tasks into fun games. Researchers de-Marcos et al. conducted a study in which they evaluated new social network and gamified learning methodologies on 371 undergraduate students enrolled in an Information and Communication Technologies course that covered the basic competencies in computer and office applications [De-Marcos et al., 2014]. They split up the students into three groups: one who took the course supplemented with gamified instruments, one who took the course supplemented with social networking instruments and a control groups. Their research questions regarded if gamification and social networking instruments would impact learning in large classroom environments, if they will impact participation rates and if students will have a positive attitude towards these tools.

The gamification element was a plug-in deployed into the learning management platform BlackBoard, and split up learning activities into challenges and levels and rewarded students with badges and trophies upon the completion of each level, which was intended to give students a sense of mastery and progression as they learn. Badges would be awarded when a student completed an entire section to mark their status, or marking a user as a "rookie" when they first joined the system, or awarding them randomly after completing an event to provide a sense of surprise to the process. See figure 2.8. A leaderboard created a sense of competition between students and as a chance to compare performance between students.

The social networking element of the platform provided how-to videos for basic operation of certain tools, step-by-step videos of the solutions for certain activities, while students were allowed to submit any related video that they found or created. See figure 2.9. A blogging feature for both students and teachers, a following function that allowed students to get notified on selective

Figure 2.8: An example of the badging system built into the Blackboard platform for this experiment

content across the site, a question and answer section where students were able to ask, answer and rate questions, a built in Twitter application that allowed students to publish short blurbs and a commenting and "liking" function that provided students the ability to share ideas and interest regarding the content posted or produced by any other student in the system.

The results indicated that both experimental groups outperformed the control group in the four learning modules. And in the comparison between the two experimental groups, the researchers found that the group using the social networking element performed significantly better on the modules for spreadsheets and word processing. However, the results of the final exam for the course had some different results. It turned out the students in the control group outperformed both experimental groups on the final exam. The researchers suggest that this might have been the result of their experimental sections and their traditional e-learning courses were all delivered at the same time, and it was an overload having to deal with all of those materials at once. In addition, the nature of the gamified and social networking elements tended to focus on the practical application of computer concepts, while neglecting the acquisition of knowledge that comes with traditional approaches. The students were surveyed after the study concluded and answered questions about their use of the social networking and gamified elements. Time availability, lack of knowledge about the tools existence, technical problems and dislike of competition were all reasons students gave for why they didn't use the tools.

Figure 2.9: An example of the social networking element built into the Blackboard platform for this experiment

For future study, de-Marcos et al. have some insight and suggestions. Regarding the choice between including social networking elements or gamified elements, the researches believe that a hybrid of both technologies should be blended for the best results. "Long-term motivational benefits of gamification can be coupled with the collaborative and participative capabilities offered by social networks" [De-Marcos et al., 2014]. They believe that the next steps should include more gaming elements like a narrative structure and immersive 3-Dimensional environments.

Kyle Felker is a digital initiatives Librarian at Grand Valley State University, and he wrote about the process of gamifying experiences in libraries in order to further engage users. He begins by addressing two different ways to apply gamified concepts. One way matches that of the experimental design of de-Marcos, where game-like structures are applied to an existing system, like applying badging, trophies or a point system in a classroom [Felker, 2014]. Felker states that even though this approach is easier to apply up-front, it can feel artificial and fails to change the underlying nature of the learning experience. The second approach that Felker addresses is to design learning experiences from the ground up as games. He cites industry expert Raph Koster's definition of a game as "a system of rules that, taken together, creates a simplified model of some aspect of reality." Consider how Monopoly uses a system of rules about movement and resources to simulate

capitalism, while Chess uses a different set of rules to simulate warfare [Felker, 2014].

Felker states that some libraries have already implemented some gamified applications. One used Apple iPods and the note-taking application Evernote to create a scavenger hunt experience for library orientation, another turned the orientation process into an online mystery scenario. At Felker's home university of GVSU, they developed a quest-based mobile game that aimed to create an engaging experience in introducing library services to students. Putting users into the shoes of different roles is also a useful way to engage users. Felker uses the example of open access in libraries, where users could take on the role of a researcher or a publisher in a game that models information scarcity and control in a university environment. Players are given resources that represent time and money and are tasked with negotiating the cost of producing information against the number of people who will use it and be able to access it.

It may seem obvious, but Felker reiterates that most educational games fail because they aren't fun. The primary goal of a game should be to engage and reward the user, but too often the games will focus on placing the education goal before the fun of the experience of playing the game, and will fail in perfecting the gaming experience in their application. Felker suggests that using iterative development strategies, coupled with assessment of and adaptation to user feedback with high levels of testing and revision can lead to success. In addition, using a paper-prototyping strategy at the beginning of the development process can be a faster and cheaper way to map out the application. Coming up with a rewards structure is also an important element of design. Using external motivators like money and prizes can be damaging to the user's desire to learn the content because they will only participate in order to get the rewards. A second approach is to consider intrinsic drivers to reward users. Teaching players valuable lessons that align with things they find personally meaningful or empowering can be a positive, alternative way to reward users. Finally, it's important to be able to define your educational goals from the beginning of the development process. You must be able to address what you want users to be able to do after playing the game, and this will aid the development of the game and help determine the success as you continue to revise and evaluate.

2.3.3 Interview with Jordan Pike of nCino

Jordan Pike, the Manager of Infrastructure and Security Operations at nCino, a software development company in Wilmington, North Carolina oversees the selection and administration of

security awareness training for the organization's employees. This involves several elements of testing including phishing attempts on employees, creating content for training materials and ensuring compliance is met annually. The training is administered once a year and is required for each new employee upon hire.

nCino uses Litmos as their learning management system. Pike mentioned that he is satisfied with their current solution with Litmos in that it functions well operationally and is easy to use. However the features are somewhat light. "It's efficient at delivering content, capturing responses and correctly monitoring completion status." Pike creates all of the content videos and questions himself and uses Litmos and nCino University as a platform to administer the training and track performance metrics across the organization. The videos are formated as "white board" sessions with a screen share where Pike discusses training points while showing and writing relevant information on the screen and displaying the correct security driven behavior with his mouse. "You feel as if someone is there talking to you and I'm not just reading a script." Keeping the videos short is important. They are easier to follow and don't stretch the attention span of the user. Shorter videos are easier to make and far easier to update. This style caters to security training because the field is constantly shifting, and being able to push out updated training modules simplifies the training process. nCino as a company modularizes their training by department, but Pike says that there is no modularization of security training at nCino yet. However he does have sincere interest in finding a security training solution, or alternatively creating one in-house, that would modularized for developers. To his knowledge there is not a product commercially available off the shelf that offers these services.

According to Pike, when the company first started the videos were lower quality, recorded in 4:3 aspect ratio and were very bland. After refactoring the videos this year he got a lot of positive feedback. He found his own way to partially incentivize users to view and pay attention to the videos by putting the same phrase into every video, like an "easter egg." He found that users would come by and say those phrases to him and to members of his team, illustrating that his method worked and that people were watching, paying attention and bringing things away from the training. "They said the phrase two times already, where is it going to be in the next video?" After changing the style of the video, he had people talking about the training, effectively generating interest and buzz around the office.

According to Pike, testing email phishing attacks is one of the most effective way to teach

security awareness. “Some phishes are more successful than others, just depending on the nature of the phish” Pike goes on to say that it depends on who is being targeted. He will usually send phishing attacks to small groups, either pretending to be an outside entity or impersonating someone from within the company who’s email address is slightly incorrect. “There are things you can tweak to check if you are making people aware.” Not only does Pike check if the user clicks, but also if they report the attack. The system as it is does not track whether or not an individual clicks. All that is reported is a percentage of users who clicked. Pike is interested in potentially adopting the ability to “teach in the moment”; to be able to insert himself in that moment of negative behavior and provide immediate feedback is a goal of the training program.

