ENGAGING DIGITAL NATIVES WITH SIMULATIONS IN A BUSINESS DATA SECURITY COURSE

Wendy G. Ford
Queensborough Community College, City University of New York
wford@qcc.cuny.edu

ABSTRACT

To perform effectively, it is important for cyber security professionals to understand an organization's goals and objectives. This paper discusses how CyberCIEGE, a resource management simulation game, was used within a classroom setting to teach students about cyber security principles applied within a business setting. Digital game-based learning, which can be used to motivate and engage digital natives, was introduced into a college information security course and the simulation activities were aligned with Bloom's Revised Taxonomy. The course modification is outlined and quantitative data from the simulation game performance log is analyzed, along with qualitative data from a student survey. Student engagement with the simulation and student perceptions of the simulation are discussed. Findings indicated that while student engagement with the simulation was high and many students liked being able to solve business security problems in a virtual business setting, many students felt that additional help was needed to play the game effectively.

Key Terms: game-based learning, Bloom's Revised Taxonomy, student engagement, busines simulation, cyber security education

INTRODUCTION

Cyber attacks can impact all areas of business operations, which can result in loss of valuable assets, consumer trust, and business continuity. In business, it is important that leadership and key staff members create a culture of security awareness. Today, many organizations have a cyber security budget which includes funding for cyber security education at all levels of the organization. Cyber security is not just the responsibility of the Information Technology department. Based upon a research study conducted by Ponemon, the average cost of a data breach increased 6.4% from 2017 to 2018 to $3.86 million (Ponemon Institute, 2018). Increasing communication between various business units is an important step in helping to ensure that organizations approach cyber threats in an effective way (Phillips & Tanner, 2019; Krishan, 2018).

Communicating across business units can be challenging in an organization. Each business unit has their own subject matter experts, culture, budget, goals, strategies, and challenges which must align with the organization's culture, budget, goals, and strategies. Often time, cyber security professionals will have the required technical expertise that an organization needs but, they may lack insight into the organization's or business unit's goals and objectives.

This paper discusses how a resource management simulation game can be used within a classroom setting to teach students about cyber security principles applied within a business setting.

BUSINESS DATA SECURITY COURSE AND GAME-BASED LEARNING

A digital game-based learning simulation tool was implemented in a 15-week introductory data security course in a Computer Information System (CIS) associate degree program administered through the Business Department of an urban community college. The degree program requires students to take nine business credits, which include Introduction to Business, Accounting 1, and Statistics. In addition, CIS students have the choice to take either Economics 1 or Economics 2 to fulfill a general education requirement. The remaining major program requirements include courses related to computer programming, operating systems, networking, database management, and spreadsheet analysis. The Data Security for Business course is included in the program as an elective option for students. Since the CIS degree is offered through the Business Department, business applications are emphasized throughout all the courses.

The CIS degree provides students with foundational knowledge that can be applied toward a variety of professional and academic pursuits. The Data Security for Business course introduces students to the principles of cybersecurity by using the business environment as the point of reference for learning. Topics covered in the course include: malware, encryption principles, access control, identity management, business continuity, risk mitigation, vulnerability assessment, and networking security fundamentals. From its inception, the course has been taught in a computer lab, which facilitates hands-on learning. In addition to lecture-style concept reviews, textbook-based hands-on exercises have been incorporated to reinforce concepts and provide opportunities for learning-by-doing.

However, the textbook exercises lacked the context of realistic business-based scenarios for applying data security concepts and thus, did not help the students connect their learning to real world applications. To address this challenge, digital game-based learning was introduced into the course using a serious game that incorporates simulation and role-playing. The course modifications were designed using Bloom's Taxonomy of Educational Objectives, referred to as Bloom's Taxonomy, as a guide. Bloom's Taxonomy is a hierarchical classification system that was created in 1956 by educational psychologist Benjamin Bloom. Working with collaborators Max Englehart, Edward Furst, Walter Hill, and David Krathwohl, he designed a framework for categorizing educational goals. The framework consisted of six major categories: Knowledge, Comprehension, Application, Analysis, Synthesis, and Evaluation and provided a way to consistently develop and measure critical thinking and higher order cognitive abilities in students (Bloom, 1956). In Bloom's hierarchical structure, Knowledge was the starting point and Evaluation represented the farthest point in the hierarchy.

In 2001, Bloom's Taxonomy was revised to underscore the use of verbs and nouns to label all subcategories, instead of just nouns that were used in the original taxonomy. These action verbs describe the cognitive processes by which thinkers encounter and work with knowledge (Anderson, Krathwohl, Airasian, Cruikshank, Mayer, Pintrich, Raths, & Wittrock, 2001). Thus, in Bloom's Revised Taxonomy, the noun provides the basis for the Knowledge dimension and the verb forms the basis for the Cognitive Process dimension. The revised taxonomy includes the following major hierarchical categories: Remember, Understand, Apply, Analyze, Evaluate, and Create. In the hierarchical structure of Bloom's Revised Taxonomy, remember is the starting point and Create represents the farthest point in the hierarchy. Table 1 summarizes the components of Bloom's Revised Taxonomy and provides sample action verbs for each category.

