Cyber Clinics: Re-imagining Cyber Security Awareness

David T. Croasdell
University of Nevada, Reno
davec@unr.edu

James R. Elste
Cognitive Extension, Inc.
elste@inqiri.com

Adrienne Hill
University of Nevada, Reno
adrienne@nevada.unr.edu

Abstract

Cyber Clinics are modeled after the methods used in teaching hospitals to perform triage and treatment in healthcare settings. Cyber Clinics are interactive, personalized workshops that provide education on the importance of protecting devices, data and identity from physical and digital compromise; Cyber-Medics offer recommendations on achieving this goal following triage sessions designed to help identify user knowledge and experience levels. This paper examines cyber security awareness training with different awareness methods based on measurements of time, cost, personalization, relevance and interactivity. Results illustrate the potential for the Cyber Clinic model to be an effective method for educating users about cyber security. Challenges in measuring efficacy and recommendations for expanding Cyber Clinics also are discussed.

1.0 Introduction

Cybersecurity risk and society's dependence on information technology are systemic issues indelibly intertwined with our modern digital world. The hazard is of such magnitude that government, industry, and academia are marshalling significant resources and focusing substantial effort to address these problems. Cybersecurity is not an acute crisis that will one day be resolved, it is an emergent property of technology and human interaction with technology, and as such represents a fundamental area of research.

"We hypothesize that, at some point in the not-so-distant future (if it is not already true at present), cybersecurity will be recognized widely as the "master problem" of the Internet era." – Cybersecurity Futures 2020, UC Berkeley Center for Long-term Cybersecurity

Hacked emails, a cyber-attack that shut down Internet service on the East Coast, data compromised from a primary credit agency and a breach of 500 million user accounts all provide examples of cyber-attacks that have made headline news in recent weeks. Opportunities for security breaches are increasing as people continue to add to the number of devices, applications and sites they use; the public cannot help but leave behind "data exhaust" as they do everyday tasks on the Internet. They don't know how or if they can control this exhaust in a meaningful way [8]. Awareness of a global, chronic cyber problem is growing and becoming more troubling in the eyes of the public. While shocking headlines attract attention and raise awareness, they do little to communicate effectively the practices an individual should implement to improve their own cybersecurity. Rather than writing another alarming article about the threat of cyber-attacks, we need to ask a more important question: Do the methods employed for awareness and training actually improve individual cybersecurity practices?

The need for effective training approaches is clear, but the training methods vary greatly in time commitment, cost, and interactivity with the participant. This paper introduces the Cyber Clinic approach and examines cyber security awareness training comparing different awareness methods based on criteria of time, cost, personalization, relevance and interactivity.

2.0 Background

While some individuals have some awareness and rudimentary understanding of cyber security, in-depth understanding of how to protect personal data and devices from compromise is limited. A recent Pew Research Center survey asked a sample of Internet users to answer thirteen cyber security questions. Results showed respondents answered fewer than half the questions correctly on a challenging knowledge quiz about issues and concepts. Only 33% of respondents could identify what an "https://" URL meant; Fewer than 10% of respondents were able to identify what multi-factor authentication is—concepts everyone should understand at a basic level.

The focus of the United States' cybersecurity strategy is the National Institute of Standards and Technology's (NIST) Cyber security Framework which takes a bottom-up approach organizations can adapt to their risk tolerance. The NIST Cyber Security Framework starts with the executive level deciding "mission priorities, available resources, and overall risk tolerance." Cyber Security Framework is aimed toward organizations rather than individuals [15]. Because of its thoroughness and adaptability, other countries have incorporated the model into their own frameworks; Many believe it is the "standard for due diligence" for the private sector [15]. The NIST Framework Core "is an organizational map of industry-recognized best practices that are helpful in managing cyber risk and provides unified terminology for organizations to communicate more effectively" [15].