Pike does have some logistical concerns regarding gamification. He suggested that if a user fails a training and is forced to take time out of their work day and re-train, is it right to reward them with “points” even though they originally executed a negative behavior? He asks how can that play into incentivizing good behavior? Pike is also concerned with people who already don’t care about security training. He cited an example of the three users in the organization who had been putting off the training for a few months. He stated that the people who don’t realize the value of the training are likely the users who need it the most. Pike wants a way to especially insert himself into situations with those users and expressed hesitation regarding the effectiveness of gamifying their training experience. However, Pike mentioned that there are many others in the office, that if you give them points for performing tasks, they will make sure they are at the top. It’s the other users, the last 25 users in the office to complete the training that next year’s training needs to be designed around.

“There’s no current product on the market that combines good phishing with a great learning management system.” Pike is looking for a system that can combine some of the great features from PhishMe and other tools that allow you to customize phishing emails and spoof your own domain with a platform like Litmos that allows you to manage and distribute your content. He would also like to be able to see if and when users pause or rewind their videos to see if there was something that wasn’t explained well, or if something was never rewound he could make more content like that. To put more marketing analytics into how the training is consumed would be great too. He wants to get away from content that is just produced for the purpose of being consumed once a year. As far as gamifying security training, Pike suggested having a module dedicated to a worker on the road. Different environment-driven scenarios like hotels and coffee shops to teach what sort of behavior is

appropriate in those scenarios when users are connecting remotely. He had previously looked into a solution offered by Wombat Security that had a coffee shop scenario that gave immediate feedback and taught in the moment.

2.4 Education

2.4.1 Bloom's Taxonomy

According to Adams, "Knowledge is the foundational cognitive skill and refers to the retention of specific, discrete pieces of information like facts and definitions or methodology, such as the sequence of events in a step-by-step process [Adams, 2015]. Adams goes on to say that "knowledge can be assessed by straightforward means, for example, multiple choice or short answer questions that require the retrieval or recognition of information." Recalling facts from memory can indicate knowledge, but the next level in Bloom's Taxonomy regards comprehension, where a subject should be able to use related terms in their own words, compare and contrast concepts and explain principles to others. It's important to understand that increasing comprehension will help learners begin to incorporate knowledge into their existing cognitive schemas and help the learner see links between related subjects in real-world concepts [Adams, 2015]. The third level of Bloom's pyramid, application, extends comprehension by suggesting the learner apply their knowledge to these real-world situations, giving them a brand new context. See figure 2.10. In the design process for my gamified information security awareness application, I plan to utilize principles from the application level of Bloom's Taxonomy. The modules I plan to include will ask users apply understanding of the organization's security policy in a real-world context. The training modules will place the learner in situations that emulate their work day, and asked to demonstrate a sequence of actions that illustrates their comprehension of important security related behaviors.

Next in Bloom's Taxonomy comes analysis, which requires the learner to be able to distinguish fact from opinion and identify the claims upon which an argument is built. Critical thinking will help a learner break down new information into concepts and terms that they are familiar with based on the previous steps in the pyramid. Synthesis, the fifth step in Bloom's Taxonomy entails applying the previous steps in their entirety and creating a new solution or product. Finally, evaluation is the final step in the pyramid. When an instructor reflects on a concept and utilizes learner feedback and assessment to judge the potential effectiveness of their lesson, they are using critical

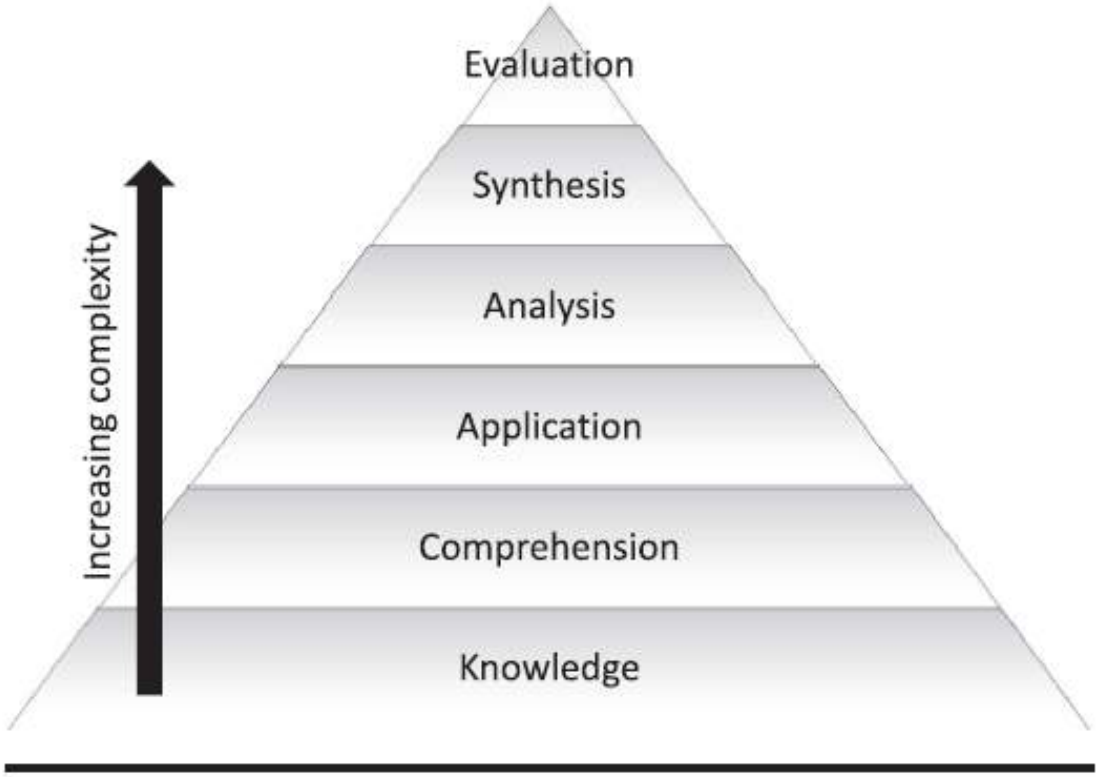


Figure 2.10: An illustration of Bloom's Taxonomy

thinking and evaluation.

Bloom's Taxonomy is useful because it encourages instructors to create learning objectives in behavioral terms to consider what the learner should be able to do following instruction. Learning objectives using some of the action verbs in figure 2.11 can be useful when gauging the structure and shape of the lesson to be taught. In future development for the gamified information security awareness application, it will be important to determine learning outcomes that will drive the development of the game modules. Defining clearly what the learner should know and be able to do after each module with learning outcomes will be critical in proving that the training is effective.