TABLE 1
Bloom's Revised Taxonomy (adapted from Anderson and Krathwohl, 2001)

	Remember	Understand	Apply	Analyze	Evaluate	Create
Definition	Exhibit memory of previously learned material	Demonstrate understanding of facts and ideas	Solve problems to given situations by applying acquired knowledge	Break information into constitute parts	Make judgements about information based on criteria and standards	Compile information together in a different way
Sample action verbs	Choose, identify, recall, select	Associate, explain, interpret, relate	Develop, determine, plan, solve	Compare, discover, examine, infer	Assess, critique, interpret, value	Build, design, discuss, imagine

Bloom's original and revised taxonomies have been widely used to structure and measure educational outcomes. Studies in active learning and online learning have found that learning activities that progress through the cognitive levels of Blooms Revised Taxonomy led to enhanced learning and increased creativity (Carloye, 2017; Abuhassna, Al-Rahmi, Waleed, Noraffandy, Zakaria, , Kosnin, & Darwish, 2020; El-Khalili, & El-Ghalayini, 2015; Kidwell, Fisher, Braun, & Swanson, 2013; Quain, Bokunewicz, & Criscione-Naylor, 2018). The hierarchical model can also help students understand learning expectations and increase student understanding when using simulations in disciplines such as engineering and business (Jaiswal, Al-Hattami, 2020; Fang & Tajvidi, 2017; Nisula & Pekkola, 2019; Marley, 2014). Digital game-based learning in a college setting provides an alternative or complement to drill and practice or lecture-based learning and can be used to motivate and engage digital natives, learners who have been exposed to digital technology since their early stages of development. This type of learning meets the needs and learning styles of today's generation of learners (Prensky, 2007) and serious games expose the learner "to a designated environment that delivers unique content such as know-how or expertise . . . along with entertainment and multimedia" (Fatta, Maksom, & Zakaria, 2018). Adapting teaching styles for the target population enhances the learning environment and can lead to a more effective learning experience. Most community college students are digital natives. Community colleges with a diverse student population that includes first-generation college students or low-income college students may have more students with limited exposure to business settings from which to develop analogies that connect classroom learning with real life applications. Furthermore, while instructors may stimulate learning through lecture, videos, and guiding discussions on assigned readings that demonstrate real world applications, digital game-based learning aligns with the learning style of digital natives, which is characterized by preferring active learning, expecting a technology infused learning environment, and expecting immediate feedback (Thompson, 2015).

CYBERCIEGE

CyberCIEGE is a resource management serious digital game that was developed by researchers at the Naval Post Graduate School and is available as a free download for educators (Center for Cybersecurity and Cyber Operations, n.d.). It is developed in the model of an epistemic game, in which students learn by role-playing within the context of an authentic re-creation of valued real-world work. As a player in the role of a cyber-security professional, CyberCIEGE promotes critical thinking and active learning as students use domain specific knowledge to achieve the game objectives (Shaffer, 2006; Thompson & Irvine, 2011). The game "enhances information assurance and cyber security education and training . . . In the CyberCIEGE virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack" (Center for Cybersecurity and Cyber Operations, n.d.). Although it is designed as a single-player game, it supports peer-to-peer learning when played in a classroom setting. The game, which has several components that enhance learning in a simulated environment, is comprised of several topic specific independent challenges, called scenarios, in which the student plays the role of an information technology decision maker in a defined enterprise with specific objectives that support the enterprise's goals. The player wins by ensuring that the enterprise's assets are not compromised.

CyberCIEGE has a full color, interactive, 3D interface. The Main window includes the options for selecting campaigns and scenarios and initiating game play. Each scenario begins with a Briefing window that provides an overview of a business scenario. The game environment window is designed with several tabs, such as Office, Component, and Objectives, that are used to play the game. Players can access these tabs in an unrestricted manner during game play. The Office tab displays an interactive business office where players interact with employees and devices. The Objectives tab displays information about the status of completed objectives and the player's remaining tasks. The Game tab allows students to see the briefing information on demand. The Network, Component, Zone, and User tabs each display windows in which players apply settings to achieve the game objectives. Finally, the Asset tab allows players to see information about corporate assets (Appendix 1).

Each scenario in CyberCIEGE represents a customized business operation that includes a specific company name and business context. The scenario also includes specific business employees with behavioral traits and clearly identified business activities, often involving corporate assets, that are needed to meet specific business goals. In addition, each scenario includes an information technology staff role, which the student plays, that has clearly identified objectives that must be achieved to win the game. The simulation provides a virtual business setting in which students can make security-related decisions and see how those decisions impact employees and enterprises in real time.

Each scenario includes a lab manual, hints, and, in some cases, quizzes. Each customized lab manual, which the student can reference at any point during the game, includes an overview of the scenario and a brief introduction to the domain-specific concepts explored in the scenario. The lab manual also includes varying levels of guidance for students to help them play the game. Hints are automatically presented to students based upon choices they have made within the virtual game environment. Some scenarios include embedded quizzes that reinforce security concepts.

In addition to the scenario specific components, CyberCIEGE includes a comprehensive knowledge base, called the Encyclopedia, that includes a wide range of information and support for players and educators. The Encyclopedia includes short concept specific videos that provide relevant content in an engaging presentation format. The Encyclopedia also includes an extensive set of concept specific tutorials that teach players about cyber security concepts. Tutorials also provide players with information on how to play the game. The Encyclopedia content can be accessed at any time during the game and, within each scenario, players are prompted by the virtual environment to access the Encyclopedia to gain information to achieve game objectives. Finally, while the game is being played, the game engine records and saves player actions in a log. The log allows players to 1) save their current game state so that they can continue their game session at a different time, and 2) save alternative game states so that they can compare the outcomes of different decisions with the virtual environment.

