Evaluating Prevalence, Perceptions, and Effectiveness of Cyber Security and Privacy Education, Training, and Awareness Programs

Marc J. Dupuis
marcjd@uw.edu

Collin Gordon
colntrev@gmail.com

University of Washington
Box 358534
Bothell, WA 98011-8246

Abstract - Cyber security and privacy issues continue to mount, particularly for non-experts. Many different attempts have been made to address the lack of knowledge, skills, and abilities in this arena. This has largely been the catalyst for several different types of cyber security and privacy education, training, and awareness programs. We discuss these various programs, followed by a discussion on a large-scale survey that was conducted to learn more about the perceived effectiveness of these programs and how enjoyable they were to participants. We also compare the type of programs one has engaged in with their score on a cyber security and privacy knowledge quiz. Most of the programs examined in the survey did show a correlation with the results obtained on the knowledge quiz. A discussion with some recommendations follows.

Keywords

cyber security, privacy, education, training, awareness, knowledge quiz

1. INTRODUCTION

Cybersecurity issues are at the forefront of the modern world. The question of how to protect oneself online at home and in the office has come up frequently due to large scale leaks of sensitive information [1]–[5]. Training for expert users – users with official cybersecurity training and a wealth of experience with computing – has been established for some time. However, non-expert users – users with basic computer knowledge and non-technical jobs – continue to be the primary focus of cybersecurity related attacks. Training and outreach to non-expert users has proven to be a more complicated task than training expert users.

The difficulty faced in this area centers around the wide array of technological competency found in non-expert users. Additionally, non-expert users, unlike their expert counterparts, do not have the same understanding of the scope of their actions online. This can result in an ambivalence with regard to using proper security measures. Both academic and corporate institutions have conducted several experiments on how to improve the dissemination of security knowledge to non-expert users due to the increasing risk of breaches secondary to a lack of security knowledge.

This paper discusses several different types of cybersecurity and privacy education, training, and awareness programs. Next, we discuss the results of a large-scale survey that sought to learn more about the perceived effectiveness of these programs and how enjoyable they were to participants. We also compare the type of programs one has engaged in with their score on a cybersecurity and privacy knowledge quiz. A discussion follows.

2. LITERATURE REVIEW

There are several methods that are in place to help both expert and non-expert users learn aspects of cybersecurity. These methods can be split up into two categories: active and passive. Active methods encourage better security practices by training individuals and groups through classroom, virtual, or gamified environments. In contrast, passive

methods aim to reduce the security risk of non-expert users by abstracting vulnerabilities through automation or other means. Both types of methods will be covered in the following sections.

2.1 Active Methods

2.1.1 Classrooms

Classrooms are often the first choice among users and organizations for formal training on a variety of subjects. While classrooms have benefits such as certifiable knowledge covered by standards [6]–[8], they do not provide adequate hands-on practice of the knowledge learned[9]. Such hands-on practice is critical due to the complex nature of some attacks and their mitigations. Lack of hands-on training increases the learning curve for users who are easily confused by or new to technology whom benefit from guided practice and tutorials.

Additionally, the standards taught and certifications earned in classrooms can become quickly outdated. This issue was exemplified in [10] when some aspects of a popular software design standard were shown to be either too vague to be practical or simply insignificant in reducing software design errors.

Another drawback is that the education may not be focused on the specific needs of the users. Studies done in [11], [12] prove that knowledge of cybersecurity differs among non-expert users based on their age and their specific interactions with technology. In [11] the concerns of the non-expert users were personal and involved issues ranging from fraudulent emails to exposure of credit card information. Most of these concerns did not consider the larger scope of consequences that an attack on their network activity might have[12].

Lack of hands-on learning tools is not present in other areas of computer science. Areas such as writing code possess environments where mistakes can be made that can easily been undone. However, if non-expert users wish to practice security knowledge gained in a classroom or even have a hands on approach to learning, they have to practice on real websites or do things that they might believe are illegal[13]. In

response, several environments have been created where websites are left broken on purpose or a sandbox lab is set up[14], [15].

