**Abstract**

Bradley French

The Cyber Awareness Challenge continues to be the main source of cyber education to all Department of Defense (DoD) employees. It strives to educate the users of the risks, best advice, and overall security concern of the DoD, according to DoD standards. The Cyber Awareness Challenge presents this challenge in an assortment of presentations styles, each of which have their own pros and cons. This paper illustrates the pros and cons of each of the presentation styles, extracts the atrocious part form each of them, and proposes a new strategy on how best to integrate the new ideas into the system. The highlights of the new proposed strategy prevail in a new reward system, as well as a more interactive learning experience. The new system aims to attract users on a more personal level and provide them with a deeper connection and understanding of cyber. This strategy also highlights that cyber retention would be higher and more people would understand the baseline of cyber, in regards to the cyber education provided by the DoD. The intent of this paper is to connect the dots between presentation style and learning experience, indicate the current aberrations of the challenge, and propose a more appropriate way to better present the concept of cyber to all DoD employees.

**Outline**

Bradley French

1. Intro of Cyber Awareness Challenge
   1. Introduce problem-set of Cyber Awareness Challenge respective to how the challenge is presented
      1. Repetitiveness in Presentation
      2. Presentation doesn’t require learning of topic (cyber)
2. Establishing Current Presentation Style
   1. Interactive Slides
      1. Can click through without learning anything
         1. Doesn’t require in-depth understanding of topics
            1. allows for incorrect answers without correcting them
   2. Mini-games
      1. Some mini-games are just a quiz with extended graphics
         1. Ex: Cyber Wolf, Security Incident Mystery, Stay a Millionaire
      2. However, other mini-games are interactive
         1. The presentation is the same every test.
            1. Not a challenge

Ex: Having a question on a homework where the answer was provided, then asking the same question later on an exam.

If the presentation is the same, then the answer will be the same; you can ask the same question a different way and make it more challenging.

* 1. Overall scoring
     1. Cyber Awareness Challenge has a point and trophy system
        1. Overall score only needs to be 70%;
           1. Getting a 100% and a 70% are not different.
           2. Saying that only 70% of cyber topics are important
        2. Answers are online
           1. Someone can click through without learning. anything

1. Analysis of Presentation Problems
   1. Point-System & Trophies
      1. Not a challenge – means. Nothing.
      2. Challenges tend to have a reward; the name “challenge” implies difficulty
   2. New Presentations
      1. Knowledge in any topic requires various perspectives.
         1. Presenting information on a topic can contain repetitive information, but should be presented in a new light to allow different perspectives, critical thinking, and broader understanding.
            1. Ask a math problem on a homework assignment and then asking the same question in exactly the same manner will not require the student to know the concept if they memorized the answer. Present the same question in a different way, and it will require a little bit of thinking to solve the problem.
2. Recommended Approach
   1. Properties of Recommended Approach
      1. Reward System
         1. Ex: PT Test has 2 different rewards depending upon the score; You can take. The test a year later if you get above a certain score, or 6 months if you only pass and not exceed.
      2. Non-Slide Interactive Learning
         1. Would provide user to be less-likely to guess on questions.
            1. Ex: Provide a question and take in user input, don’t provide any input to the user.

Ex: Catch Me If You Can, Protecting Classified Information Scavenger Hunt

1. Evaluation Strategy and Future Work
   1. \*\*Future Work will need to be presented upon when I research further about the problems above.
2. Conclusion
   1. Briefly iterate over what the paper discussed and the approach taken; glide over the big picture of audience and learning objectives of the cyber awareness challenge from the problems to the potential future work.

**Introduction**

The Department of Defense’s (DoD) Cyber Awareness Challenge prevails as the main source of cyber education for all DoD employees. The challenge combines the etiquette of cyber security and DoD security standards to create a system of cyber education for all DoD employees. This includes, but not limited to, the security of the Common Access Card (CAC), appending external hardware, classified information, the variety of threats, and personal security for all DoD employees. This course exists online and interacts with users to provide, and assess, the user’s cyber security education level according to DoD standards.

The Cyber Awareness Challenge has been, and continues to be, the primary source of cyber education for all DoD employees. As the cyber domain continuously grows and further contributes to people’s everyday life, the necessity of cyber education expands. Education can be expanded through various methods: form of content, style of presentation, tone of the environment, and the process in which information is provided. In regards to the style of presentation, the Cyber Awareness Challenge possesses minimal presentation concepts, while trying to maximize the optimal cyber education. Enhancing the presentation style of the Cyber Awareness Challenge will lead to a better understanding of the cyber knowledge the DoD requires. This paper analyzes the difficulties of the current presentation format of the challenge and suggests properties of better presentation styles to most efficiently obtain knowledge.