CyberCIEGE also includes several tools that educators and game designers can use to analyze and customize game play. It includes a Campaign Analyzer, a Campaign Manager, and a Scenario Development Kit. The Campaign Analyzer provides a facility for educators to view player logs and analyze player performance based on various metrics collected during game play, such as scenarios played, time spent on scenarios, and scenario actions and outcomes. The Campaign Manager allows educators to customize the grouping of the scenarios into campaigns based upon their educational goals. Finally, the Scenario Development Kit provides an environment for developing new scenarios based on modifying existing scenarios or constructing completely new ones.

COURSE MODIFICATION

Digital game-based learning was incorporated into the Data Security for Business course by adding the simulation activities in one of three ways: 1) to enhance an existing course activity, 2) to complement an existing course assignment, or 3) to replace an existing course assignment. First, the instructor identified which CyberCIEGE scenarios covered topics that were already covered in the course. Then, if the topic was covered in the course using only reading or class discussion, the CyberCIEGE scenario was added to enhance the topic. If the topic was covered in the course using a hands-on activity, CyberCIEGE was added to complement an existing hands-on course assignment. If the topic was covered in the course using a non-hands-on activity, CyberCIEGE was added to replace the existing course assignment. Where applicable, writing assignments were designed to align more closely with real world business documents. Thus, student engagement with simulation-based business examples was incorporated into the existing course structure and the learning which resulted from this exposure could then be applied to other learning activities.

To assess student learning with the simulation, for each CyberCIEGE scenario that a student "won", the student received a small number of points towards their lab grade. For grading purposes, the simulation was included as a set of lab exercises with a low assessment value in the grade calculation. This allowed the resource to be included as a student evaluation component but, not weighted so heavily that if the resource did not add value to the course, it would not negatively impact each student's grade. The low assessment value also assisted the researcher in determining if students were engaging with the resource due to its edutainment value, meaning they liked the game, or due to its heavily weighted assessment factor.

To examine the efficacy of this simulation game for the course, the modified course was taught for two semesters and the end of course evaluation was revised to include questions related to student perceptions of CyberCIEGE. Engagement with the simulation game was measured by examining CyberCIEGE scenario completion data.

The Data Security for Business course covers several enterprise security topics, six of which relate specifically to the simulation scenarios in CyberCIEGE. Following are brief descriptions of those six topics. Malware and social engineering threats identifies malicious software and attacks that target common human behaviors. Encryption discusses how information can be converted to a format that is unrecognizable by hackers. Network security discusses how information and software on different connected devices is protected. Device security highlights the importance of protecting the computers, smartphones, tablets, and other devices used to access and store information. Authenticating users identifies methods for validating employees, customers, and other users of information. Access management highlights the importance of controlling a user's access to the wide array of information stored on enterprise devices. The course also covers risk management and business continuity as applied to securing digital assets, which is not aligned with the CyberCIEGE game. Table 2 demonstrates how selected CyberCIEGE scenarios align with these course topics and with Bloom's Revised Taxonomy.

TABLE 2
Course Topics and Scenarios Aligned with Bloom's Revised Taxonomy

Course Topic Areas	Campaign: Scenario	Bloom's Revised Taxonomy Category Action Verbs
Malware and Social Engineering Threats	Training: Stop Worms	**Remember** how worms can spread. **Select** the procedural choice that will most likely reduce the likelihood of spreading worms.
	Training: Life with Macros	**Remember** that up to date antivirus software will likely prevent viruses. **Select** the instruction that will reduce risk of infection from macro viruses.
	Training: Identity Theft	**Understand** that the device must be connected to the network before an online purchase can be made. **Relate** connecting to the network to potential virus infections. **Apply** appropriate virus protection mechanisms.
	Training: Passwords	**Apply** password procedural settings for employees. **Analyze and Apply** password configuration settings for the system.
Encryption	Encryption: Link Encryption	Not included in course.
	Encryption: Key Types	Not included in course.
Network Security	Starting Scenarios: Introduction	**Understand** network connections. **Apply** network connections.
	Starting Scenarios: Network Filters	**Understand** network connections and filters. **Connect** devices to local network, Internet, and configure router/firewall.
Device Security	Starting Scenarios: Patches	**Evaluate** patch update pross. **Apply** patches to Web App server. **Initiate** user training for patch updates. **Plan** testing for new patches.
	Starting Scenarios: Physical Security	**Examine** the value of the assets and **Apply** security to a site dependent upon the value of those assets. **Analyze** user clearance levels and configure security so that only users with authorized clearance have access to the secured zone.
Authenticating Users	Identity Management: User Identification	Not included in course.
Access Management	Mandatory Access Controls: MAC	Not included in course.
	Mandatory Access Controls: MAC Integrity	Not included in course.

As previously indicated, digital game-based learning was incorporated into the course by adding the simulation activity in one of three ways: 1) to enhance an existing course activity, 2) to complement an existing course assignment, or 3) to replace an existing course assignment. For example, the CyberCIEGE Training campaign includes scenarios that address malicious software, identity theft and passwords, which are related to the course topic on malicious software and social engineering threats. In the original course, these specific topics were reviewed with a class discussion, followed by a short writing assignment in which the students researched various malicious software attacks. This was then followed by a hands-on activity in which students used system software to configure a password policy based upon generic password characteristics, such as password length or complexity.