2.4.2 Educational Scaffolding

According to Shapiro, the design of a hypermedia assisted learning system can support learning outcomes for both novice and high level learners. Shapiro suggests that through effective "scaffolding", learners will be able to meet their objectives through the use of site maps, global system

Bloom's Taxonomy Action Verbs

Level	Definition	Sample verbs					Sample behaviors
KNOWLEDGE	Student recalls or recognizes information, ideas, and principles in the approximate form in which they were learned.	arrange define describe duplicate	identify label list match	memorize name order outline	recognize relate recall repeat	reproduce select state	The student will define the 6 levels of Bloom's taxonomy of the cognitive domain.
COMPREHENSION	Student translates, comprehends, or interprets information based on prior learning.	explain summarize paraphrase describe illustrate classify	convert defend describe discuss distinguish	estimate explain express extend generalized give example(s)	identify indicate infer locate paraphrase predict	recognize rewrite review select summarize translate	The student will explain the purpose of Bloom's taxonomy of the cognitive domain.
APPLICATION	Student selects, transfers, and uses data and principles to complete a problem or task with a minimum of direction.	use compute solve demonstrate apply construct	apply change choose compute demonstrate discover dramatize	employ illustrate interpret manipulate modify operate	practice predict prepare produce relate schedule	show sketch solve use write	The student will write an instructional objective for each level of Bloom's taxonomy.
ANALYSIS	Student distinguishes, classifies, and relates the assumptions, hypotheses, evidence, or structure of a statement or question	analyze categorize compare contrast separate apply	change discover choose compute demonstrate dramatize	employ illustrate interpret manipulate modify operate	practice predict prepare produce relate schedule	show sketch solve use write	The student will compare and contrast the cognitive and affective domains.
SYNTHESIS	Student originates, integrates, and combines ideas into a product, plan or proposal that is new to him or her.	create design hypothesize invent develop arrange assemble	categorize collect combine comply compose construct create	design develop devise explain formulate generate plan	prepare rearrange reconstruct relate reorganize revise	rewrite set up summarize synthesize tell write	The student will design a classification scheme for writing educational objectives that combines the cognitive, affective, and psychomotor domains.
EVALUATION	Student appraises, assesses, or critiques on a basis of specific standards and criteria.	Judge Recommend Critique Justify Appraise Argue	Assess Attach Choose Compare Conclude Contrast	Defend Describe Discriminate Estimate Evaluate	Explain Judge Justify Interpret Relate	Predict Rate Select Summarize Support Value	The student will judge the effective- ness of writing objectives using Bloom's taxonomy.

Figure 2.11: Action verbs can help determine the shape of a lesson

structure and strategic hyper-link style and placement [Shapiro, 2008]. In addition, "lack of prior knowledge, poor metacognitive skill, disorientation and poor system design can prevent learners from achieving their goals" [Shapiro, 2008]. Including the fundamental components described above into a hypermedia system is referred to as Embedded Scaffolding by the author. By simply highlighting important links or making subtle suggestions to the user through the system interface, the very design of the system can aid learners in maintaining focus on the learning objectives and will control frustration by preventing disorientation in the information space of the system [Shapiro, 2008]. Among other uses, scaffolding serves to recruit interest, reduce degrees of freedom, aid learners in maintaining direction, mark critical features, control frustration and demonstrate principles.

Navigation of a hypermedia assisted learning system should be a cornerstone of the system's design. According to Shapiro, there is evidence that learners interact with systems differently in terms of site navigation; some being more "principled" than others [Shapiro, 2008]. "Specifically, some seemed to use ease of access as a criterion to guide link choice, more often avoiding inconvenient links even if they might have been more appropriate choices."

Scaffolding can also be used to adapt hypermedia assisted learning systems to learners of different knowledge and skill levels. Domain novices need more guidance when using a hypermedia assisted learning system because they are unable to use an existing body of knowledge as a foundation for new information [Shapiro, 2008]. This lack of knowledge can lead to increased disorientation of the learner while using the system and therefore distract their focus from learning the subject matter presented by the system and instead focus solely on struggling with system navigation. "Organizing a system with hierarchies or other well-defined structures is useful to novices because such structures provide learners with information about how ideas are related in the system" [Shapiro, 2008]. This can simplify the content presented by the hypermedia assisted learning system and help the learner remain oriented. Shapiro suggests that site maps are a good way for domain novices to find relationships between concepts. "Allowing learners to see the global structure of a hypermedia system is useful in that it provides a bird's eye view of the 'landscape'. Giving the learner a view of the 'big picture' provides perspective on the domain in general and can aid in the creation of global cohesion" [Shapiro, 2008]. It's highly important to design the system, the global organization and the structure with the final learning goals in mind. Especially regarding domain novices, some aspects of the learning material may appear more central than others, so it must be obvious to the learner how to continue through the system on the most relevant path when there are multiple different paths of content to choose from.

In addition, attaching helpful comments and notation to links, as well as highlighting especially important info for novice users can help with system navigation and establishing connections between topics. Flagging the most important links with a special color can be convenient for users who are unable to judge which facts, links or documents in the system are more important. However, as Shapiro points out, this strategy should be used sparingly because if too many links are flagged with high importance, the meaning of the flag will be lost. Shapiro continues by suggesting that "important instructional events" can be used to control the flow of the system. By maintaining some sort of default pathway for learners, you can steer them towards links, documents or buttons that will be tailored and potentially adapted based on their skill level, thus strengthening learning for the proposed lesson.

Application of these elements of educational scaffolding in future design iterations of my training application should be considered. Especially in the knowledge section of the application, where learners will be able to access the documentation of the organization's security policy. In the

preliminary design phase of the knowledge section, I presented the learner with recent and important updates, the ability to search the knowledge repository for information they seek and a quick guide of current tasks. Applying notation to links, color coding different buttons and flagging tasks will be important to quickly orient new domain users to the flow of the application.

2.4.3 Learning Outcomes

According to Hill, assessing learning outcomes is an integral component to ensure that quality learning is occurring [Hill, 2012]. In a general sense, learning outcomes can be defined as a broad set of competencies or, what a learner is expected to know, understand or be able to do at the end of the learning period [Caspersen et al., 2017]. Caspersen states that in some contexts, employability is also related to learning outcomes in that "anything an individual possesses that can be seen as leading to an increased probability of positive economic outcomes, or other personal outcomes relating to the area of work." Basically the learning outcome would be to increase a learner's competency of a given topic related to their occupation.

Caspersen et al. state that there many ways to measure learning outcomes, including knowledge and skill tests, grades and self-reported measures. Grades can be a good way to demonstrate a learner's acquisition of subject knowledge while also providing feedback to students and giving some context to employers (and other interested parties) to the learners level of competency. Knowledge and skills tests can also be used to assess a learners grasp of the knowledge domain. However, grades can be criticized for lacking standardization and tests don't give much feedback about the quality of the student's learning, even though it might be evidence of what was learned. On the other hand, self-report instruments (a survey or questionnaire assessing a learner's feelings, attitudes, beliefs etc) can help assess the learning experience, but does not assess the level of acquired knowledge. According to Caspersen, the above highlights the importance of separating the different purposes of measuring learning outcomes and of being aware of the contrast between measuring learning and measuring knowledge. It must be clear what is intended: the measurement of quality, competence or learning [Caspersen et al., 2017]. It's important to understand that measurements of knowledge does not necessarily indicate anything about the measurement of learning.

I believe that applying a hybrid of evaluation techniques will be important to evaluate the learning process within my gamified security awareness training application. Testing learners with post-module content questions will gauge the learner's understanding of the topics presented and

evaluate the effectiveness of how well the user actually learned and applied the principle presented in a given module. Combining this with questions that evaluate the game module will also help determine if the method of learning through gaming is truly effective or if it hindered that learner's experience.

Chapter 3

Proposed Application

3.1 Problem

As discussed in the previous sections of this paper, the main problem that my proposed project will address is the issue that human error is still a leading cause in organizational data breaches. These breaches can be mitigated through proper execution of employee training and awareness programs, but many companies don't approach employee training in an effective way. Training is often viewed as a check box to be filled in on a compliance form during an auditing period. For employees, it's usually a distraction that must be done once a year. There are many forms of training programs that organizations can adopt, each with benefits and drawbacks. One-on-one training sessions are often the most effective, but also the most expensive. Computer Based Training is often the most cost effective, but it can be difficult to reinforce complex topics in an interesting or captivating way.

