High School 12-Week Cybersecurity eLearning Pilot

Myoki Spencer (SAIC) and Duke Ayers (SAIC)

:

Abstract -This High School Cybersecurity eLearning Pilot was conceived to address a significant national issue: the Science, Technology, Engineering and Mathematics (STEM) shortfall that does not appear to have an available solution. The Pilot demonstrated that U.S. educators currently have the resources to implement a national cybersecurity training program, whether as part of a school's program, or conducted after school. From this experience, we have demonstrated that this shortfall can be immediately addressed through a formal curriculum, supported by a 24x7 online trainer technology, and procedures and tools to empower the local educators. We also know that with the right instruction and hands-on experience, the kids "get it!"

I. INTRODUCTION

The Pilot was conducted over a three-month period. Participation in the SAIC's eLearning Pilot was voluntary. More than 200 individuals from 33 schools participated in some or the entire pilot.

The pilot consisted of 10 instructional modules, with an entrance and exit examination in the first and last weeks, making this a 12-week program. The exams were intended to first establish a baseline of what the students knew before the benefit of the training and then at the end to document the degree of knowledge learned and applied in a practical, live environment. The local educators delivered the 10 modules to their students, after receiving train-the-trainer instruction from SAIC. The teachers had many tools available to them, including instructional videos and online training materials. The students exercised on an Internet-based, live exercise environment, which SAIC has employed for more than four years during competitions such as 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. This third generation technology, called, CyberNEXS, permits exercise on real systems anywhere and anytime; therefore students can study wherever, whenever.

During the course of the pilot, SAIC collected statistics and comments for analysis and inclusion in the final report. The purpose of this final report is to document the strengths and weaknesses of the curriculum and the procedures and technologies used during this pilot. Teachers, mentors, regional directors, and students provided their feedback, so that future efforts to develop a national cybersecurity program for high school students may benefit from these results.

II. CONDUCT OF THE PILOT

The SAIC High School Cybersecurity Pilot provided the opportunity to evaluate an Internet-based curriculum, instruction, and training environment. Key to the success of this program is scalability, both in terms of numbers served, but also the ability to empower the local educator with the tools they need to confidently instruct and guide the students; a one-to-many instructional model. Also key is the underlying technology to support the instruction and provide immediate feedback to the students so that they may, through trial-and-error, understand and personalize the instruction through an online, 24x7 learning system.

A. Preparation for the Pilot

Four months prior to the start of the SAIC High School Cybersecurity Pilot, SAIC introduced the concept of a pilot to various organizations to seek their interest and participation. Five organizations stepped forward and signed a memorandum of understanding (MOU) that established the overall goals of the pilot and the responsibilities of SAIC and the organizations that agreed to participate. They are:

- Los Angeles Unified School District (LAUSD) after-school program
- Huntsville, Ala. schools
- Global Institute for Cybersecurity and Research (GISCR) with Florida schools
- Hawaii schools

ISBN 1-933510-95-1/$15.00

- Manitoba, Canada school system

Approximately three weeks prior to the commencement of the SAIC Pilot, scheduled for 19 September 2011, SAIC conducted several online orientation briefings for regional directors and other associates. The purpose was to acquaint the regional leaders with the overall curriculum, the procedures for train-the-trainer, and the technology for use during local educator instruction and student exercise.

During the course of the Program, instructional briefing material was videotaped and then made available for download via the pilot web site, along with student and teacher guides and other tools. Although not a consideration in the initial planning, we made a decision to use videos for all instructional briefings and to train the trainers based on the following rationale; to:

- Provide the instructional material for teachers who were not available during train-the-trainer sessions;
- Permit those who had attended the sessions to re-watch for a deeper understanding; and,
- Be used to deliver the instructional material to the students in the event that the local educator was not confident to deliver the training.