NIST 800-16, Role (Based Model for Federal Information Technology/Cyber security Training) describes training on a continuum that can be IT security. Using this model, all users in zation have security awareness; levels of training and education depend on specific

URI: http://hdl.handle.net/10125/50427
ISBN: 978-0-9981331-1-9

organizational role [16]. Awareness is "immediate, short-term and issue specific"; for example, a user learns how to strengthen their password. The point of awareness is to explain what is allowed and not allowed, informing users of the detrimental effects of not being aware of issues [16]. The next level of training, Cybersecurity Essentials, is "an individual's familiarity with—and ability to apply—a core knowledge set which is needed to protect electronic information and systems" [16]. Examples of this knowledge includes the "technical underpinnings of and its taxonomy, terminology and challenges" and "fundamental security design principles and their role in limiting point of vulnerability" among others [16]. The publication also distinguishes role-based training from topic-based training; the former allows the user to learn what they need to know so they can implement the new knowledge based on their current role, and the latter has the same learning objectives, is more of a "one-size-fits all" solution and therefore easier to implement [16].

The NIST Special Publication NIST 800-50, Building an Information Technology Security Awareness and Training Program, is a complementary publication to NIST 800-16 that works at a higher strategic level by "discussing how to build an IT awareness and training program" [4]. The publication focuses on centralized versus decentralized policy, strategy and implementation of training, commenting on which works best given an organization's size. It recommends developing awareness materials that will reinforce desired behaviors through relevant awareness topics and timely source materials. It distinguishes awareness from training in which "awareness material is simply to focus attention on good security practices" [4]. The publication recommends various methods for delivering awareness material including posters, newsletters, email alerts, web-based and instructor-based sessions, mascots, crossword puzzles and awards [4]. Techniques for feedback and assessing progress include surveys and questionnaires, focus groups, interviews and status reports.

Written Information Security Program (NIST 800-53). The standard provides security policy, control objectives and standard security guidelines The SANS Institute has numerous educational offerings to help computer and technology users ensure they are operating in a sage and secure manner. Course offerings such a "Security Awareness training for End Users' is "designed to ensure compliance and provide training that changes user behavior ... getting learners to both "know" and "do" the right thing at the right time with accuracy and consistency.

Cybersecurity is receiving significant attention in academic institutions across the country and around the world. It is the focus of a substantial amount of grant funding and new educational programs, such as online graduate and undergraduate degrees. The launching of new programs and similar cyber security center initiatives are hallmarks of the rapid growth in the cybersecurity marketplace. It is difficult to address all relevant efforts in a brief evaluation of the current cybersecurity marketplace.

3.0 Re-imagining cybersecurity as a public health crisis

"Cybersecurity is a shared responsibility. The more systems we secure, the more secure we all are" [7]. Cybersecurity can be viewed as a "public health crisis" in which the community needs to be engaged to contain threats. "… what happens when your technology is compromised and aimed toward someone else" [8]. Approaching cybersecurity from a "public health" perspective provides effective models for cybersecurity interventions and education. Meaningful and measurable educational outcomes provide value in the context of safeguarding one's digital life and addressing broader cyber-hygiene implications for local, regional or global communities.

3.1 The Cyber Clinic Approach

For hundreds of years, universities around the world have responded to the problem of public health by organizing into medical schools and teaching hospitals. Similarly, organizing the educational and research capabilities of a university into a "cyber teaching hospital" capitalizes on a proven model for responding to a complex problem, producing highly trained experts, and conducting research into a dynamic field of study — cybersecurity.

Using the concept of a cyber teaching hospital as the organizing principle, the initial intervention focused on the problem of individual cyber-hygiene. Just as washing your hands is good hygiene practice, certain cyber practices help protect against cyber problems. Improving cyber-hygiene, just like washing hands, is good for the individual and the community.