3.2 Solution

In order to effectively design a gamified security training and awareness program, the program must:

- Be adaptive to each organization's values
- Contain gamified, scenario based training modules

- Reward users for participating and executing secure behavior
- Allow users to redeem points for real rewards they are interested in earning
- Be administered throughout the year, instead of just once a year
- Utilize elements of games, such as Badging/Trophies, Achievements, Leaderboards, Easter Eggs, etc.

My solution to the issue described above is to design a gamified security training and awareness program that is adaptive to the organization's needs. The program would feature interactive game-like modules that put the employee into scenarios they will likely have encountered before and will encounter again, in order to better reinforce more secure behavior in those situations. Examples would be working remotely from a hotel room or coffee shop, how to detect and report a social engineering attack, creating and remembering a strong password, among other topics. Each module will have different teachable moments, presenting the employee with choices that they might actually experience in their work day. The game will have multiple sequence paths, and if the employee goes down the wrong path, they will be corrected and allowed to start back over at a checkpoint; this allows them to re-experience the situation again, this time making the correct choice.

The employee's goal will be to complete the game module and earn points. Points will serve multiple purposes throughout the program. They can be redeemed for real-world rewards and incentives. Your rank on the leaderboard will be determined by how many points you have earned. Points help identify your status of mastery within the application. The more points you have earned, the more opportunities you will have to earn points in the future.

Points will also be earned in other ways. In an effort to make other real-world moments teachable, employees will be tested with fake social engineering and phishing attempts. If employees are able to detect the attempt and report the attempt, they are rewarded with points. If they are unable to detect it and the test attack is successful, they will experience a teachable moment and their behavior is corrected. There will be other ways that employees will be able to earn points as well. In that figure, you'll also see that users will be able to contribute blog articles to the knowledge repository. Rewarding users for sharing their security related experiences from their personal lives or from situations where they failed to detect a social engineering attempt at work will help keep security on users' minds year-round.

Creating an interactive, gamified security training and awareness application that provides real rewards for good performance, is implemented throughout the year and is adaptive to needs of individual organizations will be the solution to the problem presented above.

3.2.1 Scenario-Based Training Modules

It will be important to design the gamified modules around scenarios that the employee will likely encounter in an actual work day. Employees will be better able to recall the correct, secure behavior in the real world after having played the game module that addressed that situation. For example, in a module on working remotely from a coffee shop, if the organizational security policy requires users to connect to the enterprise network through a virtual private network (VPN) connection, their real world behavior will be reinforced by having to perform that action when playing the game module. Something else that will allow employees to better see how their individual role in the organization can impact company data assets is to create learning modules that are role based. If the security training program is identical across the organization, it might be easy for someone in a non-technical role to see how it doesn't apply to them. But if you can design a game module specific to that user's role, showing how a daily activity they do or error they make could be detrimental to the organization's assets, they would likely pay closer attention and have a more security focused attitude going forward.

3.2.2 Incentives and Rewards

Providing real-world incentives and rewards for good security related behavior will add another layer to the gamification of the application. However, it is important to understand that the rewards must be dynamically chosen based on the culture of the organization. Some organizations might want to redeem their points for a gift card, while others might value a ten minute coffee break with the CEO more. When configuring and adapting the training program for an individual organization, this must be part of the design process. Interviewing people in the organization and getting their feedback would be an effective way to gauge the culture of the employees and would help determine an appropriate reward structure.

3.2.3 Achievements

Achievements can give employees targets to work for. If you have a visual clue indicating your progress towards a given goal, coupled with that knowledge that you'll be granted a bonus point payout if you complete the achievement, you will be more likely to work towards accomplishing this goal. They should increase employee participation in the training program and support the effort to continue the training program throughout the year. You can unveil new sets of achievements every month or every quarter to get people to log back in and try to earn the reward.

3.2.4 Knowledge

A smart, user-friendly and complete knowledge repository should be included in the application. An employee needs to be able to access the organization's issue specific security policy with a few clicks of their mouse to ensure that every policy is understood and not obfuscated. Structuring the knowledge repository like wiki software would allow for easy navigation. Dedicating a section of the knowledge repository home page to featured articles showcasing important policies that IT wants the organization to focus on, as well as user-submitted blog posts will allow employees to quickly catch up on new and important information, as well as provide them with a chance to earn points by reading articles and writing blog posts.

3.2.5 Social Aspects

Allowing users to communicate through the application, while comparing point totals and performance is also important to persuade users to continue using the application throughout the year. Users should be able to post status updates and view other users' updates, view a leaderboard where they are ranked next to their fellow employees based on point totals and other metrics. It can help promote competition throughout the enterprise and might cause some users to work harder to hit the top spot on the board for bragging rights. The trophy case will show a quick glance at the leaderboard and display each user's most recently posted status update.

3.2.6 Trophies

Trophies will be similar to achievements, except that they will be surprise rewards. You won't know what actions will earn you a trophy, so it rewards continuing use of the program in order

to uncover the trophies and fill up your trophy case. The trophy case screen of the program will serve a few purposes. It will give quick glances at the leaderboard and your standing, show three achievements that you are currently in progress of earning and your progress towards them and a case full of the trophies that you have earned and short descriptions of each one.

3.3 Methodology

In this section I will discuss several factors that influenced my choices in the design process of the application. I chose to include several features in my prototype based on feedback I got from a interviews with professionals, common features and ideas I read about while conducting my background research and inspiration from other existing gamified experiences.

3.3.1 Background Research

A major concept that I chose to utilize in my program is to practice year-round deployment of new training modules. Suggested by the sources cited in my background research, I consider it to be one of the cornerstone concepts of my proposed security training and awareness program. In order to avoid information security awareness becoming nothing to an organization but a compliance check, it's important to reinforce key security concepts all throughout the year. In addition, another important concept I garnered from my background research, being able to tailor the real earnable rewards and incentives for each organization based on their employee culture. Being able to adapt the rewards dynamically based on what motivates each organization is one of the major keys to this programs successful implementation.

3.3.2 Interviews

I interviewed a few local professionals seeking some of their advice on what they would look for in an ideal training and awareness program. One of my interviewees is the manager of infrastructure and security operations at a local software development firm and a major portion of his responsibilities is to administer their organization's security awareness training in order to meet compliance. While discussing my prototype with this interviewee, he told me that having good phishing simulation testing is something that is important to include, but to his knowledge, there is no current security training solution that combines a learning management system with phishing.

I wanted to be able to provide phishing attack simulation and social engineering attack simulation included in my program, as well as providing points to those to detect and report these attempts. Training people to be aware of different types of attacks and how to report them can be an important way to prepare employees for real attacks.

In addition, this interviewee gave me partial inspiration to create the coffee shop game module by suggesting that he would be highly interested in a module that showed employees proper behavior while working on the road, specifically how to work from a hotel room. This is a module that I would be interested in designing in the future, but it was too similar to the coffee shop module that I was interested in developing for the initial prototype of my application.