B. Pilot Requirements

To provide for this pilot, several tools and technologies were required:

1. Tools

   Curriculum. One of the key reasons that a cybersecurity training program does not currently exist in most high schools is that there are few states' requirements for teaching this subject and there is resistance to inserting yet one more subject into an overcrowded school year;

   Guides. To instruct the subject, teachers would need essential tools such as teacher's guides and student manuals, coupled with a simple-to-use, online training environment that mirrors real-world systems while providing real-time feedback on student performance; and,

   Train-the-Trainer. Currently, there are few educators at the high school level comfortable with teaching cybersecurity. To provide for the capable local educator, a support system of train-the-trainer and mentoring was required; video instructional material proved essential in reaching both instructors and students.

2. Technology

   Realism. The training environment needed to contain live computer-based servers and workstations on which the teachers and students would train.

   Automated. The online trainer must provide real-time feedback to reinforce trial-and-error exercise.

   - Availability. It must be available to teachers and students at any time of day to support flexible training and practice schedules and conditions.
   - Scalability. It must support thousands of simultaneous users to accommodate many teachers and students across the U.S. and Canada.
   - Simplicity. It must be simple to use to empower teacher and student to become quickly capable of optimizing its use.

C. Conduct of the Pilot

Week One. The pilot began with an entrance examination. This exam was intended to baseline the students' level of knowledge prior to the formal instruction provided during the pilot. The only instruction given to students was to assume the role of a security team investigating a system that has had some suspicious activity.

Weeks Two – Eleven. Each week, the teachers were asked to present the curriculum training materials to the students. In addition to the instruction slides and lab exercises, the teachers and students downloaded VMware images that virtualized an actual Windows OS, which operated inside of the teachers' and students' school or personal computers. Each image had an embedded CyberNEXS™ client that communicated with a SAIC central server, and reported when students made positive or negative changes to the image during the weekly lab exercises. The SAIC server scored those changes and reported progress back to the student, via a "Get My Status Page" (described later). Additionally, online quizzes were provided weekly through shortcut links on the students' virtual machine. The teachers and students received real-time feedback as to their progress in accomplishing the following:

- Ability to maintain critical computer system services, such as the simple mail transfer protocol (SMTP) service for an email server; and,
- Ability to harden the system by removing common vulnerabilities, such as weak passwords, turning off unnecessary services, validating user accounts, etc.

CyberNEXS™ services were available from Monday, 7 a.m. PST – Sunday, 5 p.m. PST. Anytime during that period, instructors/mentors and students could work with the images and be scored. Weekly instruction was intended to require no more than 1-2 hours, so that the remaining time would be spent on practical exercising by the students. On Sunday evening, SAIC reset the system for the next week of instruction/exercise, thereby providing the instructors/mentors 36 hours to prepare for the following week's curriculum.

Online train-the-trainer question and answer sessions were held on Fridays at two different times to accommodate as many given different time zones and schedules. Again, for those not able to attend, the weekly lessons were pre-recorded and published to the SAIC web site, both as a downloadable file or streaming video.

Week Twelve. After 10 weeks of curriculum instruction, the students took the entrance exam again to measure the degree of learning accomplished. Again, students were instructed to act as a security team investigating a system breach and to use the knowledge they had gained during the previous weeks' instruction to find and fix as many security vulnerabilities as possible
.
Scoring. The exercises were not competitive events, and no student's nor school's degree of success is identified in the final report; all results were reported respecting anonymity. Each student could view their own score, the instructors viewed all their students, and the regional director had access to the regional scores.

D. Roles and Responsibilities

These were established in the MOU signed prior to the start of the pilot.

Regions shall:

- Demonstrate serious commitment to provide encouragement to stay with the program and other resources listed below
- Provide a single point of contact (POC) as the primary interface and coordinate with the high schools under their purview
- Identify and organize mentors (students/educators) to work with assigned high school educators
- Educators and mentors deliver weekly instruction to students using the curriculum provided by SAIC
- Provide computers with minimum of 2 GB RAM, 20 GB free disk space and 128 KBps bandwidth internet availability per student, allowing outbound HTTPS (port 443)
- Provide user feedback on the curriculum and training exercises for areas of improvement, what worked well, and what didn't work well, etc.