In the modified course, after the class discussion, the writing assignment was replaced with two CyberCIEGE game rounds focused on malicious software, followed by a debriefing discussion. In addition, a CyberCIEGE game round focused on identity theft was added to enhance the class discussion. Finally, the CyberCIEGE Passwords Scenario was used to complement the existing hands-on generic activity. In this case, the students played the CyberCIEGE game after the class discussion and experienced various issues related to password policies, insider threat, sabotage, and disgruntled employees within a simulated business setting. This allowed the students to role play as an information management professional and see how their actions, the actions of employees, and specific password policies impacted employee productivity and corporate assets. After a short debrief, students then completed the generic hands-on activity by using system software to configure a password policy. However, this generic hands-on activity is now being completed with the insight gained from the simulation, which provided a real-world context for the corporate password policy. Lastly, this also demonstrates an example of how the simulation prompted or generated a new assignment. In a real business setting, when system software is used to configure a password policy, the policy is also communicated to the employees in writing. This can be done through a policy manual, a memo, or other business communication forum. In this case, a new writing assignment was added in which the students write a business memo to the employees to introduce and explain the new password policy. Table 3 summarizes the impact of simulation use on existing course activities and assignments for three course topic areas.

TABLE 3
Impact of Simulation Use on Existing Course Activities

Course Topic Areas	Existing Activity/Assignment	Corresponding CyberCIEGE Campaign: Scenario	Simulation Impact
Malware and Social Engineering Threats	Writing: research malicious software attacks	Training: Stop Worms Life with Macros	Replaced existing assignment
	Class Discussion Only	Training: Identity Theft	Enhanced existing activity
	Hands-on: Use OS software to configure a password policy	Training: Passwords	Complemented existing assignment Prompted Writing Assignment
Network Security	Hands-on: Configure a software firewall	Starting Scenarios: Introduction Network Filters	Complemented existing assignment
Device Security	Writing: research patch management policies for several applications	Starting Scenarios: Patches	Replaced existing assignment
	Class Discussion Only	Starting Scenarios: Physical Security	Enhanced existing activity

When incorporating simulation software into an existing course, it is important to ensure that the course's learning objectives and outcomes continue to be met. In this business course, communicating in written form is a key learning objective, thus, it was important to ensure that writing assignments were not completely eliminated. It was equally important to find innovative ways in which student writing could be meaningfully aligned with the course content. In this course, by replacing a short research paper with a real-world enterprise password policy document, students were able to practice purposeful writing in a business context.

STUDENT ENGAGEMENT AND PERCEPTIONS

The course modification resulted in a total of eight CyberCIEGE scenarios being included in the course: two writing assignments were replaced with three CyberCIEGE scenarios, two class discussion topics were enhanced with two CyberCIEGE scenarios, and two hands-on activities were complemented with three CyberCIEGE scenarios. Over two semesters, 33 students played CyberCIEGE, each over a 7-week period. In the first semester, 17 students enrolled in the course and 16 students played the game. In the second semester, 17 students enrolled in the course and played the game. Additionally, in the first semester the students played all eight scenarios but, in the second semester, due to scheduling adjustments, the students played seven of the eight scenarios.

Table 4 indicates the student engagement with each simulation scenario for each of the two semesters. In the table, the scenarios are listed in the sequence in which they were applied in the course. The data demonstrates that as each campaign progresses, student engagement with the campaign decreases. For example, in the Training campaign, in semester 1 and semester 2, over 90% of the students completed the first three scenarios. This indicates that the students easily grasped how to play the game and understood the concepts covered in those scenarios. However, reduced student engagement was recorded for the last scenario, Passwords, in the campaign. Likewise, a similar pattern is also evident in the Starting Scenarios campaign. This indicates that additional support may be needed for students when they are playing later scenarios in a campaign.

TABLE 4

Student Engagement with Simulation Scenarios

Semester	Training Scenario: Stop Worms	Training Scenario: Life with Macros	Training Scenario: Identity Theft	Training Scenario: Passwords	Starting Scenario: Introduction	Starting Scenario: Filters	Starting Scenario: Physical Security
1 (n=16)	100%	100%	100%	75%	81%	69%	81%
2 (n=17)	100%	100%	94%	71%	94%	82%	76%

Student perceptions about the simulation software were captured through the end of course evaluation. Students were asked two questions related to the simulation software: 1) What did you like about CyberCIEGE? and 2) What did you dislike about CyberCIEGE? The open-ended questions were designed to allow students to establish the context of their responses. In their responses, 41%, the largest context cluster, referenced the business scenarios when indicating what was liked about CyberCIEGE. The students liked the real-life examples, the company setting depicted in the game, and the exposure to dealing with solving a real business problem. This indicates that the simulated business scenarios included in CyberCIEGE helped students apply cyber security principles within a business setting.

However, while students liked the business scenarios, many students thought that they needed more help when using the simulation. Forty-four percent of what students did not like, the largest context cluster, referenced the lack of help provided in the simulation. This perception may be related to the student engagement data which suggested that students may need additional support when completing particular scenarios.

CyberCIEGE includes several built-in help features in multiple learning modalities to assist students throughout the game. Several videos provide an overview of particular security topics and six videos are related specifically to the topic areas that were the focus of the course modification: malware and social engineering threats, network security, and device security. During game play, students are not required to watch the videos. In addition, CyberCIEGE includes an encyclopedia which contains detailed information on security topics and on how to perform actions in the scenarios. CyberCIEGE also includes real-time, contextual, active-response pop-up windows that direct students to access the encyclopedia or that provide game hints for assistance. Active-response windows require the user to click “OK” to close the pop-up window. Similarly, CyberCIEGE includes real-time, contextual passive-response pop-up arrows that guide students through the scenario with words and visual arrows. Lastly, each of the CyberCIEGE scenarios included in the course includes an in-game accessible student Lab Manual that includes instructions to complete each scenario. In addition, most students played the game during class sessions when the instructor was available to provide help.