I also got the perspective of a user of a large company's cybersecurity training. I observed him while he took the training and we discussed his likes and dislikes of the training modules throughout the process. My main takeaway from this interview was that a well-designed, user-friendly and easy to search knowledge repository should be included in the application. After completing each module, we were presented with a hard to read page with links to knowledge articles for the issue specific security policy. Clicking on the links lead us to the knowledge articles, but we found it hard to search for specific information we were looking for. We also noticed that the videos included in the training had a lot of recycled images and animations, to the point where it was noticeable. The interviewee commented that he would prefer training that was fresh and original. Which gave me the idea to deploy new and original training modules throughout the year.

3.3.3 Observation of Other Gamified Experiences

Lastly, I was inspired to include elements of my application based on observation of real-world gamified experiences. Nike + uses methods to gamify exercise and encourage fitness by allowing users to track their performance and attempt to beat their previous scores. In addition, they make exercising social by letting you communicate with friends and compete to earn higher scores. You are able to work towards earning achievements and get surprised by trophies. One example of a trophy rewarded in the Nike + application is that if you went for a run on Halloween, you earned a special trophy you might not have known was coming to you. I chose to incorporate all of these elements into my application.

Chapter 4

Prototype

My approach to developing the application prototype has gone through two iterations. One being a paper phase where I drew out each major screen of the application with pencil and paper, and the second being adapting those paper prototype screens into a more interactive model using Sketchflow, a prototyping tool built into Visual Studio 2013 Expression Blend.

4.1 Tools

After drawing out each necessary screen with pencil and paper, I was ready to begin translating those ideas into Sketchflow. I wasn't too experienced with the tool so it took some time to get acclimated to the software. It has built-in tools like buttons, text boxes and scroll bars that can add interactivity between screens and several ways to program animation to give the application a more game-like feeling. I treated screens like the leaderboard and Trophy Case as early iterations to practice designing with this tool. I treated those early screens as practice for the most important portion of the prototype: the coffee shop game module. By this time I was experienced enough with the tool to confidently add animations and interactive elements, linking multiple screens together to create a short example of what a finalized game might look and act like.

The Sketchflow application interface allows you to access everything you might need to work on your project within a few clicks. See figure 5.1. Adding assets, creating states (used for simulating animation), changing opacity of objects based on user input to control the flow of the game can all be done in the Sketchflow main editor screen. Sketchflow also has a useful map feature built in. You

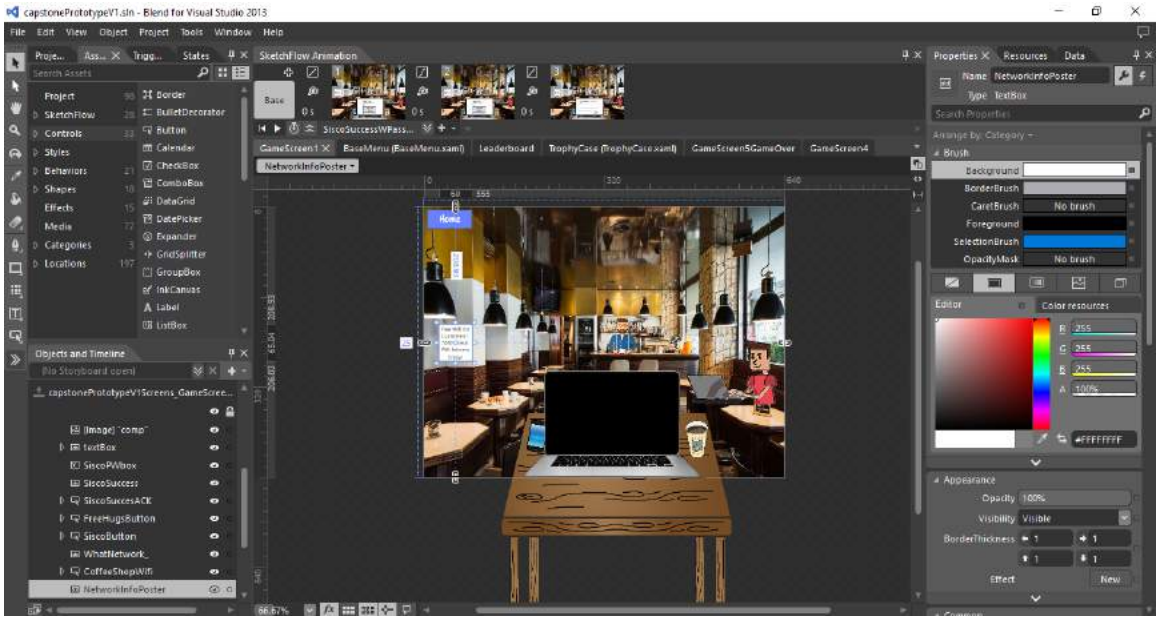


Figure 4.1: A quick glance at the sketchflow user interface.

can see which screens rely on other screens, how the navigation flow of the application will go and can help when the design of your application becomes more complex. See figure 5.2.

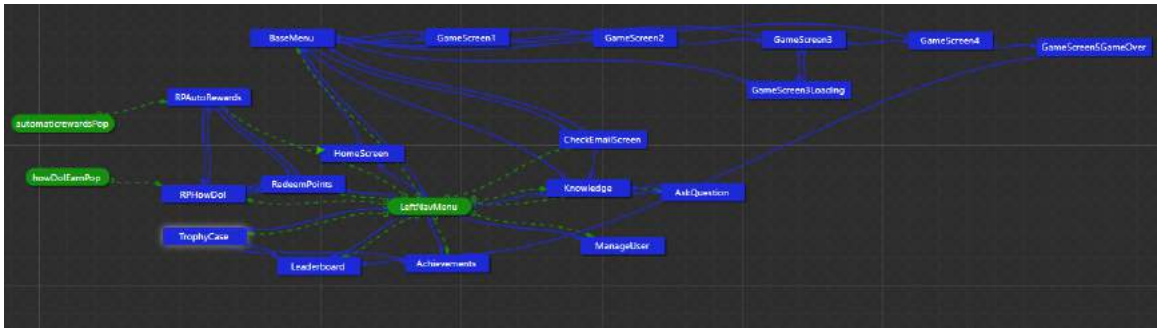
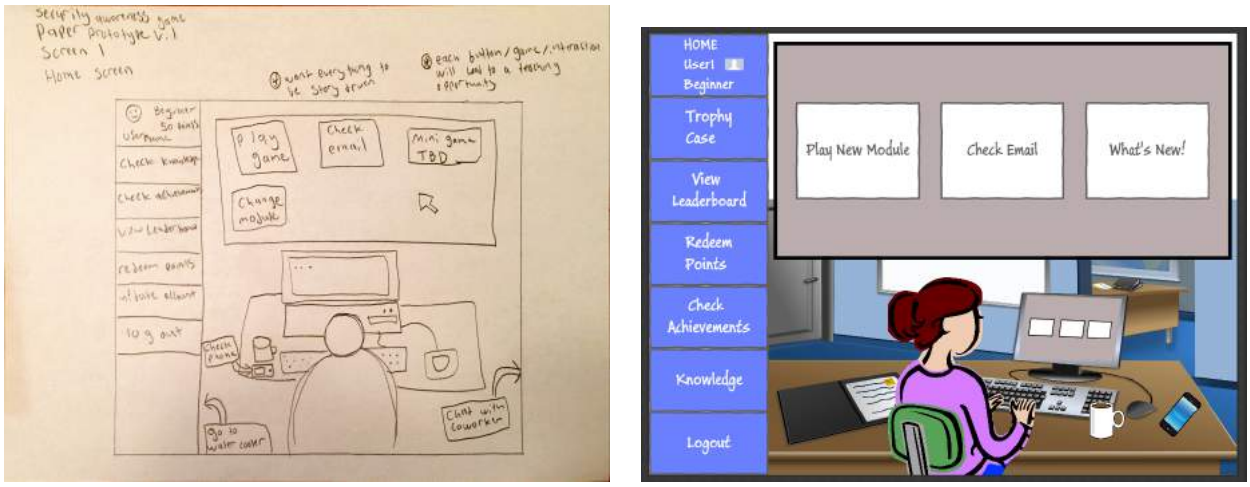


Figure 4.2: Map of prototype screens. This layout helped map out the application.

