Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Online Information Security Education through Anchored Instruction

Eric Imsand[1], Larry Howard[2], Ken Pence[2], Mike Byers[3], Dipankar Dasgupta[1]

[1]Center for Information Assurance
University of Memphis
Memphis, TN 38138

[2]Institute for Software Integrated Systems
Vanderbilt University
Nashville, TN 37235

[3]SPARTA Inc
401 Diamond Drive
Huntsville, AL 35806

Abstract – The Internet is unquestionably the most extensive and accessible resource for information and commerce in history. But it is also providing a medium for new forms of crime, espionage, and even terror, targeting organizations and individuals alike. Broad awareness of vulnerabilities and defenses is needed to protect against all types of cyber attacks. While online learning environments provide a great opportunity to train large numbers of people, they have yet to demonstrate effectiveness in high-stakes situations. In an effort to better prepare cyberspace defenders, we are developing a multidisciplinary training program that encompasses topics from computer science, management information systems, and legal and ethical studies, using state-of-the-art online learning methods and technology. This paper describes the Adaptive Cyber-security Training (ACT) Online program, giving details of its targeted training population, curriculum, and instructional design strategy. We further report pilot testing results from two recently developed courses that show significant learning gains following this cyber security training.

Index terms – Cyber Security, Cyber Ethics, Information Security Basics, Online Training, STAR Legacy cycle.

I. INTRODUCTION

As recent cyber-incidents have demonstrated, cyber-attacks of the future will likely be decentralized and multi-faceted, causing major damage to critical information infrastructures. Computer users, from novices to the knowledgeable, are at risk in losing personal information, and may also inadvertently play roles in such attacks. Online training offers unique opportunity in broadening cyber awareness and ensuring sound security practices. Such training needs to be user-centric to achieve learning effectiveness.

The University of Memphis, in collaboration with the Vanderbilt University and SPARTA Incorporated, is developing a multidisciplinary program (ACT Online). It boasts innovations in both training delivery and evaluation, creating online cyber security courses that are *rigorous*, *engaging*, and *adaptable*. When fully deployed, ACT Online will be a comprehensive, multi-level training program offering courses at introductory, intermediate and advanced levels for people who use, develop and maintain computer networks and information systems. In particular, training is directed to federal, state and local responders, IT managers who administer computer systems, criminal investigators of cyber crimes involving terrorism, and others responsible for the protection of critical information systems.

The ACT system employs dynamic, interactive, scenario-based training modules to prepare students to deal with a wide variety of security challenges. The capability of ACT system allows training to be individualized for the user's current skill level, using advanced instructional design and standards-based online learning technologies. The training objectives of the program include:

1. Provide a working knowledge of cyber security technologies (e.g., encryption, authentication, intrusion detection, firewalls, etc.) and "best practices" (e.g., effective security mechanisms and policies) from theoretical, design, and operational standpoints.
2. Provide detailed training in security-specific hardware, software, and methodologies. Educate students on ethical, managerial, policy related and legal issues and requirements in the field of information assurance.
3. Advanced courses provide training in cyber forensics to analyze security risks and respond to emerging, novel cyber attacks.

The goal of this cyber security training program is to prepare Internet users, IT professionals and law enforcement officers to identify, prevent, protect

against, respond to, and recover from cyber attacks at the local, state and federal levels.

We begin the paper with a description of the ACT Online course curriculum and expected release information. Section II discusses the instructional design methodology used in structuring ACT course modules. The next section provides an explanation of the approach to summative assessment and course certification. Section IV reports pilot testing results of first two courses; the final section summarizes the current state of this training program.

II. ACT Online Curriculum

ACT Online curriculum is a comprehensive multidisciplinary three-track training program (tracks in target capabilities) with three different courses for each track, where each course consists of 5-7 modules. Contents of each of the courses are the equivalent of a 12-15 hour-length college course. Table 1 shows the proposed courses in three training tracks, where each track has courses covering introductory to advanced level of content.

For example, the introductory course in general track addresses the security needs of (non-IT/non-manager) individuals who use computers and the Internet with little or no prior security knowledge. It covers a high-level description of security topics that regular users can relate to their daily computer use so that they can understand why they need to know, and can follow easily.