2.1.2 Sandbox Labs and Websites

Sandbox labs and websites such as [15] are potentially viable to educate non-expert users. These environments help users by allowing them to experience and observe the potential for danger that can be brought on by seemingly simple means such as choosing a bad password or uploading an image from an unchecked source[15]. The problem with training tools such as [10] is that they are often set up for expert users to both practice legal exploitation and learn about safe application design. As a result, non-expert users may find themselves wading through technical jargon that is not necessary for their understanding of what is happening.

Sandbox labs are an ideal option for training non-expert users in hands-on security awareness. In such labs, actual hardware is present that can contain real applications. Scenarios can then be implemented based on the level of the trainee and the goal of the training. Being able to visualize and manage the software in real time can be vital towards applying knowledge gained in a classroom environment or by other means.

However, sandbox labs have several drawbacks. The first is the cost of setting up a lab[14]. Depending on the scenarios that companies and academic institutions want to train their users on, the hardware and technical expertise required to set up the lab can be very expensive [14].

Another factor to consider when setting up a sandbox lab is how to secure it in such a way that outside users cannot break into the institution through the machinery inside the lab. This complication often leads labs to be lacking in the types of exercises and scenarios they can perform. Thus, limiting the scope with which users can learn security concepts.

2.1.3 Virtual Workspaces

Much of the current academic and corporate literature in other aspects of computer science has begun to focus on using virtual environments as

platforms for hosting businesses, sample applications, and computing clusters [13], [14], [16]–[18]. Virtual environments solve many of the problems surrounding physical sandbox labs. For instance, cloud based virtual machines such as [16] offer the ability to have a space with a fully functional desktop computer that can be set up remotely and cloned several times through imaging.

Imaging is a unique tool that can allow for several machines of the same type to be connected into a cluster or network with the ability to spawn new machines at their factory default with ease [16]. As shown in scenarios such as [17], the costs that would be incurred in the implementation of a physical lab are reduced to paying for the space on the cloud server.

The benefit of these environments for education are plentiful. When it comes to training advanced non-expert users machines can be spawned with vulnerabilities that can be exploited and at the end of the exercise all that is required is a reboot of the image to its original setting. Additionally, platforms such as [16], [18] interface with a wide variety of frameworks and operating systems allowing teams of users in different environments to be able to train with little effort in the way of set up.

Virtual environments do have one major drawback: They lack the real feel of a physical lab. Virtual environments focus solely on virtual attacks leaving trainees uneducated in other forms of cybersecurity risks such as telemarketer frauds or writing passwords in a visible location.

2.1.4 Gamification

Gamification is the practice of using techniques from video games to create tools for alternative learning. These techniques have been praised in various industries due to their ability to be immersive and addictive as well as safe sandboxes for the application of knowledge [9]. Gamification is an interesting subject in terms of training non-expert users in that it can teach a wide array of concepts through accessible media.

One type of gamification, role playing, could be an effective training tool [19]. The advantage of role playing is that it encourages the individual to

embrace a character. Characters can range in personality from very like the individual to very different. This personality is shaped through a range of choices given to the player. The level of interaction required in role playing games encourages the individual to explore the world in a more engaged, realistic way.

In [19] a study was conducted on the effectiveness of the video game Second Life as an educational tool for cybersecurity. The study took place on an island that was accessible to players. Upon arrival players were presented with bits of dialogue about common security threats. As the players explored the island they became afflicted with different ailments representative of different security threats. Users were educated through curing their characters of the ailments by engaging in simulations of common cybersecurity mitigation strategies[19]. This solution proved effective in not only engaging visitors who wished to learn about cybersecurity, but also the students who created the simulation.

An example of gamification comes from the military. The military has had a long history of attempting to gamify their security training [9]. Some, such as CyberProtect, tested appropriate topics while others lacked the reality or topic coverage to effectively train personnel [9]. As a result, a team of researchers attempted to create a new, efficient game. What they came up with was CyberCIEGE. CyberCIEGE solves many problems that early attempts at security gamification failed to address [9].

CyberCIEGE provides security instructors with the ability to change features and depth of knowledge covered. This customizability allows instructors to engage a wide audience with a single tool. Furthermore, CyberCIEIGE provides users with a simulation that is more engaging and challenging than a regular classroom environment[9].