To deliver the cyber-hygiene guidance in the most effective manner the model of a mobile medical clinic was adapted to take public health approach to "treat" individual participants. Cyber Clinics follow a triage, treat, and train approach where trained "Cyber-Medics" (students with sufficient knowledge to teach basic cybersecurity practices) provide personalized cyber-security guidance. The main objective of a Cyber Clinic is to evaluate an individuals level of knowledge and current cybersecurity practices and then, in a one-on-one sessions with Cyber-Medics, to teach participants effective techniques in cyber self-defense. Cyber Clinics provide a mutually beneficial value proposition; the "patients" learn how to improve their cyber self-defense, and cyber-medics apply their cybersecurity knowledge and develop practical experience.

In the cyber clinic, trained "cyber-medics" provide individualized guidance on good cybersecurity practices to the participants. This provides a more engaging and

effective interaction for the participants and allows the students to apply their cybersecurity knowledge in a meaningful way, generating an experiential learning opportunity. One individual who participated in the clinic felt compelled to provide the following feedback:

> "Wanted to take a minute to tell you the Cyber Club Clinic was excellent! What an innovative, fun and effective way to further user's knowledge of device, data, and identity security! It was fun, well organized, very professional guidance sheets, and each student that I talked to on the individual topics was EXTREMELY knowledgeable and well versed in communicating technical talk in easy to understand terms. Very impressed with them! They did an exemplary job! Have a good day and thank you for coordinating this event with them! Well Done!"

Researching good cybersecurity practices to develop cyber clinic guidance, then training to deliver the approved guidance to individuals in a cyber clinic setting provides students with an immersive learning experience. Training is designed to assess current practice and behaviors as well as to convey methods to modify existing behaviors as appropriate to the individual. The purpose is clear for the Cyber-Medic: Develop expertise so that they can help individuals and organizations improve their cybersecurity through better cyber-hygiene.

3.2 Triage, Treat and Train Process

The participants or "patients" in the cyber clinic process start at the triage station, which assesses their current level of knowledge and identifies any potential cyber problems. After triage, they then receive individualized guidance, according to their knowledge level, on recommended cybersecurity practices that will help protect their identity, data and devices. For example, we recommend the use of passphrases, which are more secure and easier to remember than a regular password.

Triage was first used by Napoleon's Surgeon-in-Chief during the Napoleonic Wars to prioritize patients by the severity of their wounds and treat them accordingly, creating a process of patient treatment in battlefield settings [10]. The continued use of triage centuries later in emergency rooms where patients are quickly assessed to determine which order they are seen is a testament to how effective this dynamic process is; through triage, a medical professional can assess and prioritize strangers within a matter of minutes [10].

At a Cyber Clinic participants are given a triage handout, which asks generic questions about their knowledge in data, device and identity security. One question asked is "Do you know how to use the recovery features on your device?" Cyber-Medics providing triage evaluate the patients responses and give them a designation of "basic," "intermediate" and "advanced" for the data, device and identity stations. Patients then proceed to an open station presenting their triage assessments to the Cyber-Medic. The Cyber-Medics continue the process of treatment and training by giving guidance based on the individual participant's level of knowledge assessed in triage. During this process, participants are welcome to ask questions about the guidance and Cyber Medics can ask more probing questions about the individual's knowledge. Cyber Medics are conservative with guidance beyond what they have been trained to give to prevent misleading or contradictory advice; the Cyber Clinic model is predicated on uniform guidance with flexibility in the level of specifics for each participant.

Cyber Clinic guidance for each topic illustrates why it is important to protect one's data, device and identity from physical and digital threats (i.e. asks participants to imagine what it would be like to lose their most important digital assets) provides background information to help educate the participant, and then providing specific guidance on what to do and resources with details on how to do it. Rather than teach the step-by-step process to accomplish the practice, the interaction is focused on supporting the individual's underlying motivation to take action and providing the means to accomplish the objective of applying the practice. The Cyber-Medic discusses with the participants what to do and why to do it— the specific actions they can take are reinforced by handouts with links to resources and instructions on implementing the guidance.