III. Instructional Design Methods

A. Motivation

Online learning represents a potentially cost-effective training method to reach large populations, but this economy is only important for high-stakes training situations if the training itself is also effective. In selecting approaches to training and assessment for ACT Online, we were confronted with two different, but equally ineffective, prevailing approaches to learning via the World Wide Web.

The first, employed by traditional schoolhouse educators, views the web as merely an extension of the existing learning environments. So what we find are pod-casted lectures with slides and notes, or online homework systems with grading and perhaps in-place diagnosis and remediation, supported by chat and discussion forums. The second, employed by the computer-based training community, with its roots in the CD-ROM era, provides click-through "tell and test" modules in which the trainee does little more than advance to the next page, and whose assessments confirm little more than immediate recall. Like the simple ports of experiences by the academic community, these artifacts are not at all like the web. Their instructivist pedagogy is also not consistent with what the modern learning sciences tell us about how people learn and about effective learning environments [1].

The high-stakes training situation of confronting cyber threats motivated the rejection of both of these "models" of online learning in favor of something more engaging and indigenous to the web.

Level / Track	Cyber Security - Technical (Track 1)	Cyber Security - General (Track 2)	Cyber Security - Business Continuity (Track 3)
Beginner/Introductory	*Information Security Basics* (Pilot Tested)	*Information Security for Everyone* (Q3- 2008)	*Business Information Continuity* (Q3- 2008)
Intermediate	*Secure Software and Security Administration* (Q4-2008)	*Cyber Ethics* (Pilot Tested)	*Risk Management in Information Security* (Q3- 2008)
Advanced	Digital Forensics (Q1-2008)	*Cyber Law and White Collar Crime* (Q3-2009)	*Cyber Incident Analysis and Response* (Q1-2009)

Table 1: ACT Course Catalog and Availability

The modern web experience centers on "browsing" and "searching", and is exclusively directed by the trainee. Yet fashioning learning experiences entirely in this way would provide too little structure to make trainees efficient and keep them "on track". So the challenge in designing ACT Online learning experiences was to preserve the trainee's freedom of action, keeping the experiences like the web, while providing enough structure and scaffolds to keep trainees efficient.

B. Modular Design

Courses in the Adaptive Cyber-security Training (ACT) Online series are made up of modules whose designs are based on a paradigm for technology-based learning called *anchored instruction*, developed by John Bransford and the Cognition and Technology Group at Vanderbilt (CTGV) in the early 1990s [2]. Anchored instruction shares similarities with problem-based, project-based, and inquiry-based learning as well as discovery learning. Insufficient scaffolding, often cited as a criticism of constructivist learning approaches, is addressed in ACT Online through the use of an explicit learning cycle called STAR (Software Technology for Action and Reflection) Legacy, developed by Daniel Schwartz and others in the CGTV in the later 1990s. Anchored instruction and STAR Legacy reflect an extensive body of learning sciences research by the CGTV and others [3].

C. The STAR Legacy Cycle

Anchored instruction emphasizes grounding learning experiences on authentic problem-solving situations, thereby contributing to learner motivation and providing a "macro-context" for combining sets of complementary learning activities (Figure 1).

Figure 1: The STAR Legacy Cycle

In ACT Online modules, the STAR Legacy Cycle begins by presenting a challenge drawn from real-world situations or cases related to cyber-security or cyber terrorism. Then the cycle incorporates a set of learning activities centered on the challenge:

1. In the *Thoughts* phase, learners explore salient features and issues involved in the challenge by considering a set of probing questions. This activity helps scaffold the inquiry supported by other cycle phases by helping learners recognize what they will need to know to address the challenge.
2. In the *Resources* phase, learners can access multiple learning resources that address various aspects of the challenge. A second tenet of anchored instruction is that learners should be granted freedom to explore such resources.
3. In the *Assessment* phase, learners are provided an opportunity to confirm their understanding of materials presented in *Resources* using formative assessment questions with progressive remediation.
4. In the *Wrap Up* phase, learners synthesize what they have learned *vis-à-vis* the challenge by returning to the questions posed earlier in *Thoughts*. They are further asked to consider applying what they have learned to a similar situation as a means of addressing knowledge and skills transfer.

