Proceedings of the 2012 IEEE International Conference on
Cyber Technology in Automation, Control and Intelligent Systems
May 27-31, 2012, Bangkok, Thailand

Exploring Game Design for Cybersecurity Training

Ajay Nagarajan, Jan M. Allbeck and Arun Sood
International Cyber Center
George Mason University
Fairfax, VA, USA
{anagara1, jallbeck, asood}@gmu.edu

Terry L. Janssen
Cyber Defense, Intelligence and Operations
SAIC
Columbia, MD
terry.l.janssen@saic.com

***Abstract*—Cybersecurity awareness and cyber skills training are vitally important and challenging. A huge number of attacks against everyday users occur routinely. Prevention techniques and responses are wide ranging but are only effective if used effectively. The objective of this research is to teach everyday users the requisite cybersecurity skills through gaming, beyond the current state of practice. Because the skill level of the trainees is also wide ranging, from causal computer users to software engineers to system administrators to managers, the games must also be capable of training this wide range of computer users. Computer games can provide a media for delivering training in an engaging format at levels appropriate for the individual trainees. In this paper we (1) describe the state of practice by describing the gaming tool used in most cyber challenges at high schools and colleges in the U.S, i.e., the cybersecurity gaming tool CyberNEXS™ (Science Applications International Corporation), (2) outline some of the additional topics that should be addressed in cybersecurity training and (3) note some other approaches to game design that might prove useful for future cybersecurity training game development beyond CyberNEXS.**

Keywords: cybersecurity; cyber defense; cyberwar game modeling and simulation; training; gaming; game design.

I. INTRODUCTION

Cybersecurity training is becoming more and more vital to global security. The large number of network intrusions and malicious attacks that have taken place over the past several years only reassures the growing need. Some of these events include the following: massive data breaches of consumer information at Sony and Sony PSN [1]; Stuxnet worm's stealthy attack on the Iranian nuclear program [2] and the Chinese electronic break-in at Google [3].

Intrusions are becoming more and more accepted as a norm. Ever increasing bandwidths, the phenomenon of social networking and the accessibility of mobile devices are part of the reason for this growing cyber attack problem. Given that cybersecurity is a real and near threat, it demands comprehensive training in a variety of areas. Games can help here by providing an engaging interface that enhances training, draws more trainees in and simulates a variety of scenarios.

The idea of using games to support health, education, management and other sectors have already yielded positive results [4]. The application of gaming concepts to training can also be equally fruitful. Furthermore, research is advancing in modeling and simulation that seems potentially applicable to cybersecurity and defense (cyber war) gaming [5].

II. CYBERSECURITY TRAINING

A. *Cybersecurity training topics*

The goal is to train the current generation to retool today's workforce and next generation to instill the skills necessary to attain the highest achievable level of cybersecurity and defense against cyber attacks. Defending against cyber attacks in near-real time is highly stressful. Typically, higher user stress levels lead to more user errors. The game design should put the player in a range of stress levels, thus enabling the user to function more effectively in real life.

Password usage and management – In today's world, passwords protect your computers, data and online accounts. Hackers are becoming increasingly sophisticated at cracking passwords using techniques like brute force attacks, dictionary-based attacks and phishing. It is therefore important to create awareness about making strong passwords the first line of defense. Techniques for creating, using and frequently changing strong passwords can be presented.

Protection from malware and spam – A recent New York Times report [6] quotes the Microsoft Internet Safety Enforcement team: the "mean time to infection of an unprotected computer on the internet is less than 5 minutes." Viruses, worms and Trojans are the most common forms of infection and are designed to inflict loss of productivity / economic damage to the target. According to a study conducted by Ferris Research, the annual worldwide economic damages from malware exceeded $130 billion in 2009. Therefore, any effective cybersecurity skills training session must cover the use of anti-virus / anti-malware tools along with training on scanning and updating definitions.

Patch management – Patches are additional pieces of code developed to address problems in software post-release. They enable additional functionality or fix security flaws within the software. These security flaws / vulnerabilities can be exploited if left unpatched, thereby making your system open to compromise. Timely patching of security issues is critical to maintaining service / operational availability, confidentiality and integrity of the system. New patches are released on a daily basis, and it often becomes difficult even for experienced system administrators to keep track of all important patches.