These findings on student perceptions of CyberCIEGE are consistent with a previous study which compared the use of CyberCIEGE for information assurance training with the use of a Department of Defense video for information assurance training. This study also found that participants liked using CyberCIEGE to apply security knowledge to solve real world problems. However, the study similarly found that some students felt that additional clarification was needed to complete some scenarios (Jones, Yuan, Carr, & Yu, 2010).

CONCLUSION

This paper discusses how a resource management simulation game can be used within a classroom setting to teach students about cyber security principles as applied within a business setting. An introductory information security course was modified to include digital game-based learning that focused on role-playing and simulations of business scenarios. The modifications included enhancing existing class discussions with simulation activities, complementing existing hands-on activities with simulation activities, and replacing some non-hands-on activities with simulation activities. In some instances, new writing assignments were added that reinforced writing within a purposeful business context. The modified course was run for two semesters and student engagement with the game and perception of the game were discussed.

Overall, students completed the majority of the simulation modules that were assigned with high accuracy and liked being able to solve business security problems in a virtual business setting. However, many students felt that additional help was needed to play the game effectively.

FUTURE RESEARCH AND LIMITATIONS

This study contributes to the existing literature on the use of simulations and games for learning by furthering the discourse on course modification techniques, on student engagement with simulation tools, and on student perceptions of learning resources. However, due to its small sample size and limited data collection techniques, it is by no means exhaustive. Nevertheless, the results have prompted several research questions and areas for further study. Some of these include:

- Exploring simulation introduction, use, and debrief methods to identify supportive techniques for student assistance
- Surveying instructors to identify best practices for incorporating simulation software into an existing course
- Exploring student perceptions of individual CyberCIEGE scenarios
- Exploring methods for effective assessment of student learning with CyberCIEGE
- Exploring engagement with the CyberCIEGE Training scenarios, which focus on information assurance, for non-technical students

Game-based simulation provides an effective way to engage today's learners and meet the needs of our digital society. CyberCIEGE is a freely available resource management game-based simulation tool with role-playing, that reinforces learning cyber security principles in an engaging way. Further studies at this point of intersection are warranted.

REFERENCES

Abuhassna, H., Al-Rahmi, W. M., Yahya, N., Zakaria, M., Kosnin, A., & Darwish, M. (2020, Oct). Development of a New Model on Utilizing Online Learning Platforms to Improve Students' Academic Achievements and Satisfaction. *International Journal of Educational Technology in Higher Education, 17*(1).

Anderson, L.W. (Ed.), Krathwohl, D.R. (Ed.), Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., & Wittrock, M.C. (2001). A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives (Complete edition). New York: Longman.

Anderson, P. H. & Lawton, L. (2009, Apr). Business Simulations and Cognitive Learning Developments, Desires, and Future Directions. *Simulation & Gaming, 40*(2), 193-216.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (Eds.). (1956). Taxonomy of Educational Objectives: The Classification Of Educational Goals; Handbook I: Cognitive domain. New York, NY. Longmans, Green.

Carloye, Lisa. (2017, Jul/Aug). Mini-Case Studies: Small Infusions of Active Learning for Large-Lecture Courses. *Journal of College Science Teaching, 46(6), 63-67.*

Center for Cybersecurity and Cyber Operations. (n.d.). Retrieved September 30, 2019, from Naval Post Graduate School: https://my.nps.edu/web/c3o/cyberciege.

El-Khalili, N. H., & El-Ghalayini, H., (2015). Comparison of Effectiveness of Different Learning Technologies.
International Journal of Emerging Technologies in Learning, Special Issue ALICE 2014, *10*, 56-63.

Fang, N. & Tajvidi, M. (2018, Feb). The effects of computer simulation and animation (CSA) on students' cognitive processes: A comparative case study in an undergraduate engineering course. *Journal of Computer Assisted Learning, 34*(1), 71-83.

Fatta, H. A., Maksom, Z., & Zakaria, M. H. (2018, Dec). Game-based Learning and Gamification: Searching for Definitions. *International Journal of Simulation -- Systems, Science & Technology, 19*(6), 1-5.

Gummineni, M. (2020). Implementing Bloom's Taxonomy Tool for Better Learning Outcomes of PLC and Robotics Course.
International Journal of Emerging Technologies in Learning, 15(5), 184-192.

Jaiswal, P., & Al-Hattami, A. (2020). Enhancing Learners' Academic Performances Using Student Centered Approaches. *International Journal of Emerging Technologies in Learning*, *15*(16), 4-16.

Jones, J., Yuan, X., Carr, E., & Yu, H. (2010). A Comparative Study of CyberCIEGE Game and Department of Defense Information Assurance Awreness Video. *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)* (pp. 176-180). Charlotte: IEEE.

Kidwell, L. A., Fisher, D. G., Braun, R. L., & Swanson, D. L. (2013, Feb). Developing Learning Objectives for Accounting Ethics Using Bloom's Taxonomy. *Accounting Education, 22*(1), 44-65.

Krishan, R. (2018, May 1). Corporate Solutions to Minimize Expenses from Cyber Security Attacks in the United States. *Journal of Internet Law, 21*(11), 16-19.