D. Example of ACT Online Scenario

To illustrate the scenario driven nature of an ACT Online module, an example of the *Challenge* and *Thoughts* sections are provided from the "Freedom of Speech" module in the Cyber Ethics course:

Challenge: "Communication over the Internet has become increasingly known for its abrasive and extreme content and tone. It is not uncommon to read postings on message boards in which one writer will openly discuss or recommend the possibility of another writer suffering physical harm. Such was the case of Kathy Sierra, a technology writer and popular blogger. Following a technology column she wrote, several people posted comments on message boards indicating

that Kathy should be murdered and physically assaulted for her writings."

Thoughts: *Were the writings advocating Kathy Sierra's physical harm protected by free speech?*
Would these statements be examples of defamation?
Could these statements be classified as hate speech?
Can software filters be used as a form of defense in this case?
Could the comments be considered sexist?

The use of the Challenge scenario gives the trainee a real-world situation that hopefully illustrates the need for the training to be provided later in the module. Returning to the example, it can be argued that, devoid of context, most U.S. citizens would favor freedom of speech, even on the Internet. By providing the user with the case of Ms. Sierra, though, the module is able to quickly illustrate why this seemingly straightforward topic is, in reality, anything but.

E. ACT Online Module Content Organization

The content inside of an ACT Online module is organized around the familiar notion of learning objectives. ACT Online modules feature two different types of learning objectives: terminal and enabling. For our purposes, a terminal learning objective (TLO) represents a large scale task that the user should be capable of completing following successful completion of the module and certification exam. An example of a TLO might be, "Following completion of this module, the trainee will be capable of successfully deploying a securely configured network firewall." Enabling learning objectives (ELO) represent smaller tasks that must be mastered if the overall TLO is to be achieved. An example of an ELO might be, "The trainee will be capable of successfully configuring a firewall to filter outbound network traffic except for web and e-mail service."

Each module in an ACT Online course currently features, on average 3-5 TLOs, with 5-8 ELOs comprising each TLO. This yields a total of 15-40 ELOs, or discrete skills, per module. It is interesting to note that this learning objective total represents the conveyance of more skills per module than is ordinarily found in STAR Legacy based training. Future training and analysis may suggest reducing the number of objectives taught per module.

IV. ARCHITECTURE, TESTING AND CERTIFICATION

The ACT Online system became online with the first version of courseware on October 1, 2007. The initial operational capability included the website, registration process, adaptive delivery engine (ADE), and other support capabilities. Unlike some online training platforms, ACT Online can be considered both a certification and training system. To achieve this goal of providing training and certification services, the ACT Online system is divided into two distinct parts: the evaluation system and the training system. The purpose of each system is relatively straightforward.

The evaluation system is tasked with generating examinations designed to test the trainee's mastery of the material. These examinations are constructed by randomly selecting questions from a pre-generated pool. The evaluation system maintains a record of prior student examinations, so as to ensure that a student is not posed the exact same question twice. Furthermore, as will be described in greater detail in this paper, the evaluation system also retains a memory of any modules that have been successfully passed on prior examinations. This allows the evaluation system to avoid the problem of re-testing. Tests generated by the evaluation system are known to be equivalent, though not identical. This equivalency is assured by the manner in which examinations are generated. One question (that the student has not yet seen) for each ELO in the course is pulled randomly from the question pool. The resulting body of questions comprises an examination. This examination is then administered to the student. The use of ELOs as the backbone for generating examinations allows us to be assured that the coverage for each examination is equivalent. Finally, any student that fails to pass the qualifying examination will be placed back into the training system, as shown in Figure 2.

While its internal machinations are extremely complex, the training system serves a rather clear purpose: to serve the actual modules to the trainee in the form of easily navigable web pages. Like the evaluation system, the training system has significant record keeping facilities, allowing it to remember which resources inside of a module the trainee has already seen, as well as which modules the trainee has already fully completed. Because trainees are

allowed to move freely from any point in any module to a point in another module at anytime, this feature becomes an important feature for the trainee. The training system allows them to quickly assess whether or not they have seen a set of material.