**Current Presentation Style of Challenge**

The DoD’s Cyber Awareness Challenge presentation style can be broken four distinct different presentation styles.

1. Interactive Slides

One of the forms of presentations the challenge uses is various interactive slides. These slides are designed to present information for the user to read, understand, and move on to the next item. To help increase understanding of the cyber topics, the DoD even included some questions on some of the slides to help the user better assess their education level. However, these questions can be guessed correctly. Also, the questions are static and most, if not all, of the answers can be found online. Through various research methods, it is shown that courses should ban slides due to boring presentation of information, resulting in less interested and less knowledgeable students, leading to less understanding of the material (Ralph, 2017). Additionally, slides don’t require any in-depth of knowledge. The user can wait the time necessary to move-on to the next slide, without requiring any Interaction or understanding of the material. The Cyber Awareness Challenge is not any different. Although the slides are a little more interactive, the overall concept of using slides-based presentations will have less of an impact in providing cyber education to DoD users.

1. Quiz-Based Mini-Games

Mini-Games are another form of presentation the Cyber Awareness Challenge utilizes. Although there are different forms of mini-games, this section will be referencing the mini-games that are similar to that of a quiz. Using the Cyber Wolf mini-game inside the Cyber Awareness Challenge, it can be noted that it is just a quiz with extended graphics to make the user more intrigued. However, there is no actual interaction. The only difference between using this method versus displaying an actual quiz or test is the graphics provided by the wolf and pigs as you answer questions. This visualization actually removes the focus of the content presented and directs it toward an animation that doesn’t provide any details toward the content being presented. Although the Cyber Wolf was the example provided, there are many other challenge-type mini-games in the Cyber Awareness Challenge that provide similar animations and redirect the attention from the content to an animation such as the Security Incident Mystery and Stay a Millionaire.

1. Interactive Mini-Games

Similar to that of quiz-based mini-games, the Cyber Awareness Challenge contains some interactive mini-games that present the cyber content in a unique way to maintain the user’s attention towards the content being displayed. While challenging the user’s understanding of the material and ensuring a unique and interactive time of the user, the Cyber Awareness Challenge presents various interactive mini-games to engage the user. While these are challenging and can provide a good understanding of concepts, they are repetitive. The Cyber Awareness Challenge requires annual training to maintain DoD standards, however, the challenge itself never changes. Some of the answers, if not all of them, can be found online. There are even unclassified versions of the video that have been released online with all the correct answers. Any user could follow the video as they take the challenge, click on the buttons the video clicks, get a perfect score, and have not learned anything. Eventually, having to take it every year, a user will get dull of the presentation, leading to zombielike behaviors while taking the challenge and going through the motions. While interactive mini-games are definitely a positive in terms of presentation styles as the user has to stay engaged with the content, the mini-games presentation should change ever so slightly to keep users on their toes.

1. Scoring and Reward

Furthermore, the Cyber Awareness Challenge incorporates a scoring system using points and trophies. The user taking the test can acquire points by getting questions correct. The test requires that the user make a seventy percent (70%) of the overall points to obtain a passing score. Like most courses, a common minimum understanding of a topic is usually required in attempting to asses a user’s comprehension of said topic. The trophies, however, are not required and are able to be procured in each sub-section. In each sub-section of the test, there is one of the three presentation styles mentioned above, and they evaluate your understanding for that specific topic. If you get all the questions correct in that specific sub-section, you win the trophy for that specific sub-section. It is even possible, in the same Cyber Awareness Challenge, to go back and retake a particular section to make sure you obtain the trophy for that section. However, the trophies don’t provide any reward. Collecting all the trophies, obtaining the maximum number of points, and trying your hardest to rework sections that you answered incorrectly, will equate to the same conclusion of someone who executed the bare minimum amount of work to get the minimum score with no trophies. There is no challenge in this. Challenge, by definition, means a stimulating task or problem (Webster-Dictionary). However, the Cyber Awareness Challenge allows for people to slide by without completely comprehending the cyber topics presented in this course. Using a similar assessment as an example, the PT Test, the bare minimum required can be presented as seventy-five percent (75%). Then, you retake the test every six months after to be adequately maintained with Air Force standards. However, you can obtain a ninety percent (90%) and be rewarded with only having to take the PT test a year later. Therefore, some people are more opt to maintain their health and fitness to obtain the higher score and be rewarded with the higher reward. In the Cyber Awareness Challenge, there is no higher score to work towards. Therefore, people will only provide the work necessary to complete the challenge with a passing score and move on.