978-1-4673-1421-3/12/$31.00 © 2012 IEEE

Training on effective patch management should hence form an important part of the cybersecurity skills training program.

Social engineering phishing techniques – Phishing-based social engineering is an attack on human judgment as opposed to software vulnerabilities; they pose a threat to unsuspecting users and are a form of electronic deception. As more and more users continue to access the Internet daily, they become more susceptible to phishing. Social engineering is evolving so rapidly that security policies alone cannot protect critical infrastructures anymore. Even with rigid safeguards, hackers manipulate employees using social engineering phishing techniques into compromising personal, social security and other sensitive information. Hence, it becomes important to develop a security-aware culture that keeps users / employees abreast of the latest security threats. This can only be achieved through periodic and routine cybersecurity training programs.

Some of the other cyber-security training topics that need to be presented are

- Methods to monitor and measure compliance and developing specifications to ensure compliance with security requirements .
- How to handle e-mails / attachments from unknown senders and SPAM. Malicious emails coming from recognizable emails are a particular challenge.
- Implementation of new technology.
- Monitoring allowed and prohibited web usage – evaluating a system's compliance with IT security requirements.
- Data backup and storage procedures – do's and do not's
- Incident response procedures and trigger points
- Implications of shoulder surfing
- Use of personal system/ software in work environment
- Creating, editing and managing changes to host / network access control lists – take into consideration issues like separation of duties, least privilege, privilege escalation, etc..
- Individual responsibility and accountability
- Physical access to spaces based on work demands, and
- Incentive schemes such as prizes for good security hygiene and penalties for bad security hygiene.

Note: The NIST NICE Cyber-security Workforce Framework [11] emphasizes on skills training for technical security positions over basic cybersecurity awareness. In this research we are influenced by NICE and also by the need for tools to constantly update the skill levels of computer users in the workplace.

B. Existing Training

A number of techniques exist to get cybersecurity training material disseminated through an agency. The technique chosen depends on resources available and also the type of cybersecurity message that is being sent out. Some of the most common techniques used are

- Web-based session – virtual classrooms
- Computer-based sessions – computer labs or CD-ROMs
- Teleconferencing sessions
- Instructor-led sessions
- IT security days, Cybersecurity Week and similar events
- Posters with do's and do not's list
- Screensaver and warning banner / messages
- Periodic newsletters
- Agency wide e-mail messages / alerts
- "Brown bag" seminars, and
- Awards / incentives program.

Shortcomings of the current techniques are as follows [7, 8]

- Thirty minutes of information about why security is important is not going to change how users behave daily. It should be a continuous process. Most of the training programs now happen to be once a year events. Users cannot be expected to retain the information from this session and change their daily behavior. Cybersecurity skills training must be a continuous life cycle where users must be trained updated and reinforced periodically. A user's retention capacity must be taken into account.
- Too many topics discussed in too little time – users cannot be expected to understand / retain all of them.
- Training environments are usually not realistic – different stress levels have an impact on how users act.
- Most training programs are presented by security professionals who are bad communicators. Instructor-led training headed by security professionals turn out having long information sessions that end up overwhelming people and not getting the intended point across. These sessions cannot afford to be boring; they must be involving and fun.
- If users make the same mistake a number of times even after training and reinforcement, there has to be some sort of disciplinary action. And similarly, there must be incentives for users with good security hygiene.
- One must be able to perform a measurement of user behavior (some sort of score maybe) before and after training to actually see if the training has had a positive impact. Techniques used in current security skills training programs do not facilitate this. It requires an additional survey to make that determination
- Except for the instructor-led session, most approaches are passive and do not facilitate interaction with the user. Most of the time "the question of why should I be doing this goes unanswered" and
- A successful cybersecurity skills training program must be able to do two things: one is to get and retain the user's attention for a span of time, and two is to communicate the training material to the user effectively in that span of time. Most current techniques are found lacking in achieving both.

This ongoing research is supported by a grant from SAIC.