By moving participants through a process of multiple, short, five to seven minute interactions, physically moving between stations and re-engaging with a new Cyber-Medic each time forces maximum participant attention and focus. It is much more difficult to get distracted in a one-on-one conversation than in a classroom or online training session. Time is also optimized with an individual time commitment of between twenty to twenty-five minutes for the entire cyber clinic process.

Five Cyber Clinics have been conducted by a student organization at a university in the western United States. The students held these cyber clinics in Fall 2016 and Spring 2017. The second cyber clinic, held at the university in the same semester, focused specifically on providing guidance to fellow students and faculty. A third clinic was held for state employees, the forth and fifth were held for state's Attorney General's Office.

4.0 Methodology

To better highlight the different strengths of the various cybersecurity awareness and training methods, including the cyber clinic approach, a simple assessment along five criteria representing dimensions of effective training contrasts five different methods. This initial, simplified analysis provides an indication of the potential for future, more detailed analytical studies of innovative

delivery models and the efficacy of communicating cybersecurity practices.

Five approaches to delivering training are explored: print media, video presentation, in-person security conferences, on-line training modules and cyber clinics.

Print material: includes books, posters and manuals related to cyber security; examples include books found on Amazon.com such as Cyber security 101: What You Absolutely Must Know, Cyber security for Beginners and Computer Security for Dummies and posters found online and in NIST 800-50. The Department of Homeland Security developed print materials for their 'Stop. Think. Connect.' campaign to increase public awareness of issues and encourage the public to think of as a "shared responsibility" among community members, coworkers and students [15]. Resources include tip sheets, presentations and blogs [2].

Videos: include news, interviews, explanatory and instructional videos found on websites such as YouTube, blogs and awareness training companies. For example, the company Security Awareness Training has dozens of videos related to HIPAA, PCI data security standards and IT certification. They can brand videos for companies; however, their videos are not free [12].

Cyber security conferences and workshops: are held around the world for specific industries and roles within organizations and range from the very prestigious to the very obscure. An example of a more prestigious conference is the Industrial Control System's (ICS) Cyber Security Conference which appeals to critical infrastructure organizations. The four-day conference features various breakout sessions, prominent keynote speakers like Admiral Michael Rogers, Director of the NSA, and registration starting at $1,595 [14]. Other conferences such as SecureWorld's events start at $30 to attend open sessions [13].

Online training: includes sites like Udemy, Teach Privacy, Future Learn, Coursera, and the SANS Institute, to name just a few. Online training is different from videos because online training platforms allow for practice, exercises, supplemental resources, labs, quizzes or some form of interactivity with the user. Online course prices and relevance vary. Teach Privacy, for example, has courses developed by Daniel Solove, a professor of law and preeminent figure in the field, and Udemy courses are developed by "experts" within the field.

Cyber Clinics: as previously discussed, use a public health approach to educate participants in using triage and treatment to tailor the participant's experience.

Five criteria are used to benchmark each method, each rated with a score of 1 to 4 where 1 is poor performance and 4 is excellent performance.

Interactivity: Can the facilitator and participant give and receive feedback and questions? Interactive learning has been shown in studies and anecdotally to increase student learning performance when the student can, for example, replay and slow down instructional videos [11] or when they can talk with other students about questions posed by an instructor [1].

Personalization: Does the training material change to suit the current knowledge of the participant? Personalization is important to accommodate participants from various technical and professional backgrounds.

Time: How long does the training take? Training time varies greatly among methods but shorter training methods are more accessible for working professionals or those with little knowledge.

Cost: How much does the training cost? Low or no cost options are more available to the public whereas high cost methods usually used by IT or business professionals.

Relevance: How current is the content of the training material and was it developed by a reliable source? Content that is continuously updated to keep up with the changing landscape is more valuable to the user regardless of their knowledge level. Content developed by professionals or experts in are more likely to true and constructive information.

5.0 Results

A comparison was performed based on subjective rankings of awareness training delivery methods. Results are presented in Table 1 and discussed below.