Figure 2: ACT Online Evaluation and Training Workflow

A. Pre-Qualification

To permit certification based on prior knowledge and experience, ACT Online begins each course with a comprehensive pre-qualifying examination. The Pre-Qualifying feature of ACT Online gives individuals credit for what they already know, possibly leading the granting of the course certificate and moving to higher level of training. Even an unsuccessful pre-qualifying attempt indicates the trainee's prior knowledge to ACT Online. ACT Online uses this information to adapt the training, so that the trainee is not required to complete portions of the course for which they have already demonstrated mastery. This examination provides exactly the same coverage as that of the qualifying examinations to grant course certificate to trainees, scored and evaluated in exactly the same way.

B. Qualifying Exam

Each qualifying attempt covers all sections (modules) for which the trainee has yet to successfully demonstrate mastery. Qualifying attempts are thus *progressive*. Qualifying attempts offer similar features to the prequalifying attempt in terms of continuous performance feedback, question by-pass, and section opt-out. There is no selective tailoring of qualifying examinations: they always cover all modules for which the trainee has yet to demonstrate mastery through a passing score.

Trainees themselves determine when they are ready to attempt the qualifying examination subsequent to training. While the Evaluation System supports unlimited numbers of such qualifying attempts, ACT Online limits the number of qualifying attempts to five for practical reasons. Upon exhausting the maximum number of given attempts, the trainee is considered as "failed", and ineligible for the course certificate.

V. ACT Courses and Pilot Testing Results

We have released two ACT online courses so far which have gone through rigorous pilot testing and evaluation. The initial training started on October 1, 2007, and continued until February 1, 2008. The descriptions of these courses are:

Information Security Basics (ISB): This course is designed to train entry and mid-level IT workers on the fundamentals of information security [4-6]. There are six modules, covering topics such as

- An Introduction to Information Security
- General Concepts,
- TCP/IP Networking,
- Network Security,
- Operating System Security
- Cryptography.

One of the long term goals for the ACT Online curriculum is to mirror the CNSS standards as closely as possible. The initial goal of Information Security Basics was to encompass the entire 4013 standard. It became clear, though, that the entire standard constituted too much material for a single web-based course. Consequently, the material included in the final version of Information Security Basics was designed to represent approximately 50% of the 4013 standard, with the remaining 50% of the standard to be offered in a future ACT Online course, still to be developed.

Cyber Ethics (CE): This course is designed to teach students about various ethical issues and dilemmas that are related to Internet usage [4, 7-9]. Like Information Security Basics, Cyber Ethics was also composed of six modules. These modules included:

- Terminology,
- Privacy,
- Intellectual Property,
- Codes of Ethics and Professional Practices,
- Freedom of Speech on the Internet,
- Ethical Hacking.

Unlike Information Security Basics, which was designed to cater to a specific audience, Cyber Ethics was developed to be approachable by all computer users. For this reason, the topics that were covered were chosen because they represented topics which

any computer user would immediately be able to identify with.

A. Pilot Testing Results

Pilot testing helped us to ensure that the ACT training does its job for all those it intends to serve. The evaluation records of pre-qualifying and qualifying attempts on ACT Online provide complete accountings of every question selected, posed, answered, and evaluated, as well as the evaluation results for each section of the examination.

Information Security Basics (ISB): The pilot testing group for this course included 44 testers. Of these, five testers achieved a certifying score on the pre-qualifying examination and 39 received the course certification following the training. Table 2 summarizes the data of trainees who opted-out of the pre-qualifying examination and those who successfully completed the corresponding section of the examination, thereby being excluded from the pre-post analysis.

Table 2: Pre-Qualifying Opt-Outs and Successful Completions by Module of ISB

ISB Pre-Qualifying Results		
Modules	**Opt-Outs**	**Completions**
M1	5	23
M2	8	18
M3	7	12
M4	7	15
M5	7	12
M6	9	18

The pre-test and post-test averages are graphed in Figure 3. The data used in the analysis is charted in Table 3.