C. *Interactive Computer-based Training*

To overcome these shortcomings, the use of "Interactive Computer-based" training like video games for cybersecurity skills training is now gaining momentum. Given the current landscape, such games generally fall into two broad classes: [8]

- First-person interaction games – Example: first person games where the user is confronted by an adversary / problem and must take a proper course of action or else is penalized severely and,
- Resource management simulation games – manage a virtual online environment with provided limited resources. Good choices result in a richer environment and additional resources, bad choices result in diminishing resources.

Motivation for the games is either recognition (i.e., if you do well and play fair, you will receive recognition) or certification to enhance your professional career. It is conceivable that cyber games of the future might offer financial or other incentives like prizes for first, second and third places in the competition. In regard to the latter - a high quality, valued certification from a game probably does lead to career growth and the corresponding increased salary.

The primary objective of such games is cyber training. Some of the games teach advanced cyber-defense concepts and penetration testing in addition. Some such existing games are

- CyberProtect® (Carnie, Inc.) – Developed for the U.S. Department of Defense in 1999. It teaches information assurance concepts [8]
- CyberCIEGE – Developed by Naval Postgraduate School in 2005. The game employs resource management and simulation to illustrate information assurance concepts for training and education [8]
- Multiple micro-games by Wombat Security Technologies for cybersecurity awareness and training of US Air force personnel. For Example: "Anti-Phishing Phil™". Wombat is currently developing a dozen more similar micro games
- NetWars – NetWars is an offense-oriented cybersecurity competitiion that is held completely online and made available to high school students as well. It is an online game where the primary objective is to penetrate into systems, gain access to files and provide proof for the same. It is conducted by the SANS Institute and is a player in training and certification of cybersecurity professionals
-
- CyberNEXS – is an emulation game that provides skills development and measurement in offensive, defensive and forensics cyber skills. A brief look at CyberNEXS follows.

CyberNEXS gaming

CyberNEXS is considered somewhat of a de facto standard in cyber-defense competitions due to its wide spread adoption as the cybersecurity training tool and as a game for professional cybersecurity certification. Thousands of students have used CyberNEXS. It has a client-server architecture that provides game access to anyone with Internet access. One such training exercise is the SAIC High School 12-week Cybersecurity e-Learning Pilot, which makes use of the CyberNEXS training platform to educate high school students on advanced cyber-defense techniques. These students have gone on to participate in a number of cyber-defense competitions over the past four ears. Some such notable competitions are the Air Force Association (AFA) Cyber Patriot National High School Cyber Defense Competition, the Maryland Cyber Challenge, the State of Maine High School Competition and the San Diego Mayor's Cyber Cup.

CyberNEXS has five different models of operation: They are

- On-site training
- Remote training
- Certification
- Competition/gaming
- Licensing

Gaming is facilitated through the "competition" model. Here the objective of all 5 gaming modes is to teach cyber defense and penetration testing skills to participants. There are five CyberNEXS gaming modes:

CyberNEXS-CND (Computer Network Defense Centralized) – CyberNEXS-CND is a realistic cyber-defense exercise in which the participants (blue team) are tasked with defending their network while under attack from the red team. Blue team's primary objective is to ensure availability of their critical services and secure their host throughout the duration of the attack. Blue team also has to detect and mitigate red team's attack and communicate its findings to the administrator (white team).

CyberNEXS-CND Lite – This game mode is similar to CyberNEXS-CND. However, here the objective is only to maintain availability of critical services and secure hosts. There is no need to detect or mitigate the incoming attacks from red team. The benefit of this game is that it scales to thousands of simultaneous users for such purposes as qualification rounds and eLearning.

CyberNEXS-Forensics – In this game mode, a series of cyber forensic challenges are given to the participants. The objective of the participants here is to find evidence of intrusions, discover malware, analyze payloads, analyze log and audits and trace attacks back to attackers. It is also important for the participants to effectively communicate all of their findings to the white team.

CyberNEXS-CNA (aka Computer Network Attack or penetration testing) – The objective of this game mode is for the participants to assess a network of computers for vulnerabilities and successfully exploit the vulnerabilities to gain user or administrative control of the system. Participants can use any of the network assessment tools that are at their disposal for this. It is also important to effectively communicate their progress to a "white team," which is basically an observer team.

