Cyber Security Training and Awareness Through Game Play

Benjamin D. Cone, Michael F. Thompson, Cynthia E. Irvine, and
Thuy D. Nguyen

Naval Postgraduate School, Monterey, CA 93943, USA
{bdcone,mfthomps,irvine,tdnguyen}@nps.edu

Abstract. Although many of the concepts included in staff cyber-security awareness training are universal, such training often must be tailored to address the policies and requirements of a particular organization. In addition, many forms of training fail because they are rote and do not require users to think about and apply security concepts. A flexible, highly interactive video game, CyberCIEGE, is described as a security awareness tool that can support organizational security training objectives while engaging typical users in an engaging security adventure.[1]

1 Introduction

Effective user security awareness training can greatly enhance the information assurance posture of an organization. [1] Yet holding a trainees attention sufficiently long to impart a message is a considerable challenge, particularly when the training is mandated and the topic is viewed by the target audience as potentially mundane. Video games have been proposed as an engaging training vehicle. [2] This paper describes how a video game-like tool called CyberCIEGE was employed to develop security awareness training targeted for the requirements of a specific organization, and how this extensible tool can offer training and education for a range of target audiences.

Our study centers on cyber security training for uniformed and civilian personnel associated with the U.S. Navy. We describe how two CyberCIEGE scenarios, one for general awareness and the other for IT personnel, were created to fulfill organizational information assurance training and awareness requirements.

2 Background

The United States Computer Security Act of 1987 mandated periodic security training for all users of federal information systems. In response, the Department of the Navy placed the burden of responsibility for training and awareness on

[1] This work was funded in part by the Office of Naval Research.Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

local Information Systems Security Managers [10], who were, in turn, responsible for developing local training sessions or computer-based training (CBT). To supplement other IA directives [3, 4], in 2004, the U.S. Department of Defense (DOD) issued DOD Directive 8570.1 [5], which mandated initial and annual refresher information assurance training for all DOD information system users. Since then, all users of Navy information systems have been instructed to complete a DOD IA awareness CBT. The CBT is a web-enabled slide presentation. It is trivial for personnel to click through the training to its successful completion without absorbing any of the material.

Directive 8750.1 has highlighted the importance of fostering a security culture and the need to find training techniques that will actively engage the typical user. A participatory video game requires more user involvement than slide presentations or other standard training and awareness vehicles.

2.1 Common Current Training and Awareness Techniques

Training and awareness is generally accomplished using one of a combination of several techniques described below.

Formal Training Sessions can be instructor-led, brown-bag seminars, or video sessions. Formal training in sessions facilitated by local information security personnel represents the traditional approach to user training and awareness within the Department of the Navy. The success of this approach depends upon the ability of the training facilitator to engage the audience.

Passive computer-based and web-based training represents a centralized approach to the training and awareness problem. CBT offers the user the flexibility of self-paced training, and provides the organization with the ability to train users to an enterprise-wide standard. Its disadvantage is that training and awareness becomes a monotonous slide show that fails to challenge the user and provides no dialogue for further elaboration. Often, users attempt to complete CBT sessions with minimal time or thought. The CBT developer must attempt to provide engaging instruction within the constraints of a passive medium.

Strategic placement of awareness messages seeks to raise the level of consciousness through the delivery of messages in the workplace. Some of the more common delivery methods include organizational newsletters and memos, email messages, posters, screen savers, and security labels.

Interactive computer-based training, such as a video game, generally falls into two broad classes: first-person interaction games or resource management simulations. The majority of games fall into the first category and include first-person shooter games where the player is confronted by an adversary or problem and must take an appropriate action or is penalized, sometimes severely. In contrast, resource management games require the player to manage a virtual environment using limited resources. The player attempts to make choices that improve the environment within the constraints of the available resources. Good choices result in a richer environment and additional resources. SimCity^{TM}, other "sims" games, and RollerCoaster Tycoon (R) are popular examples of resource management games.