Researchers in [9] conducted an experiment on the flexibility and effectiveness of scenarios inside CyberCIEGE. This was done using two scenario types: Basic and advanced. The basic scenario was focused on teaching computer security fundamentals to personnel with limited technology experience. The scenario involved users being placed in the

role of a decision maker aboard a ship[9]. Users would have to make choices and complete objectives that raised the overall security level of the ship's systems[9]. The second scenario placed users in the role of a security manager. The user was required to make decisions covering physical security, mechanisms, access control, antivirus, and other network vulnerabilities spread across three internal networks[9].

These scenarios not only provided different decisions, they also had different consequences for choices made by the users[9]. In the basic scenario, researchers gave the user feedback and resources linking the choices they made for each objective to real life scenarios. Players did not incur severe penalties for wrong choices, but were simply educated on the gravity of the choices made[9]. In contrast, the advanced scenario gave fatal errors and technical evaluations of each choice made increasing the consequences of poor decision making[9].

Like virtual lab environments, video games can lack the realism of a classroom and thus reduce the effectiveness of the lessons learned. Hackathons can fill this gap. A hackathon is a competitive challenge where groups of people try to solve a problem with a limitation such as time or technology.

Hackathons are unique among training and awareness options covered thus far because they can be used to both test the effectiveness of existing methods and measure the success of experimental methods. One notable hackathon is Cyber Storm[20].

Cyber Storm is a biennial hackathon designed by the Department of Defense to test and strengthen the preparedness of both public and private organizations[20]. After each Cyber Storm, an action report is generated that details the current capabilities of various organizations to handle attacks, the quality of information communicated amongst different organizations, and the processes used to share sensitive information across different sectors without compromising private and governmental interests[20].

The purpose of these measurements is to pinpoint issues, train skills such as strategic decision making, and improve coordination of

responses between different organizations[20]. These measurements are obtained through the execution of exercises.

The exercise presented in [20] involved multiple adversaries that distributed complex malware resulting in crippling effects throughout critical infrastructure[20]. To effectively beat the scenario, teams had to work together to share cybersecurity knowledge and implement the best practices available.

As Cyber Storm has published meaningful data in its action reports, more organizations have joined in the exercise. As of [20] several organizations including law enforcement, state governments, and commercial retails have participated in at least one Cyber Storm event.

2.2 Passive Methods

2.2.1 Situational Awareness

Situational awareness is a security practice that relies on automation to monitor the state of the network and the communications taking place[21]. While situational awareness creates a secure environment through automation it still has a training component.

Situational awareness attempts to model complex decision making behavior in a program and give the program the ability to adapt to new situations based off its previous training[21]. This practice helps non-expert users focus more on the details of their work and less on aspects of security that may complicate their job. While this may seem like an easy alternative to training non-expert users in classrooms or with games and hackathons, one issue stands in the way: Trust [11], [21], [22].

What has been found in various studies is that the non-expert professionals that work with situationally aware systems do not trust the machines to do their jobs [11], [21], [22]. Therefore, effort has been spent training non-expert users in the way that the systems work. Training consists of higher level details of the system's inner workings as well as demonstrations of functionality in simulations and live test runs.

What makes this field interesting in the context of promoting cybersecurity training and awareness is that it focuses on building trust in the technology through explaining how it works. This presents an argument for a security training method that incorporates the same level of trust through demonstration of how the security measures being taught make non-experts more secure in their internet usage.

2.2.2 Passwords

Passwords have long been the subject of scrutiny in the cybersecurity community. They are a cornerstone for frustration from non-expert users. The difficulty that users experience with passwords is that properly secure password sequences are difficult to remember. A body of research has begun to be collected on ways to elicit better memory of passwords by non-expert users.

The primary alternative method used on non-expert users is a form of graphical password. Graphical passwords focus on triggering the primitive associations between color and images, such as the picture superiority effect (PSE), to promote better memory[23].

One such image based method is based on the recollection of images. In this method, users are asked to pick a combination of images from a palette with no restriction. When entering the password, users can choose the images they chose in any order if the images match the original selections. The benefit of this method is that it draws heavily upon the aforementioned PSE and other cognitive stimulants that effect multiple areas of the brain strengthening the memory[23].

Another method of graphical password implementation involves the recollection of images in a specific order. In [23] this method was employed when users are asked to either draw an image or pick images in a precise pattern and then replicate the drawing or pattern to log in.