Another tool I found myself using often was a freeware application called GNU Image Manipulation Program or GIMP. In order to get any asset that wasn't already built into Sketchflow, I had to acquire images from elsewhere. In order to edit them down to size and customize to my needs, I would open them in GIMP and use tools to edit, crop, alter color, and remove image backgrounds. After this, it was an easy process to copy the image and paste it into the Sketchflow screen, only needing to move it around and resize it.

4.2 Prototype Screens

When drawing out the initial paper screens, I had a few ideas in mind I had gotten from doing background research into security awareness programs and other gamified applications. Keeping the the game personal was going to be a big part of the application. Making the base menu the perspective of the user from behind their back while sitting at their workstation was really important to me because I wanted the user to feel like they were in the game and could relate to the actions of the in-game player. A goal for later iterations would be to make the base menu even more interactive. I would allow the user to move around the game environment, going to various spots you might find in an office(kitchen, friend's desk, etc), and hiding easter eggs, which are unexpected or undocumented features in software or games, for the user to find and enjoy, giving the game a little more depth and feeling of freedom. For example, allowing the user to click on their phone on the desk and be able to check their messages, and hiding some secret functionality there. See figure 5.3 for a side-by-side comparison of my initial paper prototype screen and a completed Sketchflow screen for the base menu of the application. I had the same strategy when designing the coffee shop



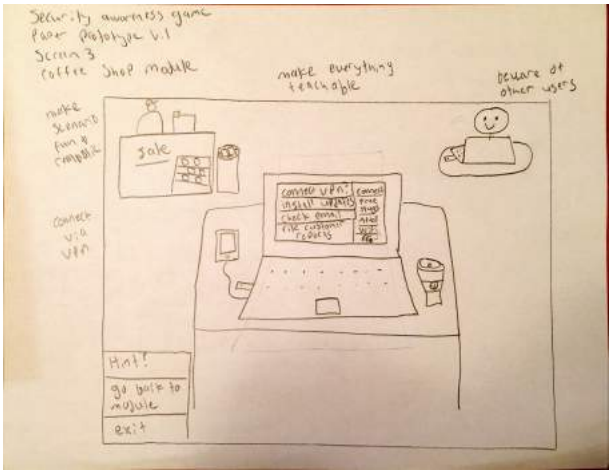
(a) Initial Paper Prototype Screen

(b) Completed Prototype Screen in Sketchflow

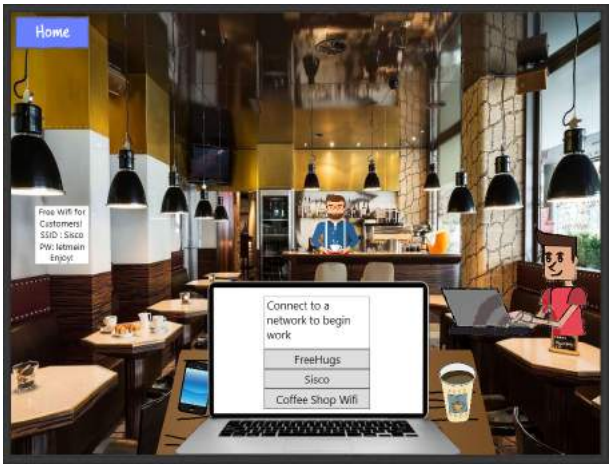
Figure 4.3: The base menu prototype screen. Side by side comparison of initial paper prototype screen and completed prototype screen

module. I wanted to have the user be able to feel like it was actually them making the decisions, so I put the game into a first person perspective. See figure 5.4 for a side-by-side comparison of my initial paper prototype screen and a completed Sketchflow screen for the coffee shop module of the

application.



(a) Initial Paper Prototype Screen



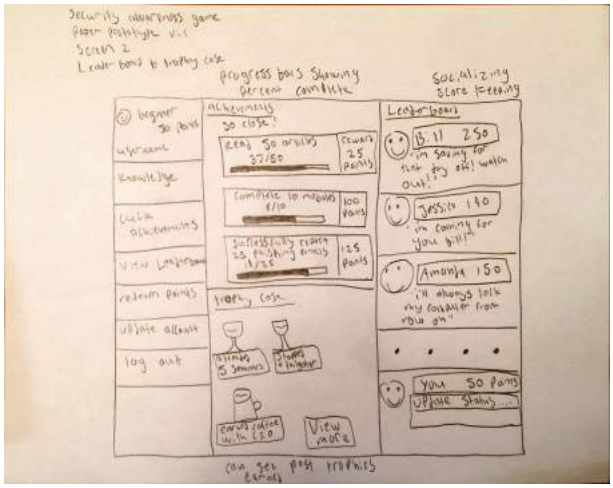
(b) Completed Prototype Screen in Sketchflow

Figure 4.4: The coffee shop module prototype screen. Side by side comparison of initial paper prototype screen and completed prototype screen

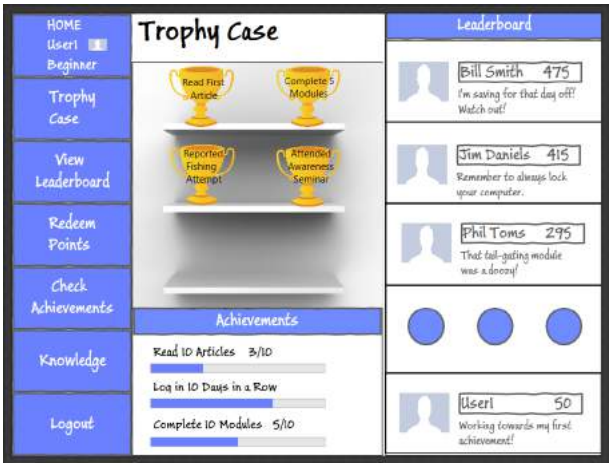
For some screens, I found myself needing to adapt after originally designing the screen on paper. An example would be my screen for the leaderboard. When designing on paper, I had the idea to show achievements and earned trophies on the same screen. When it came time to develop those screens in Sketchflow, I realized that the leaderboard and achievements would need their own screen, but that the original screen I designed on paper still would have a place in the application. It became the Trophy Case screen that gave quick glances at some of the most important information from both the leaderboard screen and the achievements screens, as well as displaying the trophies that the user has earned while using the application. See figure 5.5 for a side-by-side comparison of my initial paper prototype screen of the leaderboard and a completed Sketchflow screen for the Trophy Case.

4.3 Future Iterations

One thing that I struggle with towards the end of the first Sketchflow iterative cycle was getting a good sharable version of my project to distribute and collect usability testing results. My goal was to export my project as an .exe file to maximize the number of people I could collect surveys from. Unfortunately I was unable to do this. In future iterations it will be important for



(a) Initial Paper Prototype Screen



(b) Completed Prototype Screen in Sketchflow

Figure 4.5: The trophy case prototype screen. Side by side comparison of initial paper prototype screen and completed prototype screen. Originally planned for this screen to be the leaderboard during paper prototyping phase, but ultimately chose to give achievements and leaderboard their own screen and make this the Trophy Case

me to switch to a prototyping tool that will easily let me export the project file into an executable to share.