2.2 CyberCIEGE

In 2005, the Naval Postgraduate School released a U.S. government version of CyberCIEGE, a video game intended to support education and training in computer and network security. Simultaneously, our collaborators at Rivermind, Inc. made a version available to non-government organizations. The game employs resource management and simulation to illustrate information assurance concepts for education and training. [6, 7] In the CyberCIEGE virtual world, players construct and configure the computer networks necessary to allow virtual users to be productive and achieve goals to further the success of the enterprise. Players operate and defend their networks, and can watch the consequences of their choices, while under attack by hackers, vandals and potentially well-motivated professionals.

CyberCIEGE Components. The building blocks of CyberCIEGE consist of several elements: a unique simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video-enhanced encyclopedia. [8] CyberCIEGE is intended to be extensible in that new CyberCIEGE scenarios tailored to specific audiences and topics are easily created. [9]

The scenario definition language expresses security-related risk management trade-offs for different scenarios. The CyberCIEGE simulation engine interprets this scenario definition language and presents the player with the resulting simulation. What the player experiences and the consequences of the player choices are a function of the scenario as expressed using the scenario definition language.

The game engine and the language that feeds it are rich in information assurance concepts so that it is possible to simulate sophisticated environments subject to a variety of threats and vulnerabilities. They also include substantial support for relatively brief, scripted training and awareness scenarios. This support includes cartoon-like balloon speech by the virtual users, message tickers, pop-up quizzes and conditional play of video sequences, e.g., a computer worm.

3 Requirements Analysis

Training and awareness requirements were developed from the legacy Information Security program of the U.S. Navy and from the current Department of Defense IA training and awareness computer-based training course.

Many of the requirements for the awareness scenario were obtained from the U.S. Navy Information Security Program. Navy requirements for user security training are found in the Navy INFOSEC program guidebooks for local Information System Security Officers [11] and Network Security Officers [12]. These documents offer recommended training curriculum topics and subtopics.

- Value of information, e.g., personnel files, legal records, and trade secrets.
- Communication and Computer vulnerabilities such as malicious software, internet risks, human errors, and internet security risks.

- Basic safe computing practices such as locking computers when unattended.
- Password management including password generation, protection, and change frequency.
- Local security procedures, e.g., cipher locks and violation reports.

The other requirements source was the DOD Information Assurance Awareness CBT. The majority of naval organizations currently use the “DOD Information Assurance Awareness” CBT [13] to fulfill obligations for enterprise-wide annual refresher training. It addresses the following topic areas:

- Importance of IA (overview, evolution, and policy)
- IA Threats (threats, vulnerabilities, social engineering, and internet security)
- Malicious Code (overview, protection, and internet hoaxes)
- User Roles (system security and protecting DOD information)
- Personal and Home security (online transactions and security tips)

These topics provided the requirements for the video game-based training and awareness.

4 Scenarios for Training and Awareness

Two CyberCIEGE scenarios were designed to fulfill the Navy IA training requirements. The first seeks to make the player aware of basic IA problems and principles. The second is intended is for more sophisticated users of computer-based assets. An brief summary of other CyberCIEGE awareness and training scenarios is provided in Section 4.2.

The basic user scenario focuses on computer security fundamentals. The player is placed in the role of a security decision maker aboard a ship, who must complete objectives that raise the security posture of the organization. If objectives are not completed within a specified time, appropriate attacks are triggered by the game engine and the player is penalized. After completing each objective, the player is presented with an awareness message that relates the action taken in the game with real-life circumstances and provides feedback regarding the players choices. The player wins by completing all the objectives without incurring “fatal” penalties.

For each topic identified in the requirements analysis, a scenario element was created that requires the player to do something that will convey the concept to be learned. Some of the topics and activities are described in Table 1. Features that made this scenario Navy-specific included the protection of classified information and cultural aspects of organizational security associated with the hierarchical command structure of the DOD.