SAIC shall:

- Provide 12-week cybersecurity training and exercising via the Internet at no cost
- Provide Cyber Defense Level One pilot instructional material for high schools (with speaker's notes)
- Provide pre-pilot guidance to local educators
- Provide weekly online train-the-trainer instruction
- Capture student and trainer feedback and results
- Provide help desk function (normal working hours)
- Work with participants to finalize measures of effectiveness (MOEs)
- Produce final report

E. Overview of the ten curriculum modules:

1. Windows Basics:

- Identify basic computer components
- Describe information security
- Go through the Windows "boot" sequence
- List the different Windows versions
- Explain the basic architecture of Windows
- Describe why "default installations" left alone are bad
- Describe Windows installation limitations
- Use Windows utilities to determine settings
- Use third-party tools to determine settings

2. Windows Networking:

- List the differences between various types of networks
- Identify common network devices

- Explain the purpose and basic operation of (TCP/IP)
- Identify Windows networking configuration tools
- Explain basic components of wireless networking

3. Accounts Basics:
   - Identify basic properties of Windows user accounts
   - Understand the basics of user account permissions and privileges
   - Understand the different built-in Windows user accounts
   - Know the difference between a local account and networked (domain) account
   - Know what tools are used to create local user accounts
   - Explain a few Windows 7 groups
   - Explain security issues with the "administrator" account

4. Threats and Vulnerabilities:
   - Describe the concept of threats, vulnerabilities, and exploits, and their relation to each other
   - Explain the concept of risk
   - Describe the concept of dealing with risk issues
   - Explain motivations for hackers/attackers
   - Explain forms of hacking techniques
   - Review the Microsoft System and Security Center
   - Describe the Windows firewall

5. Threats and Vulnerabilities/Patching:
   - Describe how threats, vulnerabilities and exploits are related to patching
   - Understand why attacks are targeted toward unpatched systems
   - Explain "why do we patch?"
   - Understand different patching methods
   - Describe the Microsoft patch process
   - Understand using anti-virus software
   - Understand the anti-virus update installation process

6. DNS, Routes, Workgroups/Domain:
   - Explain workgroups and domains
   - Understand a domain controller
   - Understand organizational units
   - Explain active directory and trusts
   - Describe the fundamentals of DNS
   - Understand basic routes and routing

7. Services/DR/shadow copies:
   - Explain basic service components
   - Explain ports and service mappings
   - Describe the services attack vector
   - Identify Windows default services
   - Understand the enabling/disabling of services
   - Identify tools to check services
   - Understand the importance of backups
   - Understand the importance of restores

8. Authentication/Access Controls/basic crypto:
   - Understand strong password management and creation
   - Understand password cracking techniques
   - Understand system permissions and rights
   - Understand strong cryptography and its uses
   - Understand the importance of file integrity

9. Servers -File Server:
   - Understand your server's role
   - Understand why multiple roles present vulnerabilities
   - Understand each services unique vulnerability
   - Understand strong configuration options for services
   - Understand the importance of server placement within your network
   - Understand the placement of IDS/IPS devices within your network

10. Locking down Servers with utilities -add on utilities:
    - Understand your server's role
    - Understand why multiple roles present vulnerabilities
    - Understand each services unique vulnerability
    - Understand strong configuration options for services
    - Understand the importance of server placement within your network
    - Understand the placement of IDS/IPS devices within your network

F. Measures of Effectiveness

1. Exam Scores

Our goal was to establish a clear comparison between the entrance and exit exams to determine the amount of student learning that occurred. Unfortunately, during the entrance exam, both teachers and students participated so the results are slightly skewed, but the overall results were clear. Even with the higher grades recorded by adults, the scores had increased at least 20 percent.

Also encouraging were the scores recorded during the weekly exercises. With a low of 63 percent and a high of 94 percent, one can see how certain modules can use a rewrite, or an increase of time, to ensure that the subject is clearly understood. Still, the following scores do reflect a positive learning experience.