CyberNEXS-CTF (Capture the Flag) – The Capture the Flag mode is similar to the CTF modes found in first-person shooter / strategy games. There are two parts to this game. First, the participants have to assess a network of computers for vulnerabilities, exploit them and take over a series of target hosts. Secondly, once the hosts are compromised and are under control, the participants are now required to defend these hosts against other incoming attacks while maintaining availability of their critical services.

Although CyberNEXS has been very well received and given great marks, moving forward we want to build on this to develop more games that are even more engaging, entertaining, and educational. Some of the things that we believe can be done to improve on the current de facto standards are

- Motivate participation by creating a broader certification program that could further better employment opportunities; NIST NICE [11] is adopting CyberNEXS.
- Make the game even more scalable and flexible. Present optional game modes where the participant is in full control of the environment, not requiring a white team. This helps the participant understand the working of the network. A well implemented Learning Management System (LMS) could potentially take care of one or both of white team and red team activities. It could facilitate in using self-guided services, delivering personalized content and knowledge reuse, tracking progress of participants on a long-term basis etc.
- In the real world, both the attacker and the defender get to make moves all the time. There is no constraint; this is true of CyberNEXS. Attacker adapts to defender's move and vice versa. Similarly, an expert system or a learning engine could potentially help in a student-system game by the system learning and adapting to the user's moves.

III. COMPUTER GAME DESIGN

When designed well, video games can enthrall players, drawing them into a virtual world, motivating them, and challenging them, and CyberNEXS does this well. Research has also shown that games can support and enhance learning and training [9]. In this section, we will discuss some important elements of game design with enhancing cybersecurity training in mind.

Good game designs focus on the player experience; CyberNEXS does this well also. These games create goals that a player feels motivated to reach and rules that must be followed in pursuit of those goals. They are also formulated to match the knowledge and skill level of their target audience (though it may be a wide range). Furthermore, games designed for education and training must be focused on the training goals. What do you want the player to learn? Do you want them to learn a specific procedure for patching an operating system? Do you want them to learn how to think rationally under stressful conditions? Do you want them to learn the mindset and tools of their combatant? Having a clear understanding of who the player is and what you want them to learn will help you design a game that provides both the player and instructor feedback about the player's progress. One good example for such an initiative is the SAIC High School 12-week Cybersecurity e-Learning Pilot which does a good job addressing these questions with the aid of the CyberNEXS training platform.

There are several approaches to and decompositions of game design that can help jump-start the design process. *Themes* can provide a narrative for the game and begin to immerse the players into an alternate world. This immersion can strengthen the training results [9]. Themes can include a specific story, such as a plumber searching through a Mushroom Kingdom to save a princess (i.e. *Super Mario Bros*® (Nintendo of America Inc.)) or a less specific feel, such as a dark, dangerous world or a fast-paced, cartoon kingdom. When chosen well, themes make the mechanics of a game feel more natural. CyberNEXS makes good use of themes.

In the next couple of sub-sections, we will discuss other breakdowns of game design, including *genres*, *dynamics*, and *core mechanics*.

A. Game Genres

Game genres provide both the designers and players an instant idea about the nature of the game and the type of skills required. It should be noted that games can be a hybrid of multiple genres. Below we review a number of different game genres and their potential applicability to cyber skills training:

1) Action Games

Action games keep the player moving and involved at all times, providing an adrenaline rush. They often include a lot of hand-eye coordination and quick reflexes. First Person Shooters (FPSs), such as "*Quake*® (ID Software LLC.)", fall into this genre. Actions in games of this type are not complex and do not require a lot of deliberation. Applicability Example: In the case of CyberNEXS to fend off the attacker.

2) Role Playing Games (RPGs)

RPGs generally have more developed stories and are played for longer spans of time in more expansive worlds. These games also tend to focus on character growth. As the game progresses, characters obtain more experience, capabilities, and weapons. The outcome of actions in this genre can include an element of chance. Even if the player performs an action perfectly, it could still fail. "*Final Fantasy*® *(Square Co., Ltd.)"* is an example of a game from this genre. A game for cybersecurity training could easily involve the player taking on the role of a system administrator to defend a group of servers that are critical to the future of the country or even a hacker that needs to break into a series of systems to obtain the information needed to save a hostage. As the player's knowledge and skills

increase, the player would be given more sophisticated tools and also bigger challenges to further develop their abilities.