Table 1: Comparison of training delivery methods

Criteria	**Print**	**Video**	**Conference**	**Online Training**	**Cyber Clinic**
Interactivity	1	1	3	3	4
Personalization	3	3	1	3	4
Time	2	3	1	2	4
Cost	3	4	1	4	3
Relevance	2	3	4	4	4
Total	**11**	**15**	**10**	**16**	**19**

Print materials perform poorly in interactivity, time and relevance since they are static, the time it takes to read the material varies and their advice may be outdated as soon as they're printed. There are many options for users with varying levels of knowledge and experience, so the print option does better in personalization. Cost is also relatively low.

Videos score well in personalization, time, cost and relevance because users can easily access videos for their level of knowledge, the videos are usually free and new content is added frequently. They score poorly on interactivity because users may or may not be able to interact with the creator of the source material or they may receive answers to questions from users with unverified credentials.

Conferences and workshops score high on relevance and interactivity but low on personalization, time and cost with the acknowledgment that these variables vary greatly depending on the conference.

Online training scores high in interactivity, personalization, cost and relevance for reasons mentioned previously and for their relative low cost and the user's ability to select courses that match their knowledge level. The courses score low on time because courses often take upward of an hour to complete.

Cyber Clinics score high in all criteria. Cyber Clinics are extremely interactive because the process is one-on-one between the participant and the Cyber Medic; the participant can ask questions and Cyber Medic can answer them and ensure the guidance is understood or rephrase it for greater understanding. Changing stations forces participants to focus and engage in the process, unlike videos or print material in which one can fall asleep during more mundane instruction. Cyber Clinics are more personalized than a conference or workshop setting because the triage stage and the treatment that follows are tailored. The Clinic can be completed in 20 minutes, is free to participants, and the guidance stays relevant as the participants can check online for periodic updates.

6.0 Discussion

Using the public health metaphor under a cyber teaching hospital construct produced the cyber clinics as an intervention designed to improve individual participant cybersecurity practices. In comparison with other common awareness and training approaches, the cyber clinics appear to provide a superior performance across all evaluation criteria.

6.1 Cyber Clinic Challenges

The greatest challenge with the Cyber Clinics is assessing their efficacy. Initial efforts to test the model precluded a participant survey during the Cyber Clinic process. One constraint was limited manpower: administering a survey would have taken away from resources at the cyber-medic stations. There were also privacy and security concerns regarding the tracking of participants. Consequently, there is little data to determine whether participants implemented guidance afterward and if they found the guidance valuable. However, in the preparation of this manuscript, previous participants completed a survey about the clinic they attended. The sample size is very small and there was a five-month delay in completion of the survey, but notable results are listed below:

- All participants said their knowledge of data, device and identity security issues and their awareness of issues increased after the clinic
- All participants said the Cyber Medics were "very helpful" and they would attend another Cyber Clinic
- Multiple participants implemented advice from the Cyber Clinic, specifically changing their passwords more often and backing up their device

Many more participants will need to be surveyed to assess the clinic's efficacy and whether improvements should be made to the triage, treat and train technique and cyber clinic approach.

6.2 Recommendations

Cyber Clinics have the potential to change the way in which the public is educated on cybersecurity practices. Additional Cyber Clinics should be conducted to assess their validity as effective cyber security awareness training methods. The clinics appear to positively affect behaviors among the participants. Additional clinics will create more opportunities to collect data on the efficacy of the approach.

Opportunities to extend the model include replicating the Cyber Clinic model to other college campuses that can train Cyber Medics and hold Cyber Clinics. The University of Nevada, Las Vegas is an example of a potential expansion location. More efforts to expose the Cyber Clinic model to the local and academic community are encouraged, whether this is through marketing and press coverage or academic papers.

It is recommended continuous improvements should be discussed and made to maintain Cyber Clinic guidance relevance and measurements of Cyber Clinic efficacy incorporated into the model in the form of participant surveys. The latter recommendation will allow for greater consideration among others interested in using the Cyber Clinic model.