Going forward, I'll be collecting usability data in person and tweaking the application based on that feedback.

Chapter 5

Results

5.1 Usability Studies

To get feedback on my application prototype, I created a usability survey that would evaluate users' experiences in three different categories. The categories were navigation, functionality and appearance of the application. See Appendix A to view the survey questions. I sought user feedback from fellow undergraduate and graduate students, from professionals at Live Oak Bank in Wilmington, North Carolina and from attendees of the Wilmington Information Technology Expo, or WITX where I had a booth set up to showcase my application. I received 23 responses to each survey question. I used a Likert scale for each question, allowing the user to select a number between 1 and 10 to evaluate the experience, 1 being the highest rated option and 10 being the lowest rated option.

5.1.1 Navigation

I wanted to gauge users' feedback on their experience navigating through the application. I found that the average response to the question "Overall, how would you rate your experience navigating through the application" was 2.65 where 1 represented "very easy" and 10 was "very difficult". See figure 5.1.

The average response to the question "Overall, I was satisfied with the amount of time it took to complete the application" was 3.22. For the question "When going through the coffee shop

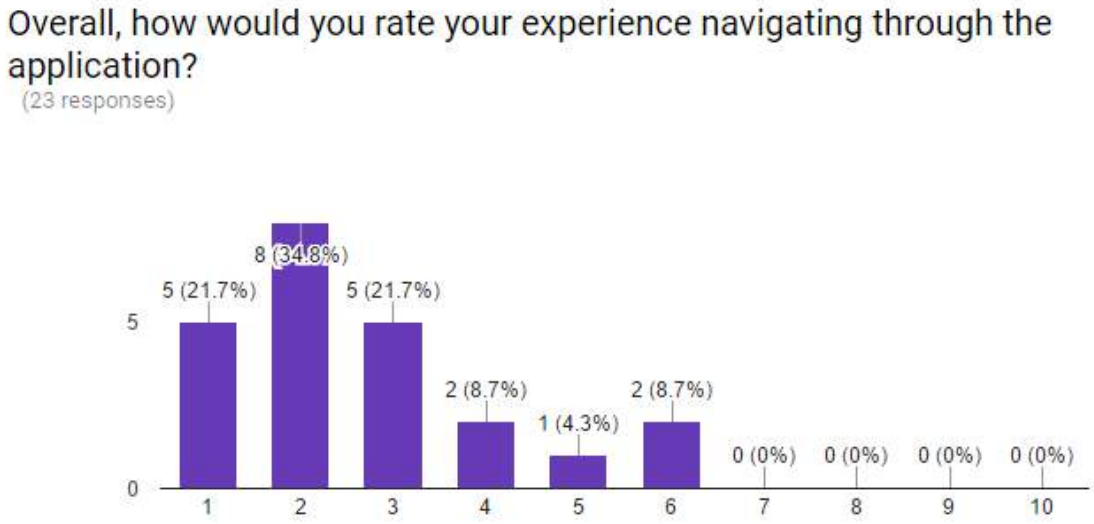


Figure 5.1: Ranking percentages of answers for the question "Overall, how would you rate your experience navigating through the application?"

module, I found it easy or difficult to navigate to the end" where 1 represented very easy and 10 represented very difficult, the average response was 2.57. The average response to the question "Was navigation through the application intuitive?" was 2.60.

The average response for the question "Did you find the screen that let you view how to earn points? If so, how easy was it to get there?" was 4.26. The average response to the question "How often did you find yourself needing to navigate back a screen, but you were unable to do so." was 2.83. For the question "Was it clear where the "Home Screen" was?", the average response was 3.17. The total average for all responses in the navigation section of the usability survey was 3.04.

5.1.2 Functionality

The average response to the question "Overall, how would you rate the functionality of the application?" was 2.43. The average response to the question "How well did you understand the terms/verbiage used in the application?" was 2.22. See figure 5.2. The average response to the question "How would you rate the consistency of the application?" was 2.48.

The average response to the question "When playing the Coffee Shop module, how clear was the distinction between error and success?" was 2.65. The average response to the question "Overall, how satisfied were you with the support information provided by the application? (Help

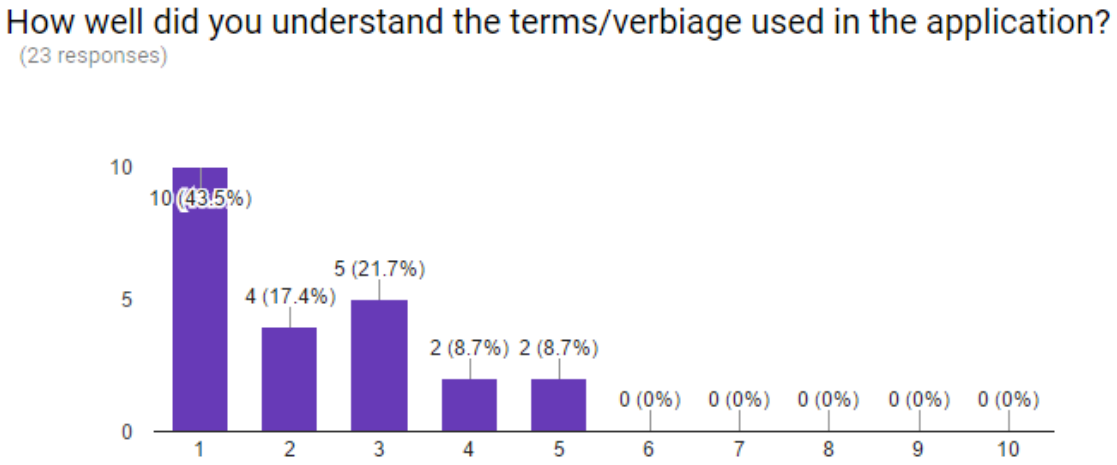


Figure 5.2: Ranking percentages of answers for the question "How well did you understand the terms/verbiage used in the application?"

messages, documentation etc.)" was 3.22. For the question "Did you view the trophy case? If so, do you think you know what it is?", where 1 represented "I know what it is" and 10 represented "I don't know what it is/I didn't find it", the average response was 3.74.

For the question "Did you view every screen in the application?" where 1 represented "I think so" and 10 represented "I don't think so", the average response was 4.35. The average response to the question "Do you have a clear understanding of what the application is designed to do?" was 2.04. The total average for all responses in the functionality section of the usability survey was 2.89.

5.1.3 Appearance

The average response to the question "Overall, how would you rate the appearance of the application?" was 2.48. The average response to the question "Did the appearance distract at all from the functionality of the application?" was 2.96. The average response to the question "How did you feel about the color scheme?" was 2.74. The average response to the question "How would you rate the layout of the application?" was 2.74. The average response to the question "Did you find the appearance of the application consistent?" was 2.48. The total average for all responses in the functionality section of the usability survey was 2.68.

Chapter 6

Conclusion

The development of this prototype training application was in response to the fact that human error still ranks as a leading cause of data breach for organizations of all sizes. The goal is to implement a gamified training and awareness program that is applied throughout the year and puts users into real-world situations where they will have to apply secure behavior to pass gamified modules and earn real rewards and incentives by participating. By doing so, it will incentivize the process of executing secure behavior, ensure that information security is more than simply a check box on an auditor's form for executives and allow all employees in an organization to see how their role is impacted by information security policy. If securing an organization's data assets truly lies in the hands of the end user, then empowering the user with the tools and motivation they need to execute secure behavior is the key to preventing and mitigating future data breaches.