**Analysis of Cyber Presentation**

The main point of the Cyber Awareness Challenge is to determine mastery and teach capabilities required to all DoD users using DoD’s standards of minimum cyber education. The word challenge is defined as “a stimulating task or problem,” (e). While the Cyber Awareness Challenge itself is a stimulating task, it is a static, repetitive task taken by many users. The presentation of the content, and the content itself, does not change. Due to these static variables at play, there is content posted to the internet providing the correct answers to the challenge. An example of this is a famous youtuber, PewDiePie, who took the unclassified version of the Awareness Challenge (B Channel, 2018). He may not have gotten everything correct, however, most of his answers were correct and open to the public for anyone to see. This reduces the challenge aspect and turns it into a follow-the-leader type situation. The only person who needs to know the answers is the one who takes the initial test. The challenge is no longer a test of mastery in terms of cyber education but a test of which online source can I find to provide me all the answers.

Challenges generally imply some sort of reward. In past times, people would challenge each other to duels, using pistols. The victor would continue to live while the loser generally lost their life. In regards to the Cyber Awareness Challenge, the only challenge requires passing the minimum requirement score of seventy percent (70%) of the questions correct. On another note, the requirement cannot be a challenge, per se, if everyone is required to pass it. Similar to that of the AF PT test, the minimum requirement is a seventy-five percent (75%). However, if you get above a ninety (90%), you get a reward of postponing the required test by six months. The AF deems you worthy of not having to test you for another PT check to see if you are within requirements within a six month span. Alarmingly, the Cyber Awareness Challenge does not present any rewards for the work required, except a passing certification; there is no difference between someone who acquires the minimum score and someone who acquires the maximum score. This aspect of the Cyber Awareness Challenge is unique because the challenge includes trophies that a user can obtain. However, these trophies don’t go toward an end-goal; they mean nothing except potential satisfactory for the user. After taking the challenge the first time, recognizing the trophies mean nothing, and only the minimum score is required, a user will be more inclined to go through the test as fast as they can without trying to fully comprehend the topics.

**Recommended Approach**

Using education in universities, techniques in presentations, and real-life examples of AF standards for passing criteria, I am presenting a strategy to enhance the presentation style represented in the DoD’s Cyber Awareness Challenge. This involves the use of an interactive learning experience provided to everyone, however, including the aspect of a challenge. This allows for users to excel in the cyber domain while learning basic DoD standards and obtain rewards for their completion of challenging work. In addition to providing a rewarding system to increase cyber education efficiency, there also needs to be an aspect of engagement and interaction requiring user input to increase knowledge retention. The recommended properties of enhancing the Cyber Awareness Challenge, pertaining to presentation style, can be described below.

1. Rewards System

The implementation of a rewards system should be utilized to reward excellent cyber knowledge retention and understanding of users. The notion of rewarding someone for behavior can be defined by Incentive Theory. Incentive Theory concludes that rewards can be utilized to obtain greater user attention (Cherry, 2018). In addition to Incentive Theory, it is noted that the attention of a person is conjoined with their ability to retain information, also known as Theory of Attention and Memory (Chun et al, 2007). Therefore creating a rewards system that users will believe to be satisfactory with the completion of the course will provide better understanding and retention of cyber knowledge. With the current system of trophies and scoring used as a partial implementation, the new rewards system would reward users based on the trophies obtained, as well as the overall score attained, instead of just providing a meets satisfactory requirement. Then, using the current system, users would then be allowed to test as much as they wanted, being that it was only required once every six months, unless rewarded by obtaining an initial excellent score, therefore postponing their essential training, similar to that of the PT test. Also using a six month requirement, instead of a one year requirements, unless the user was already adequately aware of the information being presented and achieved an excellent score, would increase cyber education and reward those who already understood the basic cyber concepts.

The trophies would be the main indication of the challenge aspect of the course, whereas the scoring would primarily indicate the level of completion of the course. While the scoring is directly related to the number of trophies, the trophies are indicated by perfection of each sub-section. The number of trophies would ideally indicate the user’s excellence in various cyber topics, and the time would increase for each cyber section the user achieved. If the user achieved a ninety percent (90%) trophy rate, they would be exempt for one set of training, moving their next due date to an annual training instead of bi-annually. This is the challenge aspect and provides users the ability to be rewarded for their excellent effort. This would also provide a more engaging atmosphere as users would need to understand the content to achieve excellent scores.