Studies such as [23] show that this method is less effective due to a high number of errors. However, [23] revealed an intriguing source of these errors. Users that were required to pick a story picked the wrong images with a fifty percent of the time. Additionally, seventy five percent of the

incorrect passwords entered by users using this method consisted of the correct images in the wrong order[23].

This represents a possible reason behind common password error. The reason being that there is a difference between simply recalling information and reproducing it exactly.

Common password methods often engage the user in reproduction of their passphrase with very little provided in the way of context to help engage their ability to recall what they chose.

In contrast, graphical password methods provide a different avenue where context is provided with visual configuration and a user's memorization is encouraged by calling upon associations that assign a significance of the image users choose in regards to a memory from the user's past [24]. The effectiveness of image based passwords can be demonstrated in one study's 85% success rate on first time log ins when employing a method that requires simple recall of images[24].

3. METHODS

The preceding section discussed several different types of cybersecurity education, training, and awareness approaches. However, there is little information available on the effectiveness of various programs or whether individuals engaging in such programs enjoy them.

In this paper, we address this shortcoming in part by conducting a large-scale survey of individuals to assess the types of training they have had, perceptions of their effectiveness, and how much they enjoyed it. After IRB approval was obtained, Amazon's Mechanical Turk was used to recruit participants, which has been shown to be an effective and efficient method of participation recruitment [25]. They were compensated with $0.71 through the platform.

Participants were asked whether they had participated in the various types of education, training, and awareness programs noted in the preceding section (no, not sure, yes), if they thought it was effective (5-

point Likert), and how much they enjoyed that modality (5-point Likert). Analysis was performed using SPSS, version 19.

Additionally, participants completed questions to assess their level of cybersecurity and privacy knowledge. We used a recent quiz developed by the Pew Research Center to determine if various types of education, training, or awareness programs were correlated with higher levels of cybersecurity and privacy knowledge [26]. While there may no doubt be several confounding variables at play with respect to how well they did on the quiz, we felt it would be interesting to see what differences, if any, exist.

4. RESULTS

As noted previously, Amazon's Mechanical Turk was used to recruit participants. We received 1,011 valid survey responses once those that failed a quality control question were removed from further analysis. Approximately 11.4% of participants failed the quality control question. Table 1 provides information on the composition of the participants.

Table 1. Participant Composition

Gender	**Percentage**
Male	45.8%
Female	53.8%
Age	
18-29	29.7%
30-39	36.1%
40-49	19.3%
50-59	10.5%
60+	4.5%

Education	
Less than high school	0.2%
High school (or GED)	8.2%
Some college	23.2%
Associate's degree	12.4%
Bachelor's degree	39.7%
Master's degree	13.1%
Professional degree	1.8%
Doctorate degree	1.5%

The composition of our participants is consistent with other research that shows Amazon Mechanical Turk workers to generally be younger and more highly educated than the population at large in the United States [27].

We also wanted to learn about the different types of cybersecurity and privacy education, training, and awareness programs they have participated in. Seven different types were identified based on the earlier discussion: 1) Classroom training; 2) Hands-on labs; 3) Virtual labs; 4) Role playing; 5) Hackathons; 6) Situational awareness, and 7) Computer-based training (CBT). Table 2 provides a breakdown of the level of participation in these various types of programs.

Table 2. Security Education, Training, and Awareness Program Participation

Type	**Yes**	**Not Sure**	**No**
Classroom training	36.8%	3.6%	59.6%
Hands-on labs	16.1%	4.7%	79.2%

Virtual labs	19.7%	4.7%	75.6%
Role playing	14.7%	4.0%	81.4%
Hackathons	3.4%	2.5%	94.2%
Situational awareness	22.2%	5.5%	72.3%
Computer-based training (CBT)	49.7%	4.6%	45.8%

Table 2 indicates that computer-based training is the most prevalent type of education, training, and awareness program that participants have engaged in, followed by classroom training and situational awareness. Very few participants have been involved in a hackathon as part of an overall program.

Beyond the prevalence of the various types of programs that participants have been involved in are their perceived effectiveness and enjoyability. This analysis was limited to participants that identified that they had engaged in that specific type of program. A 5-point Likert scale was used with a low of 1 and a high of 5 employed. Table 3 presents the results of this analysis.