	Windows Basics	Windows Networking	Accounts Basics	Threats & Vuls	Threats & Vuls - Patching	DNS, Routes, Workgroups	Services, DR, shadow copies	Auth/Access, crypto	Servers-File server	Hardening Servers	
Region One	82	92	89	86	97	50	96	83	94	81	85.0
Region Two	80	78	84	71	82	59	82	88	97	78	79.9
Region Three	83	85	87	77	90	76	89	90	100	85	86.2
Region Four	85	79	83	79	86	57	80	90	96	79	81.4
Region Five	76	84	87	73	85	74	89	78	83	88	81.7
	81.2	83.6	86	77.2	88	63.2	87.2	85.8	94	82.2	**82.8**

Figure 1. Weekly Exercise Scores by Region

Although statistically, one cannot statistically compare entrance to exit exam results, but one can still see that learning did occur.

Entrance Exam	Exit Exam
Mean = 27.6%	Mean = 46%
Median = 16.6%	Median = 44%

Figure 2. Comparison of Entrance and Exit Exams

Also encouraging was the relative consistency between regions; it appears that all groups benefited from pilot.

Region One	42%
Region Two	51%
Region Three	33%
Region Four	42%
Region Five	41%

Figure 3. Exit Exam Scores by Region

2. Online Questionnaire

During the course of the pilot, instructors, mentors, students and regional directors were asked to provide feedback. CyberNEXS™ provided performance-based exercising and therefore quantified student performance, but we were also interested in capturing other programmatic and social observations that might aid future educators in evolving this model. We hoped that a network of instructors/mentors would provide a local support network for those not as confident in delivering the instruction. Of key importance was that the students gain more knowledge than they otherwise would have available to them, and that they had fun.

The following was the online questionnaire we made available to anyone in the program who wanted to comment. The following are the questions and summary of the eleven responses:

1. How many students in your class?
   High = 45; low = 2; mean = 12; median = 8.
2. What days/time of day do you provide student instruction?
   There was no consistent answer. Some every day, others 2 days a week, etc.
3. How much time are the students spending reviewing the lesson and working on the labs?
   Average was 2.5 hours per week.
4. Do you have all the tools you need to conduct the class?
   91% answered yes.
5. What were the biggest hurdles you had to overcome?
   Some noted that image downloads took too much time, while others noted student schedules made coordination difficult.
6. What method of instruction do you primarily use?
   Majority noted they used both the slides and videos.
7. Do your students take the weekly online quizzes?
   82% noted yes. Others noted internet availability issues.
8. Do your students work on the VMware images from outside of school?
   Only 36% answered yes.
9. Are the students interested and engaged with the CyberNEXS™ Pilot Program?
   Are they having fun? 91% responded yes.
10. Are the students gaining knowledge?
    91% said yes.
11. What do you think of the videos?
    82% responded that they liked them; some noted that they were too long in length.
12. How many times do you watch the videos per week?
    Half answered once, while other half 2 or more.

13. What video format works best for you?
    Half "wmv" and other half either "avi" or both.
14. Do you attend the weekly online train-the-trainer sessions? If not, why?
    Majority of those that didn't attend stated that there had conflicts with classes or meetings.
15. If you do attend the sessions, does it help you with your instruction?
    Half noted that they did participate to have an opportunity to ask questions.
16. What do you think of the content of the course?
    8 answered "Just the right mix." 2 said it was too technical while 1 said it was not technical enough.
17. How would you grade the CyberNEXS™ Pilot (1-10)?
    High = 10; low = 1; mean = 7.7; median = 8.