The scoring system would stay the same. Users should still maintain a minimum requirement to understand the cyber content displayed in the Cyber Awareness Challenge. The score would be that indication, however, the minimum score would require a bi-annual requirement for the completion of the challenge. This system of the minimum requirement scoring, combined with the rewards for achieving excellent scores, would allow users to feel accomplished as they work for their scores as well as requiring a base knowledge set of cyber skills. Additionally, this would increase the attention of the user as they would need to provide effort to achieve the ninety percent (90%).

1. Interactive Learning

Likewise, providing a more interactive presentation environment for users to better focus their Cyber Awareness Challenge skills would allow higher rates of understanding. This comprehension would lead to better cyber education across all DoD employees and result in better retention of knowledge, as well as overall scores regarding the challenge. With interactive learning, the users are more opt to use their critical thinking skills, learn to make better decisions in situations, and become better at teamwork (Scholastic Parents Staff). Cyber education as a whole would be increased throughout DoD and cyber concepts could be expanded further.

To demonstrate how the interactive environment would be utilized, I will depict removing the CAC from a computer to properly secure gear. In the current presentation style, the slides are presented and state to remove the CAC from your system before walking away from the computer. Then, in an interactive quiz-based mini-game, a coworker walks over and asks to go to lunch with you. It to choose an action and provides one of the answers as “Remove CAC/PIV or lock computer” (Defense Informations Systems Agency, 2017). While this tests to see if you know what to do, it doesn’t let you interact with your CAC. In a real setting, there isn’t going to be an option list that appears asking you what to do next; the only way to not forget your CAC is to practice removing your CAC from an actual computer. If the interactive environment allowed for this virtual setting where you could actually play a specific scenario, with no guidance from the computer, it would better teach and assess your understanding of remembering to remove your CAC. This example can be applied to all aspects of the Cyber Awareness Challenge. The two difference presentation models allow for different levels of user interaction, and ultimately, better decide the knowledge and retention level of cyber education of the user.

Furthermore, a situation similar to the one described above, where a user plays a scenario with no guidance from the computer, would allow for complete control of the users answers without predefined answers. This would guide the direction of the Cyber Awareness Challenge towards the thought process of the user and not towards the answers provided by the system. This would substantially decrease the probability of a user guessing the correct answer, therefore removing the easy aspect of the challenge. Users would need to provide effort in this course to prove excellence, however, a basic understanding of cyber would also be required. Users would also be less likely to just skip through the presentation as they would need to know and comprehend the content to complete these scenarios. While there are similar scenarios in the Cyber Awareness Challenge, such as Catch Me If You Can and Protecting Classified Information Scavenger Hunt, the DoD, DoD employees, and the Cyber Awareness Challenge would benefit from having the majority of the presentation be provided in this manner.

In addition to not being able to skip through the process, users would need an interactive environment that changes the presentation ever so slightly. This would remove the repetition and would complete two tasks: boring users or repetitive information and presentation, as well as not allowing users to only have to take the Cyber Awareness Challenge only one time to understand it, then every time after, click through because they already knew all the answers. While changing the content could provide the same effects, changing the presentation may be a little easier, depending on how that is done, but also allows for a new perspective instead of an entirely new set of content, which might be quite difficult to do.

**Evaluation Strategy and Future Work**

1. Should the Cyber Awareness Challenge be renovated or replaced? In terms of determining what path to take, reinventing the wheel can be a wasteful and time-consuming task if done inappropriately (Azilen Technologies, 2017). However, if done appropriately, you could create a new trend and a new solution to a large problem (Kowalczyk-Harper, 2016). However, each path will provide a different result and result greatly in determining the effect of cyber understanding for the user. This debate could go either way, it truly depends on the person pursuing the renovation or replacement of the Cyber Awareness Challenge and the path they choose.
2. What concepts of gamification can apply to the proposed strategy to better present cyber security? Gamification is the application of gaming elements, i.e., points, competitions, rules, to other activities that are not normally related to games. It has the ability to increase engagement, motivation, and satisfactory in normal real-life activities that are not generally games (Tenfold, 2018). Although there are already concepts of gamification present in the Cyber Awareness Challenge, those concepts could be applied to a more interactive experience. Similarly, new concepts of gamification could be presented to provide a further in-depth gamified experience, potentially resulting in increased engagement, motivation, and understanding of the topic. Overall, the increased usage of gamification can help the Cyber Awareness Challenge in understanding, retention, and user experience.
3. What other interactive learning capabilities can be addressed that have not already been addressed? There are various presentation styles that can be presented to the user’s to provide various UI and UX experiences. However, each one of them have their pros and cons. Inserting, or even removing, an interactive learning portion to the Cyber Awareness Challenge can have significant impact on a user’s comprehension of the cyber topic. In accordance with various references, there are a minimum of three learning styles: Visual, Auditory, and Kinesthetic (Duffy, 2015; Roell, 2018). If you remove a learning style, it could remove the ability for a set of individuals to maximize learning of cyber education. On the other hand, adding another style could confuse the user as they may not learn that way. In regards to difficult topics, such as cyber, various learning capabilities and interactive tools can both help mitigate learning as well as aggravate the user and push them away.
4. Using the concept of Incentive Theory, what rewards can be awarded for completing the Cyber Awareness Challenge? Incentive theory does not state that what rewards to present to the users, as this will depend greatly on the material. However, it does state that these rewards will need to be achievable and personal (Cherry, 2018). Users will only try to obtain rewards that are worth providing. Assume the current Cyber Awareness Challenge reward, which is nothing other than getting a passing score. Users are not as likely to try and achieve all of the trophies and maximize their score, effort, or understanding. However, imagine rewarding a deadline extension of the current one-year retake on the test to a two-year retake if they get a ninety percent (90%). Similar to that of the PT test, a lot of people will try to achieve a minimum score of at least ninety to achieve the award. Overall, the reward for the Cyber Awareness Challenge will greatly determine user’s thought process, experience, and understanding of the Cyber Awareness Challenge.