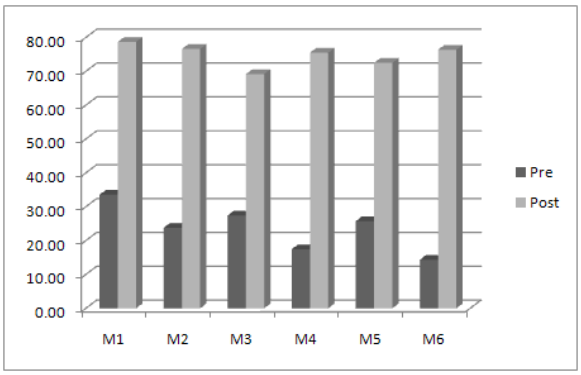

Figure 3: ISB Pre & Post Comparison by Module

The minimum delta is for Module M3 ("TCP/IP Networking") at 41.75 and the maximum delta is for Module M6 ("Cryptography") at 62.06. The aggregate training delta for all of the modules was 51.10 as shown in Table 3. Note that the zero pre-qualifying measures were for trainees that elected to attempt the pre-qualifying examination for a given section, but who scored zero, typically by opting-out once they saw the questions.

Cyber Ethics: The pilot testing group for this course included 31 testers. Of these, two testers achieved a certifying score on the pre-qualifying examination, 28 received the course certification after the training, and one failed the course after three attempts to qualify. Table 4 summarizes the trainees who opted-out of the pre-qualifying examination and those who successfully completed the corresponding section of the examination, thereby being excluded from the pre-post analysis.

Table 3: Information Security Basics Training Data Analysis

	Pre-Test				**Post-Test**				
Modules	**Count**	**Min**	**Average**	**Max**	**Count**	**Min**	**Average**	**Max**	**Delta**
M1	16	0	33.56	59	21	65	78.71	90	45.15
M2	18	0	23.78	57	26	62	76.62	95	52.84
M3	25	0	27.44	59	32	60	69.19	83	41.75
M4	22	0	17.45	58	29	60	75.52	100	58.06
M5	25	0	25.76	57	32	60	72.50	95	46.74
M6	17	0	14.35	58	26	60	76.38	93	62.03
			23.72				74.82		51.10

Table 4: Pre-Qualifying Opt-Outs and Successful Completions by Module

CE Pre-Qualifying		
Modules	**Opt-Outs**	**Completions**
M1	5	9
M2	5	5
M3	7	9
M4	4	11
M5	5	13
M6	3	15

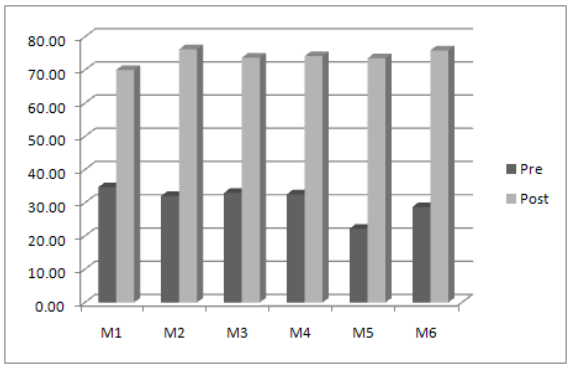

Figure 4: CE Pre & Post Comparison by Module

This data suggest that all trainees tend to attempt the pre-qualifying examination. No special instruction regarding pre-qualification was given to the pilot testers. The CE pre-test and post-test averages are graphed in Figure 4.

The minimum delta is for Module M1 ("Cyber Ethics Terminology and Introduction") at 35.34 and the maximum delta is for Module M5 ("Freedom of Speech on the Internet") at 51.32. The aggregate training delta for all of the modules was 43.39. The data used in the analysis is charted in Table 5 below.

VI. Summary

In this paper, we have described the Adaptive Cyber-security Training Online program, a scenario-based, online cyber-security training program. ACT Online fully utilized the STAR Legacy cycle to cyber-security education. This scenario-based training model has been found to be well suited for online cyber-security education.