Table 3. Participant Satisfaction and Perceived Effectiveness of Programs

Type	**Effectiveness** *Mean (SD)*	**Enjoyable** *Mean (SD)*
Classroom training	3.52 (0.933)	3.28 (1.076)
Hands-on labs	4.12 (0.884)	3.91 (0.980)
Virtual labs	3.74 (1.007)	3.57 (1.095)
Role playing	3.40 (1.079)	3.45 (1.149)
Hackathons	3.72 (1.170)	3.91 (0.995)

Situational awareness	3.74 (0.910)	3.46 (1.086)
Computer-based training (CBT)	3.60 (0.930)	3.28 (1.079)

The results suggest that participants thought hands-on labs were the most effective, followed by virtual labs and situational awareness. Role playing, classroom training, and computer-based training received the lowest scores with respect to perceived effectiveness.

The level of enjoyableness was largely consistent with these results. Participants found hands-on labs and hackathons to be the most enjoyable, followed by virtual labs. In contrast, participants did not think computer-based training and classroom training were as enjoyable, followed by role playing.

Finally, we examine whether the type of training, education, and awareness program employed and the total number of types experienced are related to a score on a cybersecurity and privacy knowledge quiz. Table 4 presents the result of this analysis.

Table 4. Security and Privacy Knowledge Quiz Results and Modality Employed

Type	**Pearson Correlation**	**Significance Level**
Classroom training	0.132	< 0.0001
Hands-on labs	0.115	< 0.0001
Virtual labs	0.122	< 0.0001
Role playing	0.066	< 0.05
Hackathons	0.044	N.S.
Situational awareness	0.115	< 0.0001

Computer-based training (CBT)	0.151	< 0.0001
Total number of types employed	0.169	< 0.0001

The results in table 4 suggest that having education, training, and/or awareness in cybersecurity and privacy does help people become more knowledgeable. The only type that did not see significant support for this was hackathons. This could be for a variety of reasons, including that only 3.4% of participants indicated they had participated in this type of activity, which was the lowest number of any type surveyed. Thus, it is possible that there was not enough power in the sample size to detect this relationship.

5. DISCUSSION

The results from the survey suggest that engaging in cybersecurity and privacy education, training, and awareness programs are associated with higher levels of knowledge in this area. However, caution should be exercises in inferring too much. It is possible that those that have engaged in these types of programs already had higher levels of knowledge.

It is worth noting that two of the types with the highest Pearson correlation values (classroom training and computer-based training) scored the lowest in effectiveness and enjoyability from the participants. The implications of this area unclear, but it does suggest that despite individuals not liking these types of programs, they are nonetheless effective.

Finally, we assessed cybersecurity and privacy knowledge. Knowledge does little in this space if it is not put into practice. Thus, measuring knowledge rather than practice in inherently flawed. Nonetheless, since knowledge is a prerequisite for practice, it is encouraging.

Based on the earlier discussion on the types of programs available and the results from the survey, we make some suggestions for organizations

looking to improve the cybersecurity and privacy practices of their employees.

Ultimately, facilitating the highest level of cybersecurity practice is achieved through a combination of the previously mentioned methods that are often employed in organizations. The following section details a plan for covering this information.

5.1 Establishing Trust

The studies on situational awareness reveal a primary issue in cybersecurity awareness: Trust [11], [21], [22]. Establishing trust between the security engineers, managers, and other personnel so that the infrastructure will be aware enough to stop and even learn from attacks is an important process. Through such a process, members of the team become aware of the infrastructure and its moving parts. In other words, they know not only that the machine will work, but why it works.

The results of story-based passwords where users were able to pick their images, but not in the right order, are analogous to the struggle faced in situational awareness [23]. Users were aware that they had to pick passwords in a story order, but did not because there was no explanation or visualization of why choosing a password in story order was more effective than selecting images at random. Additionally, in another study users did not choose color because they could not comprehend how increasing number of bits in the password space made the password more secure [28].

These examples demonstrate that the primary component of any cybersecurity and privacy program should be establishing trust through explaining why something is important in a context that directly relates to the user.

5.2 Training Courses and Exercises

Another key component of any training program is education and practice. As mentioned previously, the exact way to train a user in the concepts they need to know is unclear. However, the situation that makes the most sense is a blend of classroom learning and gamification.