Applicability Example: A game for cybersecurity training could involve the player taking on the role of a system administrator to defend a group of servers that are critical to the future of the country or even a hacker that needs to break into a series of systems to obtain the information needed to save a hostage. As the player's knowledge and skills increase, the player would be given more sophisticated tools and also bigger challenges to further develop their abilities: CyberNEXS emulates a real system and the player is the system administrator patching vulnerabilities as they become apparent from attack.

3) Adventure Games

Adventure games are somewhat similar to RPGs in that they also focus on story, but generally adventure games also include more exploration and a number of puzzles. "*Myst® (Cyan, Inc.)*", for example, involved exploring the world, encountering puzzles, and attempting to solve the puzzles so that additional areas could be explored. Along the way, the player pieces together the story of what has taken place in this world.

Applicability Example: This genre of games might fit quite nicely with training recovery operations after an intrusion has been discovered.

4) Strategy Games

In strategy games, the key is balance. There are at least two opposing teams, each with an equal chance of winning. There may be different units, weapons, resources, and goods available to the opponents, but they must be balanced. In strategy games, there is not a single right way to do things. Multiple strategies can be successfully enacted. There are normally also a series of different missions that lead to a final completion. "*Command and Conquer® (Electronic Arts, Inc.)*" requires players to construct bases, acquire resources, and attempt to conquer opponent bases.

Applicability Example: It is easy to see how this paradigm could be used in cybersecurity training. Players might use different strategies and priorities in defending penetration attacks. If trying to train administrators through better knowledge of a hacker's mind set, players might take on the role of hacker and use different strategies to try to breach a system. We are considering ways to make CyberNEXS into a strategy game; the current version is more tactical in that the players respond to current events to defeat (get a better score than) the opponent.

5) Sports Games

The genre of sports games might seem irrelevant to cybersecurity, but in fact there are possible parallels. Many sports games involve deciding on formations and calling plays. We could imagine training managers to handle security attacks in a similar fashion. What skills should his team have (or what can he afford)? What should each member of the team be doing as an attack progresses? The members of the team could be non-player characters (NPCs) or real players in an asynchronous game.

Applicability Example: In CyberNEXS the player is scored on performance within that time constrained session. This adds a dimension of stress and necessity for effective time/resource management.

6) Fighting Games

Fighting games are simple and direct, but engaging. In fighting games, the action is swift and intense, and the moves are usually easy to learn. "*Tekken® (Namco Bandai Games Inc.)*" and "*Mortal Kombat® (Warner Bros. Enterntainment Inc).*" are examples of fighting games. Opponents battling to deface and restore a web site might fit in this genre.

Applicability Example: CyberNEXS currently does the defense part by making the player close "security holes" (vulnerabilities); we are exploring the remainder to make it into more of a cyber warfare like game. In a next generation of CyberNEX students might play cyber war games to compete for points for defensive blocking, as in the current version, and also for points for penetrating offensive cyber attacks. This could be playing cyber war against the computer or a student, or teams with distinctive cyber warrior type roles.

Casual Games

Casual games tend to be easy to learn and not difficult to master. They include video game versions of card games and board games, as well as games created just for computers, such as "*Tetris® (Tetris Holding LLC.)*". Generally, a player starts a new game each play session as opposed to continuing a mission from their last session.

Applicability Example: Any number of casual games could be designed to help familiarize people with cybersecurity terminology and train them on more rudimentary techniques such as creating secure passwords.

7) Sandbox Games

Finally, in sandbox or God games, there is no preset win condition. A player is provided a variety of building blocks and constructs their virtual life or virtual environment. The game system causes different events to occur that affect (positively or negatively) the player's world. For example, in "*The Sims® (Electronic Arts Inc).*", a player's kitchen might catch on fire or they might be promoted.

Applicability Example: As of the writing of this paper, this is far beyond state-of-practice in the cyber security gaming community; as mentioned above CyberNEXS is a virtual environment contrived by the game designers into a game. No cyber security training gaming environment today provides anywhere near this degree of real-time flexibility to the player, but it might be a worthy goal for the mid to longer-term as cyber security and cyber warfare games make use of virtual reality, artificial intelligence and other user-experience enhancing technologies. In the future cybersecurity players might setup a system, be it a single computer or a large mult-network enterprise, and then engage in the "cyber war" based on their virtual hardware and software configuration .