3. Lessons Learned

General Observations:

- The official pilot start and stop dates did not work well for all participants. We anticipated that with different school schedules, there might be a problem, but we proceeded to accommodate the majority of schools. We did extend the availability of the entrance exam image for an additional week so that all the students could participate. Again, at the end, the exit examination was available for a two-week period.
- Train-the-trainer sessions were scheduled for once a week. Due to the different time zones, we set up a second session to accommodate those who could not make the first. The times established were:
  a. 8-10 a.m. Pacific
  b. 2-4 p.m. Pacific
- Still, these sessions were lightly attended, mostly due to conflicting schedules, but also we believe the curriculum videos provided the trainers with most of what they needed to provide their local instruction and mentoring.
- Originally, the CyberNEXS™ training environment was to be reset each Thursday so that we could use Fridays to train-the-trainer for the next week's curriculum module using that modules target set. This would also allow teachers to rehearse their instruction. In fact, to accommodate many requests, we extended the exercise image time, which provided greater flexibility for the students, but may have reduced the time that some teachers had to rehearse with the following week's image. We did not get any feedback on this issue.
- Also, the train-the-trainer sessions were intended to be live presentations of the following week's curriculum. Prior to the first training session, we decided to produce videos for each week; we believe this greatly benefited mentor and student instruction and relieved the need for direct train-the-trainer sessions. Some teachers noted that the videos were the single most valuable tool available, as their students were able to watch at their own pace and replay sections that were not clear.
- Kids' get it, if they are able to immediately take instructional material and personalize it through trial-and-error practical exercise. Having a training and exercise environment helps to reinforce and retain instruction.

Weaknesses:

- Curriculum pace was overly aggressive; lectures were too long, i.e. one hour in length. The 10 modules could be segmented into smaller modules of 20-30 minutes in length. This reduced time would help to maintain student interest, and provide greater time for their hands-on exercise activities.
- Difficulty coordinating meeting times when considered extra-curricula. Teachers and mentors had to be very dedicated to find time during or after school. This issue would be relieved with a state-sponsored program that establishes regular school hours for this training.
- Download of large images required too much time. It was suggested that the teachers be provided a series of VMware images prior to the beginning of the program. We didn't in this case, as we were tweaking the curriculum as we progressed through each module. A formal program with an established curriculum that would be distributed in advance of program commencement would relieve this issue.
- Few students used images outside the classroom. This may be in part due to lack of adequate home computers or a lack of student interest in pursuing the academics outside the classroom. Some students did use them at home, but we don't have any data to determine why the others didn't. We do have experience with students using images

outside of school during competitions. In Cyber Patriot III, we had some students participate from McDonald's due to Internet and firewall issues at their school.

- Some indicated lack of resources (Internet, computers, etc.) at the school. As technology refresh occurs, the computing power requirements should not grow for this type of online service, therefore, schools should be able to catch up.
- SAIC only provided actual scores without detailing in which functional area the students succeeded, such as account management, policy management, etc. This is an important detail that will assist the students in better understanding where they need to spend more time in study. This will also be an important feature in any performance-based testing program that is expected as a result of such initiatives as the National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE). SAIC will implement this capability in the next couple of months to better support future training and exercising efforts.

Strengths:

- Students grasped the instruction material. Overall, the scores were consistently high. This curriculum was fast paced and taught some difficult concepts such as threats and vulnerabilities, access control and networking.
- Videos proved effective in meeting the need for train-the-trainer sessions. Videos provided the opportunity for teachers/mentors to train and provide student instruction with flexibility and without the fear of not knowing the entire subject material. This tool is highly recommended for future programs.
- Overall weekly exercise scores averaged 82.8 percent; least was 79.9 percent
- Entrance and exit exams demonstrated significant gain of knowledge
- All MOEs measured with majority of results as positive
- Good feedback; both surveys and personal notes reflect a positive experience.
- Right mix of content. This was a recurring theme that we heard throughout the pilot. Although the pace was fast and the instruction time long, the material itself was well received by both teacher and student.

4. Additional Comments (verbatim):

Teacher 1.
First and foremost, we are extremely appreciative for the opportunity to participate in this program. I remained amazed at the volume and quality of the content and presentations and labs and quizzes and the thought that has gone into organizing and structuring the program. It is wonderful that this opportunity is being afforded to high school students. The experience has definitely had a positive impact on my students. A direct result of the students participating in this program has been increased interest in campus and other students asking if they can take the course next year.