We have presented the results of two different training experiments demonstrating the effectiveness of our approach. These experiments assessed the improvement in demonstrable knowledge in two different courses: Information Security Basics and Cyber Ethics. Our analysis found that the 28 students completing our Cyber Ethics course improved by an average of 43.39%. More over, the 39 trainees that completed our Information Security Basics course demonstrated a 51.10% improvement in their performance on the final certification exam.

The ACT system supports both the certification and training assessment. Adaptation and randomization are used extensively in the system to ensure the uniqueness of examinations. Features of both pre-qualifying and qualifying examinations provide enlarged scope, robust result summaries and question-level response feedback. The system creates highly detailed records of the evaluation process, enabling analysis of effectiveness.

Table 5: Analysis of Training Data for Cyber Ethics Course

	Pre-Test				Post-Test				
Modules	**Count**	**Min**	**Average**	**Max**	**Count**	**Min**	**Average**	**Max**	**Delta**
M1	17	4	34.71	52	22	48	70.05	85	35.34
M2	21	0	32.10	59	26	42	76.23	92	44.14
M3	15	0	33.00	57	22	31	73.73	90	40.73
M4	16	0	32.56	59	20	59	74.20	93	41.64
M5	13	0	22.23	56	18	60	73.56	88	51.32
M6	13	0	28.77	59	16	61	75.94	88	47.17
			30.56				73.95		43.39

The courses and experiments described here represent only the initial offerings of what is designed to be a nine course cyber-security curriculum targeting users with differing cyber-security needs and at differing levels of proficiency. The ultimate goal of ACT Online is to provide cyber-security training to a large number of computer users, thereby reducing this country's exposure to threats against our national information infrastructure.

We have a number of courses at different stages of development and testing. The details of this training program are available at *www.act-online.net.*

VII. ACKNOWLEDGEMENTS

This work is supported by Cooperative Agreement (Number 2006-GT-T6-K009) administered by the Federal Emergency Management Agency, National Preparedness Directorate, National Integration Center, Training and Exercise Integration. Points of view and opinions on this paper are those of the author(s) and do not necessarily represent the position or policies of the United States. Authors would like to thank Barry Bratburd, Program Manager, Section Chief National Preparedness Directorate (DHS/FEMA) for his support and helpful suggestions. They also acknowledge the valuable contributions of other members of the ACT Online project.

VIII. REFERENCES

[1] Bransford, J. D., Brown, A. L., & Cocking, R. R. (Eds.). (1999). How people learn: Brain, mind, experience, and school. Washington, DC: National Academy Press

[2] Bransford, J. D., et al. (1990) "Anchored instruction: Why we need it and how technology can help". In D. Nix & R. Sprio (Eds), *Cognition, education and multimedia*. Hillsdale, NJ: Erlbaum Associates.

[3] Schwartz, D. L., Lin, X., Brophy, S., & Bransford, J. D. (1999). Toward the development of flexibly adaptive instructional designs. In C. Reigeluth (Ed.), Instructional-design theories and models: New paradigms of instructional theory: Vol. 2 (pp. 183-213). Mahwah, NJ: Erlbaum

[4] Pfleeger, C., Pfleeger, S. "Security in Computing, 3rd Edition". 2002. Prentice Hall PTR. ISBN 0130355488

[5] Conklin, W., White, G., Cothren, C., Williams, D., Davis, R., Conklin, A., White, G., Davis, R. "Principles of Computer Security: Security+ and Beyond", 2004. Career Education. ISBN 0072255099.

[6] Tanenbaum, A. "Computer Networks, 4th Edition". 2003. Prentice Hall PTR, Upper Saddle River, NJ, United States of America. ISBN 0-13-066102-3.

[7] Tavani, H. "Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology". 2004. John Wiley and Sons, Inc., United States of America. ISBN 0-471-24966-1.

[8] Reynolds, G. "Ethics in Information Technology, 2nd Edition". 2007. Thomson Course Technology, Boston, Ma, United States of America. ISBN 1-4188-3631-1.

[9] Tavani, H., Spinello, R. (Eds) "Readings in Cyber Ethics, 2nd Edition". 2004. Jones and Bartlett Publishers, Inc. Sudbury, Ma, United States of America. ISBN 0-7637-2410-6.