Marley, K. A. (2014). Eye on the Gemba: Using Student-Created Videos and the Revised Bloom's Taxonomy to Teach Lean Management. *Journal of Education for Business, 89*(6), 310-316.

Nisula, K., & Pekkola, S. (2019, Jul). ERP based business learning environment as a boundary infrastructure in business learning. *Education & Information Technologies, 24*(4), 2547-2566.

Phillips, R., & Tanner, B. (2019). Breaking Down Silos Between Business Continuity and Cyber Security. *Journal of Business Continuity & Emergency Planning, 12*(3), 224-232.

Ponemon Institute. (2018). *2018 Cost of a Data Breach Study: Global Overview".* Retrieved Aug 28, 2019, from https://www.ibm.com/security/data-breach.

Prensky, M. (2007). *Digital Game-Based Learning.* Paragon House.

Quain, B., Bokunewicz, J. F., Criscione-Naylor, N. M. (2018 Jan). The Profit: Using Reality TV to Teach Management Theories and Strategies. *Cogent Education, 5*(1).

Shaffer, D. W. (2006, April). Epistemic Frames for Epistemic Games. *Computers and Educations, 46*(3), 223-234.

Thompson, M., & Irvine, C. (2011, August 8). Active Learning with the CyberCIEGE Video Game. *4th Workshop on Cyber Security Experimentation and Test.* San Francisco, CA. Retrieved August 15, 2019, from https://my.nps.edu/web/c3o/cyberciege-papers.

Thompson, P. (2015, Sep). How Digital Native Learners Describe Themselves. *Education and Information Technologies, 20*(3), 467-484.

APPENDIX 1

IMAGE 1
CyberCIEGE Main Window

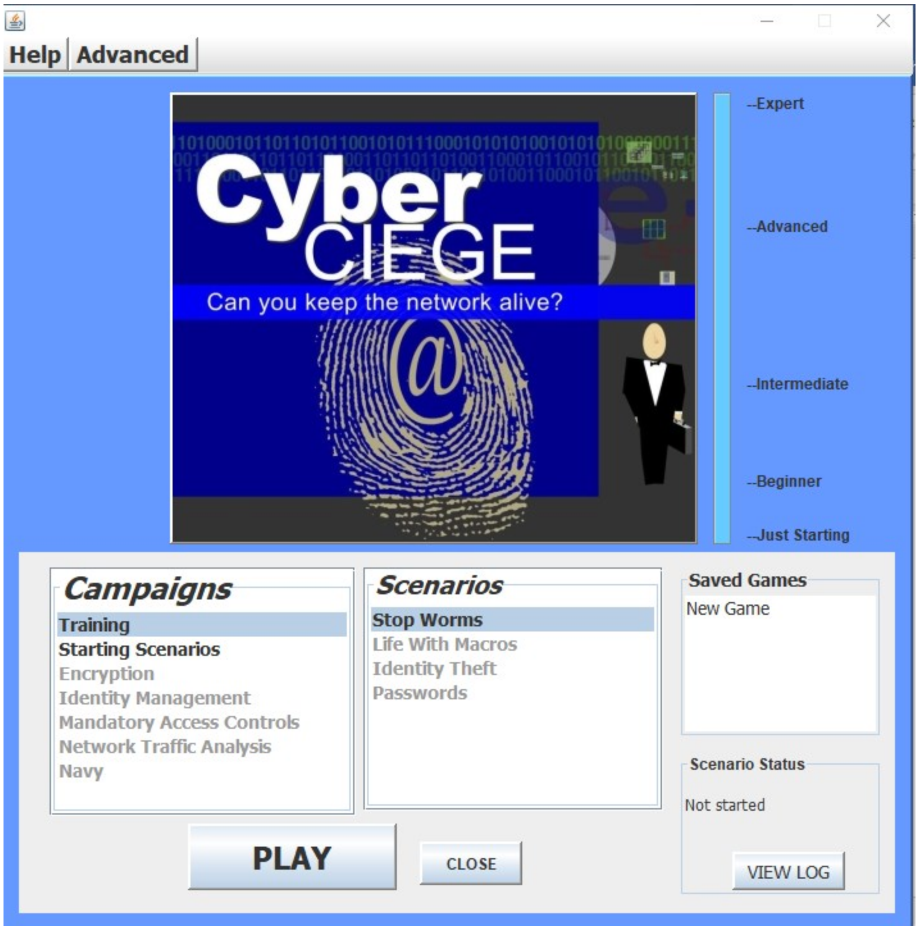
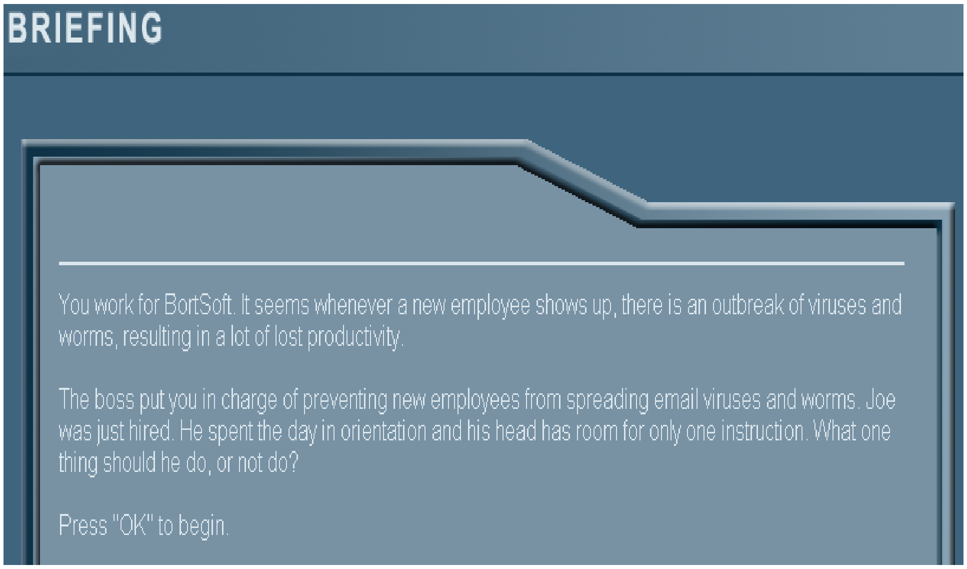