Simulations

Simulations normally focus on one piece of equipment or activity. The resulting experience can be true to life or

exaggerated. For example, many racing games allow the players to maneuver the vehicles around a course at speeds that would not normally be possible.

Applicability Examples**:** In terms of CyberNEXS, the games begins with a vulnerable emulated network and somewhat realistic network traffic, and the participant must defend against attacks.

Game Dynamics

Game dynamics are a particular pattern of play within a game and are tied to core mechanics, which will be discussed in the next section. They focus the type of actions a player can take.

8) Territorial Acquisition

Territorial acquisition revolves around a limited resource that may or may not be a land mass. The main focus of the game is to acquire as much of the limited resource(s) as possible and strategically control it. "*Risk® (Hasbro, Inc.)"* and some FPSs have the territorial acquisition dynamic. In cybersecurity, the limited resource might be memory, network bandwidth, or entire servers.

9) Prediction

The prediction dynamic is simply prompting the player to guess what will happen and rewarding them if they guess correctly. *Roulette* and *rock-paper-scissors* are examples of prediction games. A training game is unlikely to focus solely on the prediction dynamic, but it does still have a place. For example, guessing the nature of the next attack to try to defend against it.

10) Spatial Reasoning

Spatial reasoning often involves puzzles (e.g., *Tetris*, *tic-tac-toe*, and "*Connect Four® (Hasbro, Inc.)"*). A cyber-security game might include the notion of lining up security elements to form a continuous shield from attacks and strategizing about where the next attack might come from.

11) Survival

The survival dynamic taps into the instinctual need for self-preservation. There is a constant life-and-death struggle that is the focus of the game. Here we could imagine a player becoming a server or router and struggling to survive against constant attacks.

12) Destruction

Every FPS includes the destruction dynamic. With this dynamic, the goal is basically to wreck everything in sight. Consider a game set in a computer, where the player uses different weapons (i.e., security techniques) to destroy various attacks he encounters.

13) Building

Because of their focus on character development, RPGs often have a building dynamic. The main objective of these games is to build a better character or, in the case of the sandbox game "*SimCity™ (Electronic Arts Inc.)"*, a better world. How about a better network or computer system?

14) Collection

The collection dynamic can be found in card games and games known as "platformers" (e.g., collect rings, bolts, gold coins, etc.). In these games, getting the most of a resource is what determines the winner. A cyber-security parallel might involve collecting passwords or other user data.

15) Chasing and Evading

In chasing and evading games, the goal is to capture prey or escape predators. "*Pac-Man®(Namco Ltd.)"* is a good example. In cyber-security, a hacker might be attempting to gain control of a system or data while evading detection.

16) Trading

Trading requires cooperating with others. There are normally multiple kinds of resources that can be exchanged between players. This is common in card games. We could imagine a game where tokens corresponding to security software and techniques are traded. When someone has a full set, their system is secure and they have won the game. This would increase the trainees' skills on cyber-defense and security.

17) Race to the End

The race-to-the-end dynamic has the player or players focusing on getting to a certain location first or learning a technology first. The applications to cybersecurity training are straightforward.

B. Game Mechanics

Game mechanics are essentially the rules of a game. They describe how the game state changes. For example, in "*Monopoly® (Hasbro Inc.)"*, if you land on an un-owned property, then you can buy it.

There are a few common classes of mechanics. The *setup* mechanic is at least one rule describing how the game begins. *Victory conditions* describe how the game is won. Not all games have victory conditions. For example, RPGs tend to have smaller goals along the way, but no explicit victory condition. *Progression of play* mechanics include a description of whether it is a turn-based or real-time game, who goes first and how, and how conflicting, simultaneous actions get resolved. Naturally, *player actions* are also a common class of mechanics. What actions can a player perform and how? What affect do player actions have on the game state? The final class of mechanics is a definition of *game views*. This is a description of exactly what information each player knows about at any given time. Some mechanics might change this view as the game progresses (e.g., lifting the fog of war).