6.1 Future Work

This project requires an iterative approach, so it will be important to continue work to improve the application through future iterations. In order to extend this project, I will need to address some of the issues that were raised from the usability study. Improving terminology across the application might help improve low scores that were given on questions regarding not being able to find certain screens or be able to understand the concepts on those screens. It will also be important to more clearly identify what is clickable within the game module, as I received feedback from users indicating that at times during the Coffee Shop Module, it was not clear what was meant

to be interactive and what was not.

Creating additional iterations for the application and continuing the process of gaining user feedback through usability studies will ultimately lead to a complete and final prototype application. At this point it would be important to begin performing tests with businesses that are prospective clients, to discover if they have ever experienced loss of data or a breach of any kind, what they did to mititgate the risk of that breach, if they are satisfied with their current training solution and if the proposed application would meet their needs.

Chapter 7

Appendix

7.1 Materials: Usability Study

7.1.1 Navigation

- Overall, how would you rate your experience navigating through the application? (Very Easy) 1 2 3 4 5 6 7 8 9 10 (Very Difficult)
- Overall, I was satisfied with the amount of time it took to complete the application. (Very Satisfied) 1 2 3 4 5 6 7 8 9 10 (Very Unsatisfied)
- When going through the Coffee Shop module, I found it easy or difficult to navigate to the end. (Very Easy) 1 2 3 4 5 6 7 8 9 10 (Very Difficult)
- Was navigation through the application intuitive? (Very Intuitive) 1 2 3 4 5 6 7 8 9 10 (Not at all Intuitive)
- Did you find the screen that let you view how to earn points? If so, how easy was it to get there? (Very Easy) 1 2 3 4 5 6 7 8 9 10 (Very Difficult/I did not find it)
- How often did you find yourself needing to navigate back a screen, but you were unable to do so. (Never) 1 2 3 4 5 6 7 8 9 10 (Very Often)
- Was it clear where the "Home Screen" was? (Very Clear) 1 2 3 4 5 6 7 8 9 10 (Very Unclear)
- Do you have any input on navigation that was not addressed by one of the questions above?

7.1.2 Functionality

- Overall, how would you rate the functionality of the application? (Very Good) 1 2 3 4 5 6 7 8 9 10 (Very Bad)
- How well did you understand the terms/verbiage used in the application? (Very Well) 1 2 3 4 5 6 7 8 9 10 (Not at All)
- How would you rate the consistency of the application? (Very Consistent) 1 2 3 4 5 6 7 8 9 10 (Not at all Consistent)
- When playing the Coffee Shop module, how clear was the distinction between error and success? (Very Clear) 1 2 3 4 5 6 7 8 9 10 (Not at all Clear)
- Overall, how satisfied were you with the support information provided by the application? (Help messages, documentation etc.) (Very Satisfied) 1 2 3 4 5 6 7 8 9 10 (Not at all Satisfied)
- Did you view the trophy case? If so, do you think you know what it is? (I know what it is) 1 2 3 4 5 6 7 8 9 10 (I don't know what it is/I couldn't locate it)
- Did you view every screen in the application? (I think so) 1 2 3 4 5 6 7 8 9 10 (I don't think so)
- Do you have a clear understanding of what the application is designed to do? (Very Clear) 1 2 3 4 5 6 7 8 9 10 (Not at all Clear)
- Do you have any input on functionality that was not addressed by one of the questions above?

7.1.3 Appearance

- Overall, how would you rate the appearance of the application? (Very Good) 1 2 3 4 5 6 7 8 9 10 (Very Bad)
- Did the appearance distract at all from the functionality of the application? (Not Distracting) 1 2 3 4 5 6 7 8 9 10 (Very Distracting)
- How did you feel about the color scheme? (I liked it) 1 2 3 4 5 6 7 8 9 10 (I hated it)
- How would you rate the layout of the application? (Very Good) 1 2 3 4 5 6 7 8 9 10 (Very Bad)

- Did you find the appearance of the application consistent? (Very Consistent) 1 2 3 4 5 6 7 8 9 10 (Not at all Consistent)
- Do you have any input on appearance that was not addressed by one of the questions above?

Bibliography

[Adams, 2015] Adams, N. E. (2015). Bloom's taxonomy of cognitive learning objectives. *Journal of the Medical Library Association*, 103(3):152.

[Caspersen et al., 2017] Caspersen, J., Smeby, J., and Aamodt, P. O. (2017). Measuring learning outcomes. *European Journal of Education*.

[De-Marcos et al., 2014] De-Marcos, L., Domnguez, A., de Navarrete, J. S., and Pags, C. (2014). An empirical study comparing gamification and social networking on e-learning. *Computers and Education*, 75:82–91.

[Desman, 2001] Desman, M. B. (2001). *Building an information security awareness program*. CRC Press.

[Eminaaolu et al., 2009] Eminaaolu, M., Uar, E., and aban Eren (2009). The positive outcomes of information security awareness training in companiesa case study. *information security technical report*, 14(4):223–229.

[Felker, 2014] Felker, K. (2014). Gamification in libraries: the state of the art. *Reference and User Services Quarterly*, 54(2):19.

[Furnell et al., 2002] Furnell, S., Gennatou, M., and Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5,6):352–357.

[Granger, 2001] Granger, S. (2001). Social engineering fundamentals, part i: hacker tactics. *Security Focus, December*, 18.

[Gutzwiller et al., 2015] Gutzwiller, R. S., Fugate, S., Sawyer, B. D., and Hancock, P. (2015). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 59, pages 322–326. SAGE Publications.

[Hill, 2012] Hill, D. C. (2012). Learning outcomes. *Professional safety*, 57(10):53.

[Hu et al., 2011] Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6):54–60.

[Institute, 2016] Institute, I. (2016). Gamification of security awareness campaigns.

[It, 2016] It, S. (2016). Five strategies to help companies strengthen information security and get back to business.

[Jones, 2010] Jones, A. (2010). How do you make information security user friendly?

[Kalinauskas, 2014] Kalinauskas, M. (2014). Gamification in fostering creativity. *Socialns Technologijos*, (01):62–75.

[Kim, 2015] Kim, B. (2015). . gamification. *Library Technology Reports*, 51(2):10–18.

[Kingsley and Grabner-Hagen, 2015] Kingsley, T. L. and Grabner-Hagen, M. M. (2015). Gamification. *Journal of Adolescent and Adult Literacy*, 59(1):51–61.

[Krebs, 2014] Krebs, B. (2014). Target hackers broke in via hvac company.

[LLC, 2015] LLC, P. I. (2015). 2015 cost of data breach study: Global analysis. Technical report, Ponemon Institute LLC.

[LLC, 2016] LLC, P. I. (2016). 2016 cost of data breach study: United states. Technical report, Ponemon Institute.

[Marvin, 2015] Marvin, R. (2015). How gamified brain science is transforming e-learning.

[Mitnick and Simon, 2011] Mitnick, K. D. and Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley and Sons.

[Peltier, 2005] Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, 14(2):37–49.

[Puhakainen and Siponen, 2010] Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, pages 757–778.

[Shapiro, 2008] Shapiro, A. M. (2008). Hypermedia design as learner scaffolding. *Educational technology research and development*, 56(1):29–44.

[Shaw et al., 2009] Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers and Education*, 52(1):92–100.

[Siponen, 2000] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1):31–41.

[Stewart, 2009] Stewart, G. (2009). A safety approach to information security communications. *information security technical report*, 14(4):197–201.

[Winkler and Manke, 2014] Winkler, I. and Manke, S. (2014). Rsa conference. In *Gamifying Security Awareness*.