IMAGE 2
CyberCIEGE Briefing Window

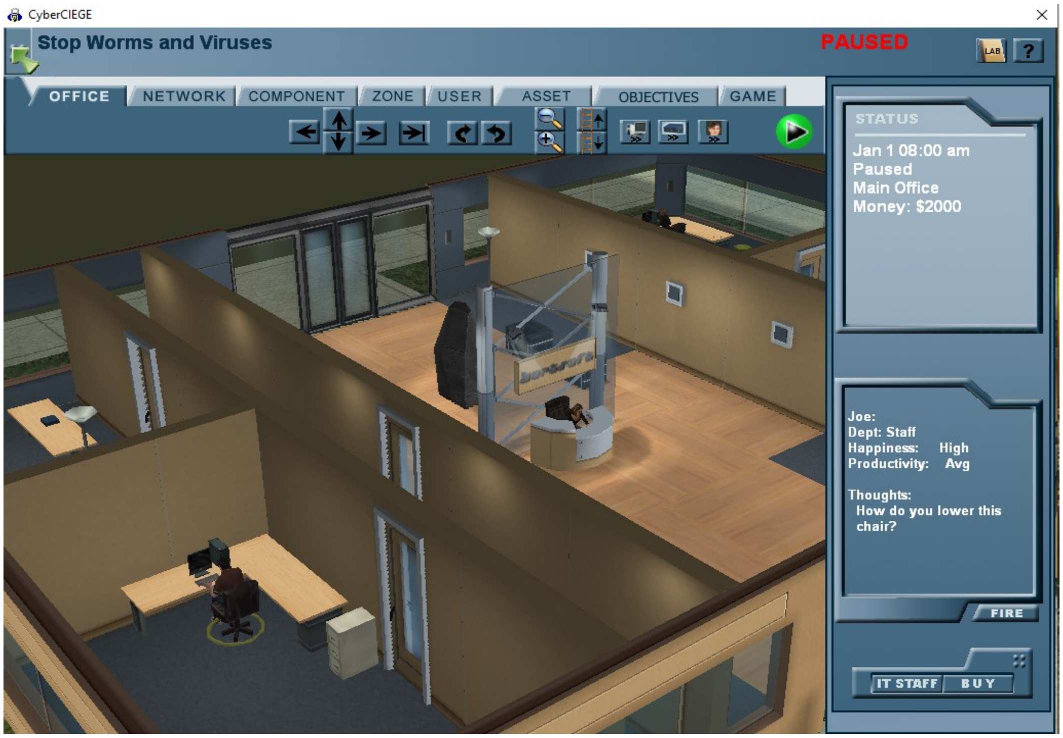


You work for BortSoft. It seems whenever a new employee shows up, there is an outbreak of viruses and worms, resulting in a lot of lost productivity.

The boss put you in charge of preventing new employees from spreading email viruses and worms. Joe was just hired. He spent the day in orientation and his head has room for only one instruction. What one thing should he do, or not do?

Press "OK" to begin.