7.0 Conclusions

Many awareness training methods are available today. Cyber Clinics are new among them but have proven to be a unique, engaging, personalized and interactive way to educate the public about awareness and its importance. While more study is necessary to prove Cyber Clinic effectiveness, initial survey results are encouraging and positive feedback among participants speak to the model's future usefulness.

8.0 References

[1] Anderson, J. (2014, November 17). The Benefit of Interactive Learning. Retrieved April 30, 2017, from http://www.gse.harvard.edu/news/14/11/benefit-interactive-learning

[2] Department of Homeland Security. (2017, March 10). About Stop.Think.Connect. Retrieved April 30, 2017, from https://www.dhs.gov/about-stopthinkconnect

[3] Dunn Cavelty, M. (September 2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering* 701-715. doi:10.1007/s11948-014-9551-y

[4] Hash, J., & Wilson, M. (October 2003). Building an Information Technology Security Awareness and Training Program (pp. 13-59, Tech. No. NIST Special Publication 800-50). National Institution of Standards.

[5] Retrieved from https://www.complianceforge.com/nist-800-53-based-security-documentation/?gclid=Cj0KEQjwxdPNBRDml9-C3-PUlZEBEiQADD5NSYVn-GY6J3hfG32VDwA7fsOVkBXX1MKzzwozqTIHfGUaAlHq8P8HAQ .

[6] Retrieved from https://securingthehuman.sans.org/security-awareness-training/enduser

[7] Johnson, J. (2015, May 29). Jeh Johnson Quote on Cyber Security. Retrieved April 28, 2017, from http://criminaljusticepursuit.com/criminal-justice-quotes-to-live-by/jehjohnsonquote

[8] O'Leary, L., & Mills, E. (Producers). (2017, March 21). (Almost) 100 Days of Trump [Transcipt, Radio series episode]. In Marketplace Weekend. St. Paul, Minnesota: American Public Media.

[9] Olmstead, Kenneth, and Aaron Smith. (March 22, 2017) What the Public Knows About Cyber security. Retrieved April 16, 2017, from http://www.pewinternet. org/2017/03/22/what-the-public-knows-about-/

[10] Robertson, I., Steel, I. (2006, February 23). Evolution of triage systems. Retrieved April 30, 2017, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2564046/

[11] Schwan, Stephan (2004). "The cognitive benefits of interactive videos: learning to tie nautical knots". Learning and instruction (0959-4752), 14 (3), p. 293.

[12] Security Awareness Training. (2016). Information Security Training for System Administrators and Managers. Retrieved April 30, 2017, from http://www.securityawarenesstraining.com/information- security-training

[13] SecureWorld. (2016). Kansas City, KS 2017. Retrieved April 30, 2017, from https://events.secureworldexpo.com/details/kansas-city- ks-2017/

[14] SecurityWeek. About the ICS Cyber Security Conference. (2017). Retrieved April 30, 2017, from http://www.icsconference.com/about-ics/

[15] Shackelford, Scott and Russell, Scott and Haut, Jeffrey, (December 10, 2015). Bottoms Up: A Comparison of Voluntary Cyber security Frameworks. UC Davis Business Law Journal, 2016, Forthcoming; Kelley School of Business Research Paper No. 16-2. Available at SSRN: https://ssrn.com/abstract=2702039

[16] Toth, P., & Klein, P. (2014). National Institute of Standards and Technology (3rd ed., pp. 10-160, Tech. No. NIST Special Publication 800-16). Gaithersburg, MD: National Institution of Standards and Technology.

[17]Undergraduate Student Presentation, 2017

[18] United States, Department of Homeland Security. (2017, January 27). National Cyber security Awareness Campaign Undergraduate Student Presentation. Retrieved April 26, 2017, from https://www.dhs.gov/sites/default/files/publications/Und ergraduate%20Student%20Presentation.pdf