4.1 Scenarios for IT Staff

Navy IT training requirements for staff with IT-related jobs are addressed by a second scenario that focuses on network security, and serves to introduce technical users into the roles they must assume. The player assumes the role of acting

Table 1. Basic Awareness Topics and Player Activities

Topic	Player Activity
Introductory IA briefing	This briefing includes definitions and descriptions of important IA elements and how they interact.
Information value	The user must protect high value information and answer questions about information dissemination.
Access control mechanisms	The player is introduced to both mandatory and discretionary access control, with the latter as a supplement to controls on classified information.
Social engineering	The player is presented with a scenario that will lead to a social engineering attack if proper action is not taken.
Password management	The player must prevent a game character from revealing his password to an outside contractor.
Malicious software and basic safe computing	The player must determine and expend resources to procure three procedural settings that will prevent malicious software propagation.
Safeguarding data	The player is presented with a situation where it appears that a game character is leaving the premises with sensitive information. Actions taken by the player allow the importance of secure storage of backups to be conveyed.
Physical security mechanisms	The player must select cost-effective physical security mechanisms to prevent unauthorized entry into sensitive areas.

security manager while the "boss" is away. The player must manage three internal networks, one of which processes classified information. During this scenario, the player must complete technical objectives addressing physical security mechanisms, access control, filtering, antivirus protection, data backups, patching configurations, password policies, and network vulnerability assessment.

4.2 Other Scenarios

The rich and flexible CyberCIEGE scenario definition language supports information assurance training beyond military environments. For example, an identity theft scenario was built to teach users about methods of identity theft prevention in home computing environments. [14] This scenario focuses on a few basic user behaviors that can greatly reduce the risk of identity theft, while highlighting consequences of risky behavior through an engaging story line.

One set of scenarios was developed solely to help train users to reduce the risks of distributing worms and viruses. Here, the player can see the damaging effects of worms and viruses, and learns that a major cause of malicious software proliferation is through user execution of email attachments.

Other CyberCIEGE scenarios illustrate more complex and subtle information assurance concepts. These longer, more sophisticated scenarios are more like traditional simulation and resource management games. For these, the target audience may be advanced computer security students, or information security decision makers.

5 Discussion and Conclusion

This paper demonstrates that information assurance awareness and training can be provided in an engaging format. CyberCIEGE was employed to meet a specific set of Navy IA training requirements, thus demonstrating that it is sufficiently flexible to illustrate a range of security topics in a variety of environments, both generic and organization-specific. Initial test results for the basic user training scenario are positive and illustrate the utility of CyberCIEGE in supporting awareness programs.

References

1. National Institute of Standards and Technology, People: An Important Asset in Computer Security, NIST-CSL Bulletin, October 1993.
2. Prenski, M., Digital Game-Based Learning. New York: McGraw-Hill, 2001.
3. DoD Directive 8500.1, Information Assurance. October 24, 2002.
4. DoD Instruction 8500.2, Information Assurance (IA) Implementation. February 6, 2003.
5. DoD Directive 8570.1, Information Assurance Training, Certification, and Workforce Management. August 15, 2004.
6. Irvine, C.E., and Thompson, M.F.: Teaching Objectives of a Simulation Game for Computer Security. Proc. Informing Science and Information Technology Joint Conference, Pori, Finland, June 2003, pp. 779-791.
7. Irvine, C.E. and Thompson, M.F.: Expressing an Information Security Policy Within a Security Simulation Game, Proc. of the 6th Workshop on Education in Computer Security, Naval Postgraduate School, Monterey, CA, July 2004, pp. 43-49.
8. Irvine, C.E., Thompson, M.F.: and Allen, K., CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness.Federal Information Systems Security Educators' Association Conference, North Bethesda, MD, March, 2005.
9. Irvine, C. E., Thompson, M. F.: and Allen, K., CyberCIEGE: An Extensible Tool for Information Assurance Education. Proc. 9th Colloquium for Information Systems Security Education, Atlanta, GA, June 2005, pp. 130-138.
10. Navy Staff Office Pub. 5239-04, Information Systems Security Manager (ISSM) Guidebook. September 1995.
11. Navy Staff Office Pub. 5239-07, Information Systems Security Officer (ISSO) Guidebook. February, 1996.
12. Navy Staff Office Pub. 5239-08, Network Security Officer (NSO) Guidebook. March, 1996.
13. DOD Information Assurance Awareness CBT Version 2.0. December 2004.
14. Ruppar, C., Identity Theft Prevention in CyberCIEGE, Masters Thesis, Naval Postgraduate School, Monterey, CA, December 2005.