



Gamifying Security Awareness: A New Prototype

John Russell Cole^(✉), Toni Pence^(✉), Jeffrey Cummings^(✉),
and Elizabeth Baker^(✉)

Univeristy of North Carolina at Wilmington, Wilmington, NC 28403, USA
jrc9569@gmail.com, {pencet, cummingsj, bakere}@uncw.edu

Abstract. Data breaches within an organization have many causes. Social engineering attacks, ransom-ware 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 mitigate. 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. Training and awareness programs are too often treated as a bandage to fix a wound inflicted by a breach after the fact. If employees were trained effectively, the breach might not have occurred in the first place. This project and accompanying research paper will explore the gamification of the security training and awareness program. 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 can be possible to reinvent security awareness and prevent future data breaches.

Keywords: Virtual environment · Gamification · Security awareness

1 Introduction

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 [6]. 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

Supported by University of North Carolina at Wilmington.

© Springer Nature Switzerland AG 2019
A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 115–133, 2019.
https://doi.org/10.1007/978-3-030-22351-9_8

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 [6]. 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 [4].

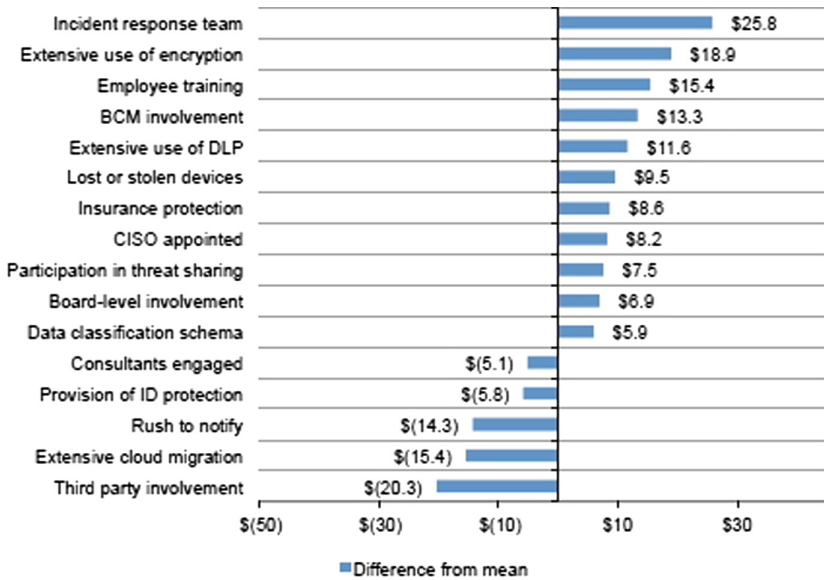


Fig. 1. Employee Training reduced the average cost per record by \$15.4. 2016 Cost of Data Breach Study: United States. Ponemon Institute

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 [7]. 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 Fig. 1 [7].

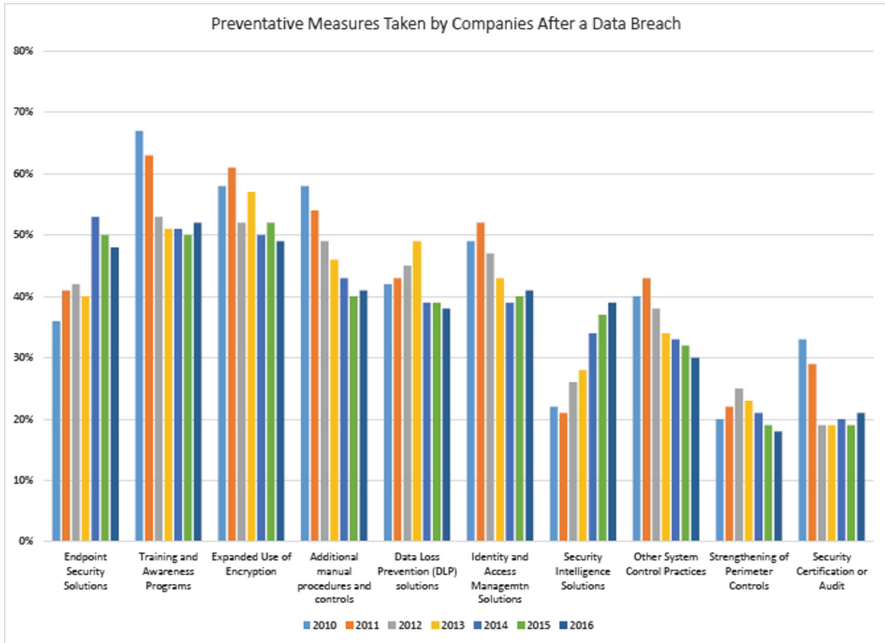


Fig. 2. Employee Training programs implemented after breach decreased by 15%. 2016 Cost of Data Breach Study: United States. Ponemon Institute

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 Fig. 2 [7].