This approach to training is used by organizations such as the Red Cross for CPR training [29].

The Red Cross refers to their training program as blended learning [29]. In blended learning, students are presented facts and rules through instructional videos and are then asked to role play what they learned in various games. The games are highly accurate scenarios guided by a narrator that helps correct mistakes and explain both good and bad choices.

In a similar vein, cybersecurity training can begin online in an environment where users can learn at their own pace and progress through skills. Scenarios could be built displaying the results of good choices and bad, providing learners with an explanation of why secure choices are the best to make, even if they appear inconvenient.

In the Red Cross training, an in-person session is conducted once the online portion is done [29]. This session serves to reinforce the basic concepts of what was covered online as well as provide additional scenarios that were difficult to communicate in the online format. Topics covered in person include an overview of the equipment, practice with the equipment, and practice with parts that were abstracted from the online scenario such as obtaining consent to perform first aid and positioning around the person in trouble. Additionally, in person sessions allow for group discussion around concerns such as performing CPR in a remote area, in a team, or without properly functioning equipment. These sessions are typically two hours in length [29].

Such a session could prove practical for cybersecurity training as well. In an in-person security training session, users would be asked to demonstrate proficiency in topics that were covered online in a physical or virtual lab space. This lab space could be set up to simulate a real work environment complete with security awareness signs and bulletins. Additionally, an instructor in the lab space could provide context and additional information about certain cybersecurity and privacy risks.

5.3 Practice and Retraining

Practice and retraining are an essential part of this method. While practicing and retraining skills may seem like a hindrance, it is a good practice.

Having non-experts retrain in their knowledge over a period would mean that updated cybersecurity information would be distributed to the masses. Breakthroughs in research (e.g., [23]) would be disseminated in a similar format to the original training.

The difference in the retraining phase would be that retraining would be done in one in-person session. This is because most of the new cybersecurity discoveries are built on top of the existing body of knowledge. Therefore, the basic training covered in an online session is not required.

The structure for the in-person retraining session would be spread over four hours. The first hour would be a review of basic concepts. The idea behind reviewing basic concepts is to make sure that non-expert users are one hundred percent refreshed on the content previously covered. Only an hour needs to be allocated to this activity due to the frequency in which non-expert users are confronted with basic cybersecurity and privacy knowledge.

The next two hours of retraining would consist of educating users on updated security information. Such subjects would include new formats for passwords, coverage of important security breaches, and other new precautions to be taken.

The last hour would be dedicated to skills demonstration. This would serve to solidify and display the importance of knowledge gained in the education portion. Any questions and mistakes would be addressed and corrected.

6. CONCLUSION

The proposed method brings together both active and passive methods of cybersecurity and privacy education, training, and awareness. While the method is not perfect, it represents the evolution of learning

techniques. With the ability of users to access resources in a variety of ways on a variety of mediums, the experimentation is virtually endless. A short coming of this method is the lack of an implementation or experimentation, both of which represent opportunities for further research. Additionally, the world of cybersecurity and privacy is rapidly evolving and changing, which makes the proposed method and the variety of other methods covered in this paper subject to change.

7. REFERENCES

[1] M. Dupuis, "'Wait, Do I Know You?': A Look at Personality and Preventing One's Personal Information from being Compromised," in *Proceedings of the 5th Annual Conference on Research in Information Technology*, Boston, MA, USA, 2016, pp. 55–55.

[2] M. Dupuis and S. Khadeer, "Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat," in *Proceedings of the 5th Annual Conference on Research in Information Technology*, Boston, MA, USA, 2016, pp. 35–40.

[3] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information," presented at the The Dewald Roode Information Security Workshop, Provo, Utah, 2012.

[4] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "Measuring the Human Factor in Information Security and Privacy," in *The 49th Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii, 2016.

[5] M. Khadeer, M. Dupuis, and S. Khadeer, "Educating Consumers on the Security and Privacy of Internet of Things (IoT) Devices," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 5, no. 2, Mar. 2018.

[6] R. Lepofsky, "Payment Card Industry (PCI) Data Security Standard Template for Report on Compliance for use with PCI DSS v3. 0," in *The Manager's Guide to Web Application Security:*, Springer, 2014, pp. 179–196.