Student 1
The CyberNEXS Pilot program was extremely helpful in preparing for the CyberPatriot competition as well as learning basic security. They covered general policies for security as well as very specific ways to make your computer more secure. The quizzes were helpful in recalling the important points of the lessons covered and the labs allowed us to practice and experience the material hands on. The only thing that I think could use improvement would be possibly breaking up the lessons with the different parts of the lab because it is sometimes a lot of information to digest. Covering one topic at a time then learning how to do it in the lab would be easier to understand and remember.

Student 2
So far the CyberNEXS competition has been really interesting. It really makes me think about what we can do to make our computers more secure and safer to work with. I also believe that the labs for the different computers were really helpful (I really like working with the virtual machines). Overall, it has been a really positive and enjoyable experience! :)

Student 3
I like how this program uses the virtual machine, so we can have an idea of how the rounds will be like, but it only used two types of servers, so it would be better if the program used a variety of servers, so we can be better prepared for other servers in the rounds. The program has the getmystatus.org so we can check the vulnerabilities in the machine, but it would be better if they also provided a description of what we solved, and how we solved it.

Student 4
These past weeks have been filled with fun. I truly enjoy being on the CyberNEXS team and learning more about computers and the mechanisms of

computers. I have learned a lot of new information about how to successfully secure the information on my computer and keep it away from any predators. I also enjoyed working with my team, they have been very encouraging and supportive during not only the competition, but also when working on the labs. We always have each other to ask about any questions or problems that arise.

The lessons were very informational. However, I believe that shorter lessons would be better. Many people get tired after listening to one person talk for quite a long time. The labs, on the other hand, were interesting. It taught me new things about computers and security. It was also a good experience to do apply everything I have learned to secure the image. The quizzes that were incorporated within the lab is good because it causes me to think and remember what I have learned from the lesson. While doing some of the quizzes, I had to research some information, which allowed me to memorize it better for future references.

Student 5
Digital Engineering class is a very interesting class. It helps us to understand more about internet security that not so many students are aware of. There are many advantages of taking this course. One of the biggest advantages is we can protect our own computers. We've learned how to fix the vulnerabilities, how to use MBSA (Microsoft baseline Security Analyzer), protect our private information from hackers, etc. In addition, the interesting activity in class is sharing what security issues are happening in our world today. It helps us to understand better and be more aware of internet security problems. Now I can be more safe and be careful when I use computers.

Another advantage of taking this class is that we learn how to work and communicate with each other which promotes sociability, teamwork, and friendship. Class is relaxing and enjoyable.

The weaknesses of this class are the class labs and lessons. I personally wish there are more specific activities that help us to learn more. Going through all the lessons are little bit boring and pretty long so we often get to skip some parts of the lessons which can be important. Overall, I really like this class and highly recommended to students. :)

Mentor 1
I know that we have been working on Huntsville training, specifically, but I would like to let you guys know what just happened on the national Cyber Patriot competition (http://www.uscyberpatriot.org). I can honestly say that without the extra training we went through with the Huntsville Pilot Program, I doubt we would have seen the improvement that our team experienced: they went from starting out cold as a newbie team (scoring only 2 of 10 in the practice round), to middle of the stack in Round 1, all the way up to place second in Round 2!! I attached my score tally sheet so you could follow the conversation, below. Basically, we made an appeal to be carried forward because we improved SO much that we would have been excluded based on the previous round score even in spite of the fact that we placed 2nd in the next round - they granted our appeal!!!

III. CONCLUSION

The pilot achieved its goals: to demonstrate that procedures and tools currently exist to establish successful eLearning programs in cyber skills, while providing weaknesses and strengths for future reference. With formalized curricula, learning management systems (LMS) to deliver instructional materials, and online realistic training environments that provide real-time feedback, the U.S. educational system should find the means to immediately implement a nationwide program.

Survey results, as well as educator and student comments, show that a similar program, with changes as noted in Lessons Learned, would be highly welcomed. The students' scores, schools' level of participation and teacher feedback has been excellent. Overall, the program was evaluated as successful; the majority of teachers and students who participated were enthused and are already wondering, "What's the next step? How can we continue this momentum?