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 [5]. 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 Background and Motivation

2.1 Information Security Education, Training and Awareness

Building an effective security awareness program requires inclusion of education and training [10]. 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.”

Shaw et al. 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 plain text 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 [9]. 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.

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” [2]. 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).

2.2 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 [11]. 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.

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” [8]. 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 [3].

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 [1]. 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” [1].

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” [1].

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

My solution to this issue 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 an 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 is to complete the game module and earn points. Points serve multiple purposes throughout the program. They can be redeemed for real-world rewards and incentives. Your rank on the leaderboard is determined by

how many points you have earned. Points help identify your status of mastery within the application. The more points you have, the more opportunities you will have to earn points in the future. See Fig. 3 for an example of this.

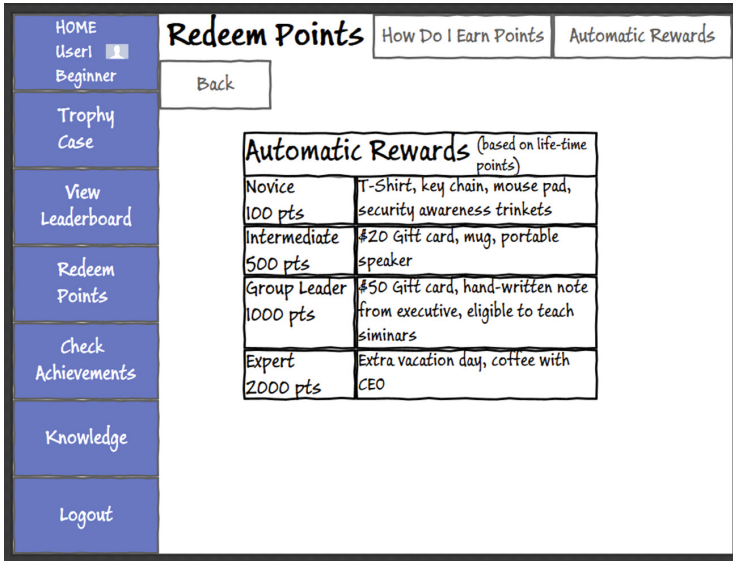


Fig. 3. Example structure of automatic rewards an employee might earn and their corresponding point value

Points can also be earned in other ways. In an effort to make other real-world moments teachable, employees will be subjected to test social engineering and phishing attempts. If they detect the attempt and report it, they are rewarded with points. If they are unable to detect it and the test attack is successful, they experience a teachable moment and their behavior is corrected. There are other ways that employees will be able to earn points as well. See Fig. 4 for more details. 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, has a plan for ongoing training throughout the year and is adaptive to needs of individual organizations can be the solution to the problem presented above.

Scenario-Based Training Modules. It is important to design the gamified modules around scenarios that the employee will likely encounter in an actual

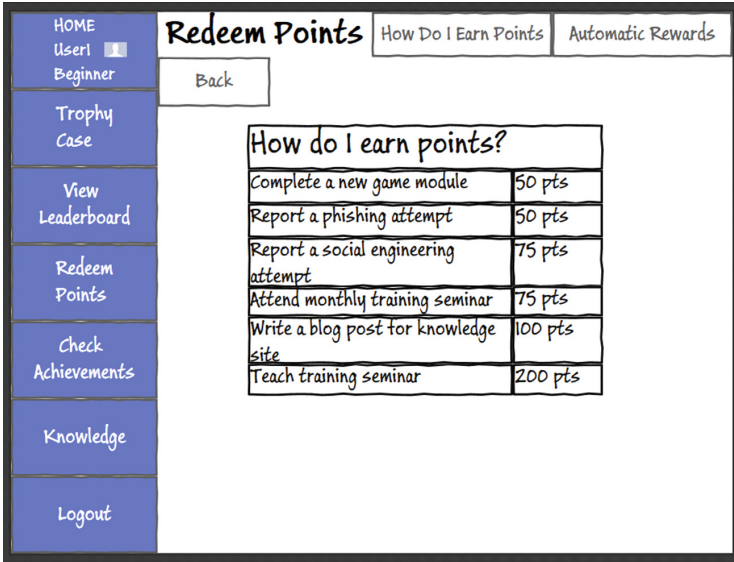


Fig. 4. Example structure of point payout

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 could 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.