**Conclusion**

The DoD Cyber Awareness Challenge presents the baseline cyber education for all DoD employees. It uses various presentation styles in attempt to maximize cyber understanding for all users. The current presentation styles include interactive slides, mini-game based quizzes, and interactive mini-games. These games are then used to create a scoring and reward-based system. Although there is a reward system, there is no actual reward. The only reward available is that of passing the test, as long as the user obtains the minimum required score. I propose that this type of system will reduce the overall understanding of cyberspace, as well as reduce the user’s interest. To counter this effect, I propose a new system with a newly integrated reward system, as well as increased interactive learning material to negate the simple, basic slide-based materials that users click through. The reward system will provide users an incentive to pursue deeper cyber knowledge, while the new interactive learning while maintain engagement of the user. This new strategy will provide users with increased attentiveness, therefore, leading to better retention and understanding of cyber knowledge, as well as a way to be rewarded for their efforts in attaining the score they desire.

**References**

Azilen Technologies. (2017) “8 Reasons Why You Should Not Reinvent the Wheel” *Medium*. <https://medium.com/@AzilenTech/8-reasons-why-you-should-not-reinvent-the-wheel-e36fcca3cfcc>

“Challenge” *Meriam-*Webster. <https://www.merriam-webster.com/dictionary/challenge?src=search-dict-hed>

Martin M. Chun, Nicholas B. Turk-Browne. (2007) “Interactions Between Attention and Memory” *ScienceDirect.* <https://ntblab.yale.edu/wp-content/uploads/2015/01/Chun_CONB_2007.pdf>

Tenfold. (2018) “Gamification is the Future of the Workplace. Here’s Why” *Lean Competency System (lcs)*. <https://www.leancompetency.org/lcs-articles/gamification-is-the-future-of-the-workplace-heres-why/>

Kendra Cherry. (2018) “The Incentive Theory of Motivation” *verywell mind*. <https://www.verywellmind.com/the-incentive-theory-of-motivation-2795382>

Scholastic Parents Staff. “Understanding Interactive Learning” *Parents*. <https://www.scholastic.com/parents/family-life/social-emotional-learning/technology-and-kids/understanding-interactive-learning.html>

Paul Ralph. (2017) “Universities should ban PowerPoint – It makes students stupid and professors boring” *Business Insider.* <https://www.businessinsider.com/universities-should-ban-powerpoint-it-makes-students-stupid-and-professors-boring-2015-6>

Hannah Kowalczyk-Harper. (2016) “Why You Should Reinvent the Wheel” *Medium*. <https://medium.com/@MsHannahTweets/why-you-should-reinvent-the-wheel-e5810c4fad1b>

B Channel. PewDiePie play Cyber Awareness Challenge. Published 9 August 2018. <https://www.youtube.com/watch?v=ghdrKwnZiOM>

Kelly Roell. (2018) “The 3 Different Learning Styles” *ThoughtCo.* <https://www.thoughtco.com/three-different-learning-styles-3212040>

Defense Information Systems Agency. (2017) “Department of Defense Cyber Awareness Challenge”

<https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm>

Dannielle Duffy. (2015) “The 3 Different Ways People Learn (VAK Model)” *LinkedIn*. <https://www.linkedin.com/pulse/online-quiz-3-different-ways-people-learn-vak-model-dannielle-walz>