Like game dynamics, these mechanics can help focus a game design and ensure that it is consistent and coherent.

C. Learning and Training Games

In educational games, the goal is to teach a body of knowledge. Before beginning the game design process, there should be a clear outline of exactly what the player should learn from playing the game. The game itself should motivate and reward the players to keep them playing the game and as a consequence acquiring more information or skill. According to Annetta, there are six principles to follow when designing games for education [9]. Players should have a unique *identity*

in the game world. This promotes their getting more emotionally involved in the game and caring about the consequences, which leads to *immersion*. *Immersion* is a heightened sense of presence that leads to the player being more engaged in the content and motivated to succeed. *Interactivity* further involves players in the game world by allowing them to interact with other players or NPCs. *Increased Complexity* keeps players challenged. Game levels can provide a platform for increasing the complexity of content and concepts, keeping players from getting bored. *Informed Teaching* focuses on providing feedback to the instructors. These games should track players' performances and record timings, actions, and mistakes and provide feedback to both the instructors and the players. Finally, educational games should be *instructional*. Players should be able to assimilate the knowledge and skills they are acquiring in the game with their existing knowledge and experiences.

IV. Conclusions and Future Work

Although many of the topics presented as part of the cybersecurity training program are universal, such training must always be tailored to address the needs and security policies of a particular organization. A major shortcoming of most of the current forms of cyber skills training is that they don't require participants to think on their feet and apply security concepts in real time. And although theoretical knowledge of security concepts is important, handling a security event in a stressful environment demands prior hands-on experience. A flexible, scalable and highly interactive video game could help simulate a similar environment for the trainees.

Moving forward, we are in the process of building on this to develop improved cyber games. The goal of our research is to maximum the extent to which these games are engaging, entertaining, and educational. We want to find ways to disseminate this training on the wide spectrum of cybersecurity topics to the wide spectrum of personnel that needs it. This might include causal games that can be played over lunch and remind computer users of security issues they might see every day, and they might include games that are on-going over the course of a typical college term or training event, or longer for very extensive, all-encompassing cybersecurity certifications. It might also include more intense and technical games played by seasoned, highly experienced system administrators to ensure that they have a firm grasp of the needed skills and will remain calm and clear-headed under the stress of persistent attacks.

In summary, in this project we are attempting to conceptualize and design an effective, advanced "cybersecurity training" gaming environment that takes CyberNEXS beyond its many current capabilities. We are doing this from three perspectives or angles: (1) a large number of end-user cyber-training requirements for well-rounded cybersecurity skill and knowledge, as documented in National Initiative for Cybersecurity Education (NICE) [11]; these compared to the current state-of-development cyber games; CyberNEXS already does many of them; (2) innovative ways to use relevant, advanced information technologies like additional modeling and simulation in our next step, and eventually virtual reality and artificial intelligence; and (3) viability as a cost-effective hardware and software cybersecurity training and certification solution, considering factors like cost-benefit in meeting the requirements in No.1 above.

V. References

1. "Sony playstation suffers massive data breach" - Reuters - 04/26/2011
2. "Stuxnet 'hit' Iran Nuclear Plans" - BBC - 11/22/2010
3. "Google says hackers in China stole Gmail passwords"-NYTimes 06/01/2011
4. Prenski M. "Digital game-based learning" New York: McGraw-Hill; 2001.
5. "A robot network seeks to enlist your computer" – NY Times, 10/20/2008
6. Security Awareness – Implementing an effective strategy, SANS Institute InfoSec reading room, 2002
7. Benjamin D. Cone et al "A video game for cyber security training and awareness" Computers and Security 26 (2007)
8. Annetta, L.A. The "I's" Have It: A Framework for Serious Educational Game Design. *Review of General Psychology*, *14* (2). 105-112.
9. Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. A Video Game for Cyber Security Training and Awareness. *Computers and Security*, *26* (1). 63-72.
10. Russell, C. Security Awareness--Implementing an Effective Strategy, SANS Institute InfoSec Reading Room, 2002.
11. Wilson, M. and Hash, J. Building an Information Technology Security Awareness and Training Program, NIST, 2003.
12. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
13. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
14. M. Wilson and John Hash "Building an Information Technology Security Awareness and Training program" NIST, 2003