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



Fig. 5. Example of an employees view of their progress towards a given set of achievements.

would be an effective way to gauge the culture of the employees and would help determine an appropriate reward structure.

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. See Fig. 5.

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 insure that every policy is understood and not obfuscated. Having the knowledge repository structured 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 can 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. See Fig. 6 for details.

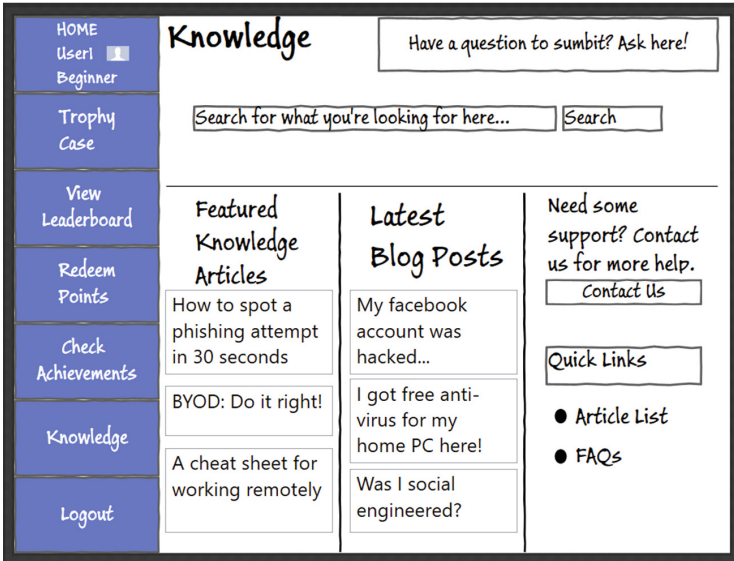


Fig. 6. Example of the knowledge landing page. See sections dedicated to featured knowledge articles and latest user-submitted blog posts

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. See Fig. 7. The trophy case will show a quick glance at the leaderboard and display each user’s most recently posted status update.

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. See Fig. 8.

4 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




		Point Total	Modules Completed	Achievements Earned	Weeks in Top 3
Bill Smith Support Admin		475	18	7	6
Jim Daniels Accountant		415	15	5	2
Phil Toms Auditor		295	11	4	2
Jess Stacy Analyst		265	5	2	1
Julie Lars Legal		255	4	3	0
Mike Marks Trainer		240	4	1	0

Fig. 7. Example of the leaderboard. Each employee can find themselves on the board ranked by point totals and see how they measure up to other employees in the organization

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.

4.1 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.

4.2 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.

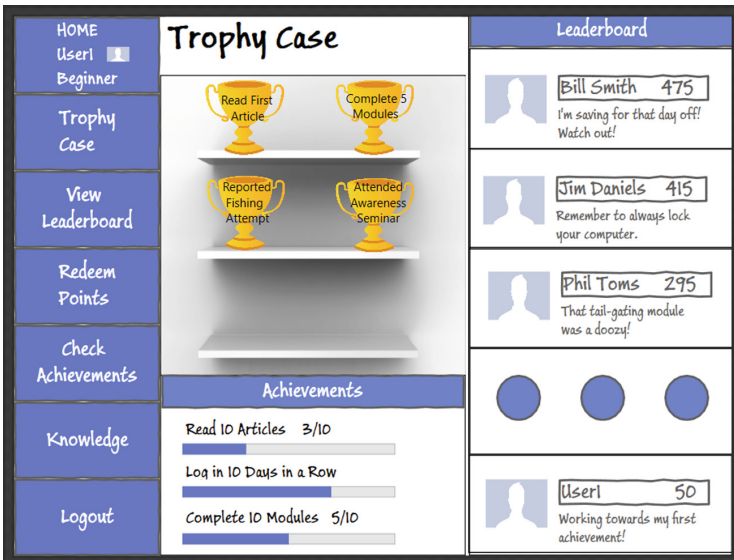


Fig. 8. Example of the Trophy Case. It will allow the user to see quick glances of the leaderboard, achievements they are currently working toward and a case of trophies they have earned.

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.