[7] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public," *IEEE Secur. Priv.*, vol. 10, no. 3, pp. 76–79, May 2012.

[8] J. Fulda, "Interactive Non-Expert Information Visualizations and their Evaluation Beyond Time and Error."

[9] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A Video Game for Cyber Security Training and Awareness," *Comput. Secur.*, vol. 26, pp. 63–72, 2007.

[10] H.-W. Jung, S.-G. Kim, and C.-S. Chung, "Measuring software product quality: a survey of ISO/IEC 9126," *IEEE Softw.*, vol. 21, no. 5, pp. 88–92, Sep. 2004.

[11] P. A. Legg, "Enhancing cyber situation awareness for Non-Expert Users using visual analytics," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 2016, pp. 1–8.

[12] Z. Yunos, R. S. A. Hamid, and M. Ahmad, "Development of a cyber security awareness strategy using focus group discussion," in *2016 SAI Computing Conference (SAI)*, 2016, pp. 1063–1067.

[13] D. Manson and R. Pike, "The case for depth in cybersecurity education," *ACM Inroads*, vol. 5, no. 1, pp. 47–52, 2014.

[14] K. E. Stewart, J. W. Humphries, and T. R. Andel, "Developing a virtualization platform for courses in networking, systems administration and cyber security education," in *Proceedings of the 2009 spring simulation multiconference*, 2009, p. 65.

[15] "Web Application Exploits and Defenses." [Online]. Available: https://google-gruyere.appspot.com/. [Accessed: 29-Apr-2017].

[16] "Elastic Compute Cloud (EC2) – Cloud Server & Hosting – AWS," *Amazon Web Services, Inc.* [Online]. Available: //aws.amazon.com/ec2/. [Accessed: 01-May-2017].

[17] "High Scalability -." [Online]. Available: http://highscalability.com/. [Accessed: 01-May-2017].

[18] "Heroku | Sign up." [Online]. Available: https://signup.heroku.com/?c=70130000001xDpdAAE&gclid=Cj0KEQjwuZvIBRD-8Z6B2M2Sy68BEiQAtjYS3HGSxWQ2kCz0N_qruUZLiV8J_x3iDhX9oOaR9dOLvZ0aApai8P8HAQ. [Accessed: 01-May-2017].

[19] B. Endicott-Popovsky, R. J. Hinrichs, and D. Frincke, "Leveraging 2nd life as a communications media: An effective tool for security

awareness training," in *IEEE International Professonal Communication 2013 Conference*, 2013, pp. 1–7.
[20] "Cyber Storm V: After Action Report," Jul. 2016.
[21] M. R. Endsley, "Supporting situation awareness in aviation systems," in *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on*, 1997, vol. 5, pp. 4177–4181.
[22] T. Kanstrén and A. Evesti, "A Study on the State of Practice in Security Situational Awareness," in *2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2016, pp. 69–76.
[23] K. Renaud and A. De Angeli, "Visual Passwords: Cure-All or Snake-Oil?," *Commun. ACM*, vol. 52, no. 12, pp. 135–140, Dec. 2009.
[24] D. Davis, F. Monrose, and M. K. Reiter, "On User Choice in Graphical Password Schemes," *USENIX Assoc.*, Aug. 2004.
[25] Z. R. Steelman, B. I. Hammer, and M. Limayem, "Data Collection in the Digital Age: Innovative Alternatives to Student Samples.," *MIS Q.*, vol. 38, no. 2, pp. 355–378, 2014.
[26] K. Olmstead and A. Smith, "What the Public Knows About Cybersecurity," Pew Research Center, Mar. 2017.
[27] P. G. Ipeirotis, F. Provost, and J. Wang, "Quality management on Amazon Mechanical Turk," in *Proceedings of the ACM SIGKDD Workshop on Human Computation*, Washington DC, 2010, pp. 64–67.
[28] H. Tao and C. Adams, "Pass-Go: A Proposal to Improve the Usability of Graphical Passwords," *Int. J. Netw. Secur.*, vol. 7, no. 2, pp. 273–292, Sep. 2008.
[29] "American Red Cross | Help Those Affected by Disasters," *American Red Cross*. [Online]. Available: http://www.redcross.org. [Accessed: 06-May-2017].