IMAGE 3
CyberCIEGE Office Window

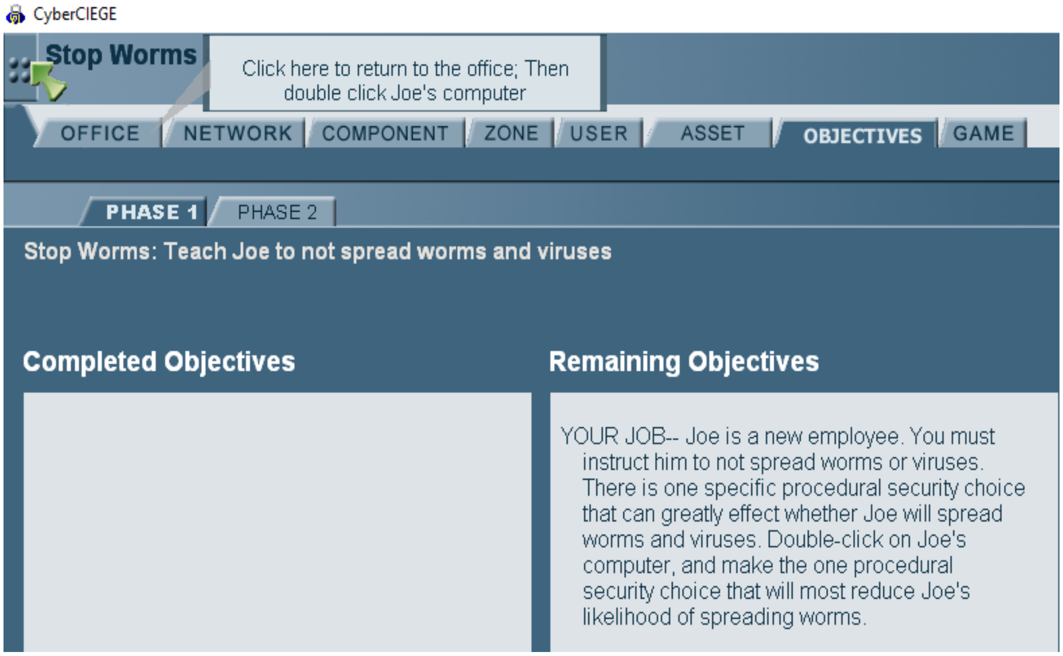


Jan 1 08:00 am
Paused
Main Office
Money: $2000

Joe:
Dept: Staff
Happiness: High
Productivity: Avg

Thoughts:
How do you lower this chair?

IMAGE 4
CyberCIEGE Objectives Window



Click here to return to the office; Then double click Joe's computer

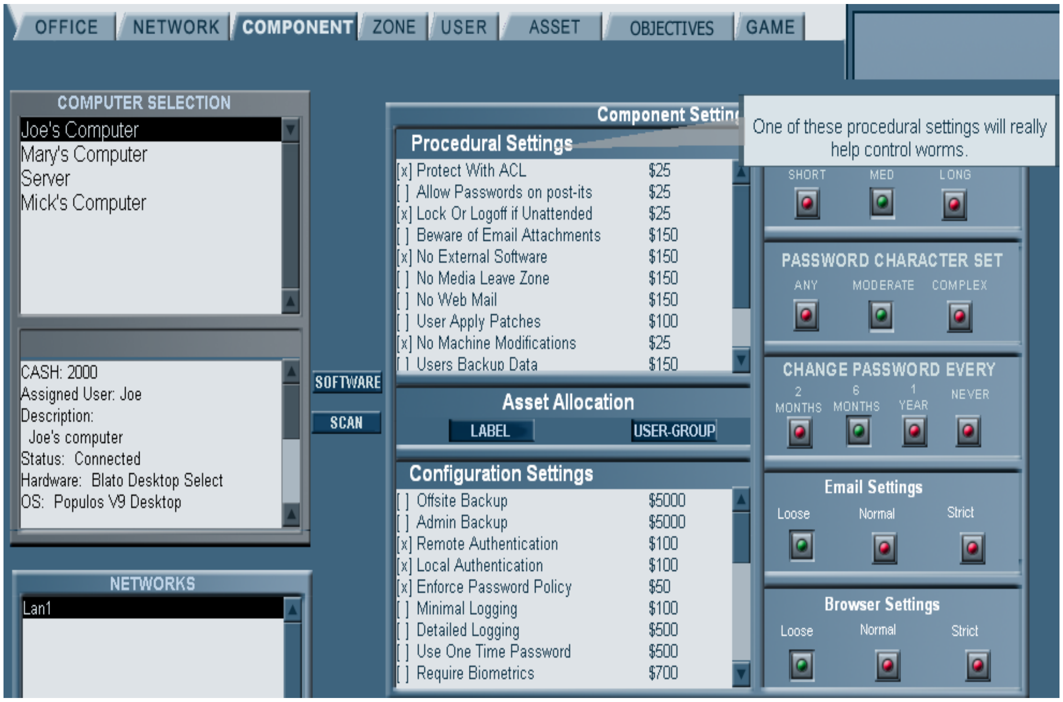
Stop Worms: Teach Joe to not spread worms and viruses

Completed Objectives

Remaining Objectives

YOUR JOB-- Joe is a new employee. You must instruct him to not spread worms or viruses. There is one specific procedural security choice that can greatly effect whether Joe will spread worms and viruses. Double-click on Joe's computer, and make the one procedural security choice that will most reduce Joe's likelihood of spreading worms.

IMAGE 5
CyberCIEGE Component Window



COMPUTER SELECTION

Joe's Computer
Mary's Computer
Server
Mick's Computer

CASH: 2000
Assigned User: Joe
Description:
Joe's computer
Status: Connected
Hardware: Blato Desktop Select
OS: Populos V9 Desktop

NETWORKS

Lan1

Component Settin

One of these procedural settings will really help control worms.

Procedural Settings

[x] Protect With ACL	$25
[ ] Allow Passwords on post-its	$25
[x] Lock Or Logoff if Unattended	$25
[ ] Beware of Email Attachments	$150
[x] No External Software	$150
[ ] No Media Leave Zone	$150
[ ] No Web Mail	$150
[ ] User Apply Patches	$100
[x] No Machine Modifications	$25
[ ] Users Backup Data	$150

Asset Allocation

Configuration Settings

[ ] Offsite Backup	$5000
[ ] Admin Backup	$5000
[x] Remote Authentication	$100
[x] Local Authentication	$100
[x] Enforce Password Policy	$50
[ ] Minimal Logging	$100
[ ] Detailed Logging	$500
[ ] Use One Time Password	$500
[ ] Require Biometrics	$700

SHORT ○ MED ● LONG ○

PASSWORD CHARACTER SET

ANY ○ MODERATE ● COMPLEX ○

CHANGE PASSWORD EVERY

2 MONTHS ○ 6 MONTHS ● 1 YEAR ○ NEVER ○

Email Settings

Loose ● Normal ○ Strict ○

Browser Settings

Loose ● Normal ○ Strict ○