4.3 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.

5 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.

5.1 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 Fig. 9. Adding assets, creating states (used for simulating animation), changing opacity of objects

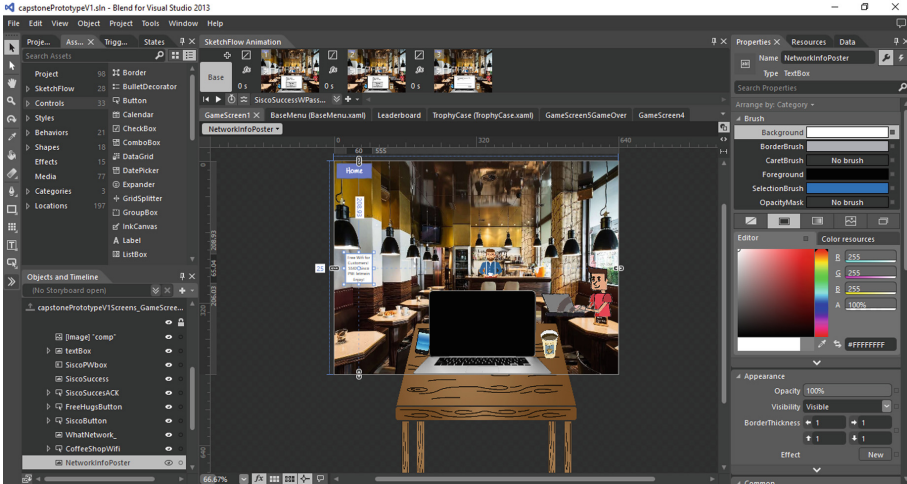


Fig. 9. A quick glance at the sketchflow user interface.

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 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 Fig. 10.

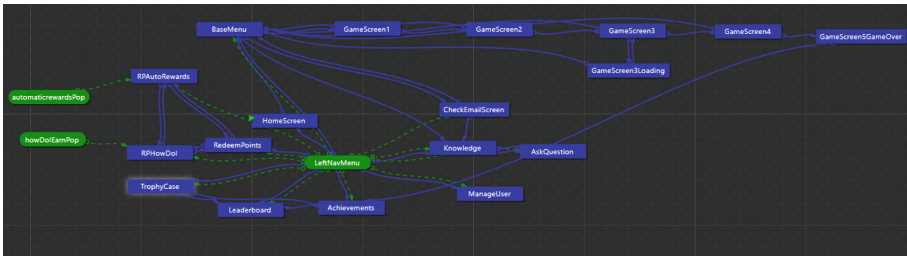


Fig. 10. Map of prototype screens. This layout helped map out the application.

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.

5.2 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 Fig. 11 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 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 Fig. 12 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.

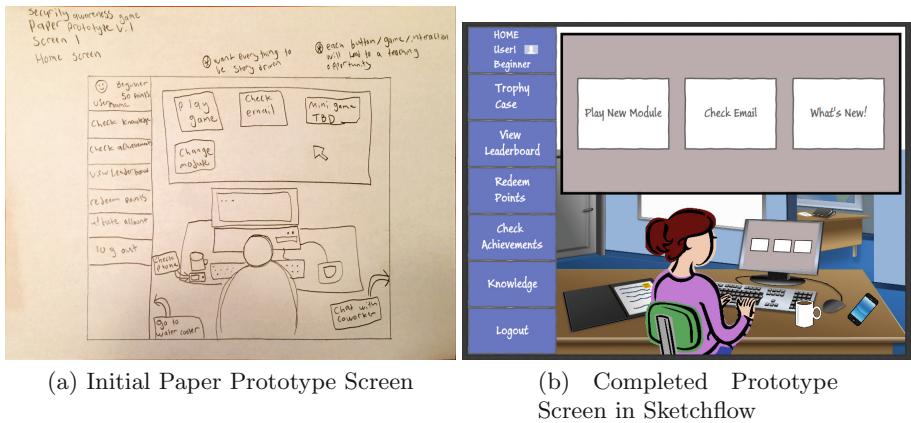


Fig. 11. The base menu prototype screen. Side by side comparison of initial paper prototype screen and completed prototype screen

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,

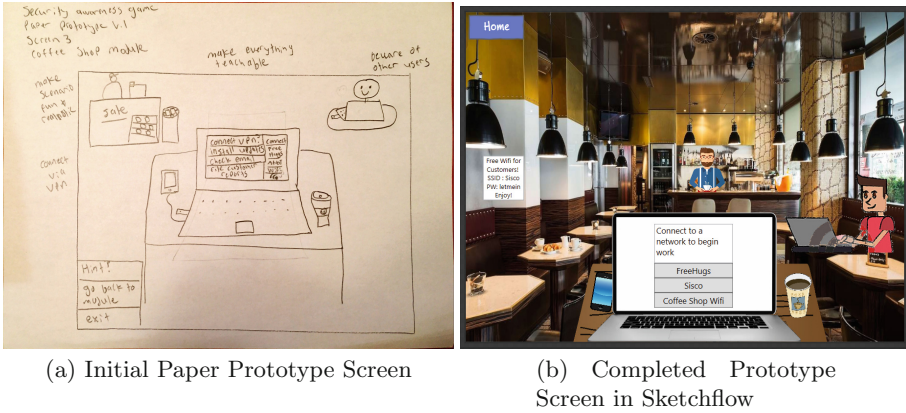


Fig. 12. The coffee shop module prototype screen. Side by side comparison of initial paper prototype screen and completed prototype screen

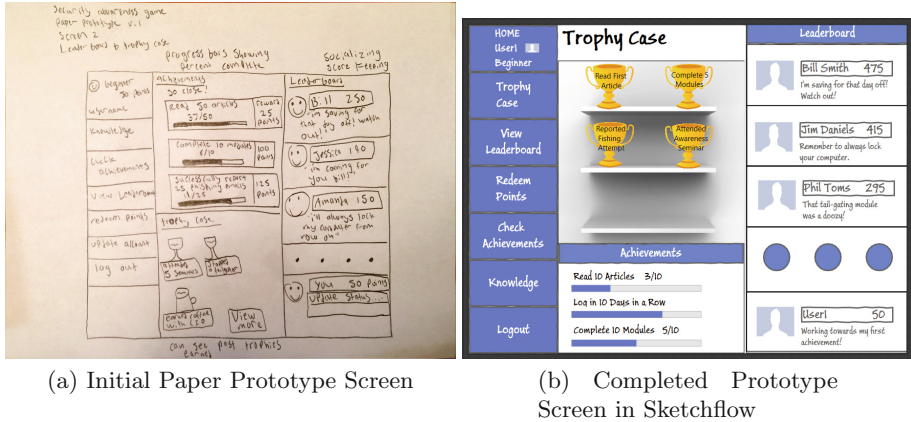
but that the original screen I designed on paper still would have a place in the application. It became the Trophy Case screen that gave quick glances at some of the most important information from both the leaderboard screen and the achievements screens, as well as displaying the trophies that the user has earned while using the application. See Fig. 13 for a side-by-side comparison of my initial paper prototype screen of the leaderboard and a completed Sketchflow screen for the Trophy Case.

6 Results

6.1 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.

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



(a) Initial Paper Prototype Screen

(b) Completed Prototype Screen in Sketchflow

Fig. 13. 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

2.65 where 1 represented “very easy” and 10 was “very difficult”. 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 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.

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. 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 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.

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.

7 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.

References

1. Gutzwiller, R.S., Fugate, S., Sawyer, B.D., Hancock, P.: The human factors of cyber network defense. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 59, pp. 322–326. SAGE Publications, Los Angeles (2015)
2. Hu, Q., Xu, Z., Dinev, T., Ling, H.: Does deterrence work in reducing information security policy abuse by employees? *Commun. ACM* **54**(6), 54–60 (2011)
3. Institute IT: Gamification of security awareness campaigns, 13 May 2016
4. Shred-it: Five strategies to help companies strengthen information security and get back to business, 16 Aug 2016
5. Jones, A.: How do you make information security user friendly? (2010)
6. LLC PI: 2015 cost of data breach study: Global analysis. Technical report, Ponemon Institute LLC (2015)

7. LLC PI: 2016 cost of data breach study: United states. Technical report, Ponemon Institute (2016)
8. Marvin, R.: How gamified brain science is transforming e-learning, 30 November 2015
9. Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.J.: The impact of information richness on information security awareness training effectiveness. *Comput. Educ.* **52**(1), 92–100 (2009)
10. Siponen, M.T.: A conceptual foundation for organizational information security awareness. *Inf. Manage. Comput. Secur.* **8**(1), 31–41 (2000)
11. Winkler, I., Manke, S.: RSA conference. In: *Gamifying Security Awareness*, 24 February 2014