INL/EXT-15-37262

Success in Industrial Control System Cyber Security Training

Emilee Harris

January 2016

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-15-37262

Success in Industrial Control System Cyber Security Training

Emilee Harris

January 2016

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Assistant Secretary for ____, OR Office of ____
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Success in Industrial Control System Cyber Security Training

Emilee Harris
Instructional Designer
Idaho National Laboratory

Cyber attacks on critical infrastructure (CI) are a growing problem. Every day, there are disclosures about vulnerabilities in computer systems that run CIs as well as news reports describing attacks against these vital systems. The rate of change regarding CI cyber risk has been astonishing; and in the last year, public reports of targeted attacks specific to water, energy, transportation, and pipelines are increasing.[1]

There has been progress in strengthening the resiliency of our control systems. However, most critical systems depend on technology that was not designed to protect those systems against the types of attacks seen today, including those that exploit new vulnerabilities in software and hardware. For every vulnerability that gets disclosed [to a software or hardware vendor so that they can provide a patch before the vulnerability is disclosed to the public], there are many more that have not been disclosed. New vulnerabilities in control system software and hardware/firmware are reported on a continuous basis via public and non-public forums such as security conferences, underground channels, chat boards, and the hacker community. For example, security researchers disclosed 32 vulnerabilities that affected mobile devices and Supervisory Control and Data Acquisition systems at the Black Hat 2015 security conference.[2]

America's economic and national security relies on the resilience and reliability of the Nation's CI. Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," calls for a national unity of effort to strengthen and maintain secure, functioning, and resilient CI.[3] Executive Order 13636 issued the same day noted that "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." [4]

The Idaho National Laboratory's (INL) Homeland Security Division (HSD) has developed an exceptional workforce training program. The program is having a positive effect on the security of our nation's CI. The foundation of INL's HSD training program is the application of a systems approach to training that includes blended learning.

Systems Approach

INL's HSD training group employs a systematic approach to workforce development and training. The concept of a systems approach to training is based on obtaining an overall view of the learning process. It is characterized by an orderly process for gathering and analyzing

collective and individual performance requirements, and the ability to respond to identified learning and training needs. The application of a systems approach ensures that learning programs and the required support materials are continually developed in an effective and efficient manner to match the variety of needs in a rapidly changing environment, such as CI where control system security personnel must respond to newly found vulnerabilities and increasingly sophisticated threat actors.

INL's HSD training group uses a five phase process called the ADDIE model: analysis, design, development, implementation, and evaluation. The first four phases are normally sequential with the output of one phase providing input to the next.

A training analysis ensures that training programs are oriented specifically to the requirements of a job and its associated tasks. The analysis phase identifies the data that serve as the foundation for the systematic development or revision of training. Analysis data are obtained from examining organizational, job, and employee needs. The results define training goals and the scope of the training effort. In addition to training, other interventions may be appropriate such as information, feedback, job aids, task redesign, updated position descriptions, and process improvements.

During the design process, the overall direction and desired outcomes of the training program are determined. Terminal objectives are developed using the data obtained during the analysis phase, and the skills and knowledge identified in the task analysis are translated into enabling objectives. The identified objectives guide the development of all training materials, tests, and delivery strategies and are used to create a design plan for the development of the training.

All instructional materials, including lesson plans, training materials, guides, training aids, and trainee materials, are created during the development process and are based on the preceding design plan. The development of additional enabling objectives, test items, rewording of objectives, etc., may also occur during this process. Both technical and instructional reviews of the products of program development are conducted. Recommendations are incorporated as necessary so that program content is both technically and educationally sound.

The implementation phase consists of activities related to the actual implementation and delivery of training as well as resource allocation, planning, and scheduling. Program

implementation includes assigning instructors and support staff as well as scheduling training, students, and facilities. During implementation, qualified instructors conduct training, and students are evaluated to verify mastery of the objectives.

The evaluation and determination of training effectiveness is a critical component of the systems approach to training process. Training programs are evaluated for adequacy of content, testing, presentation, documentation, and post-training job performance to verify the training delivered is being effectively applied to the work setting and generating the desired outcome. The evaluation process provides critical feedback to identify whether the training is up to date and reflective of the current job. Feedback obtained from instructors, students, and supervisors is reviewed for its potential effect on future training programs. The evaluation data, generated at the conclusion of the program, focus on the consistency and relevance of the completed program. The feedback received from the evaluation process is used to modify and improve program content and delivery. The program content is monitored, and revisions are made as a result of changes in areas such as policies or procedures, system or component design, new or improved control system security methodologies, job requirements, regulatory requirements, and industry guidelines or commitments. Adjustments are also made as a result of analyses of operating experience information such as occurrence reports and other applicable sources.[5]

Blended Learning

Prior to incorporating blended learning, the INL's HSD training group offered several classroom courses, ranging from 2 hours of training up to 40 hours of training. Course feedback from trainees identified several needed improvements and these were addressed by adopting a blended learning approach.

First, trainees asked that the materials be made available in a format that is more efficient to access. A suggestion was that the course in its entirety be provided online for trainees to access on their own time and in a setting that allows for an asynchronous interaction, and self paced to better fit the trainees' work schedules.

Second, trainees identified several redundancies in training materials provided throughout the control system cyber security training courses. As the training program matured and course materials were developed to support its growth, the courses were designed to build on each other.

Ideally, a trainee would take an introduction to control system cyber security course, followed by an intermediate level course, eventually completing a technical level course.

However, it was not realistic to enforce a hard prerequisite for attending the courses as the target audience is made up of employees working in many different industries and located nationally and internationally. As a result, the courses have to accommodate trainees with different knowledge levels, and so some trainees encounter redundant materials during higher-level classes, while others who had not taken the introductory level course(s) felt unprepared.

In an effort to address this problem and make the courses more meaningful for everyone in attendance, the training team included content with some basic information technology and industrial control system information in the higher-level courses. Obviously, this still left some trainees disengaged during a small portion of the class specific to material with which they were already familiar. However, the return on investment of bringing all trainees up to the same knowledge level by mid morning of the course allowed for better use of the rest of the day and a more engaged class as a whole.

Finally, travel was involved in attending the control system cyber security courses. Travel has been either curtailed or limited for trainees because of the state of the economy and budget restrictions, thus limiting trainees' access to the courses. To help with this issue, multi-day training events are scheduled in various areas of the United States providing easier access to training by more individuals without having to travel long distances.

In the past, instructor-led and web-based training have remained largely separate because they use different media and training method combinations. For example, traditional instructor-led training typically occurs in a live, synchronous, interactive environment with person-to-person interaction. Whereas, web-based training emphasizes self-paced learning with interactive learning materials that typically occur in an asynchronous, low-fidelity (text only) environment (see Figure 1).[6]

The advancement in technology has led to the ability to integrate many digital or multimedia elements into instructor-led classroom courses. For example, courses have integrated videos and interactive demonstrations. In addition, there is an increase in virtual media used to simulate instructor-led training in a web-based manner. An example of this is attending a

professional conference virtually from your desktop computer. The intersection of the two, instructor-led and web-based, depict where blended learning systems are emerging.

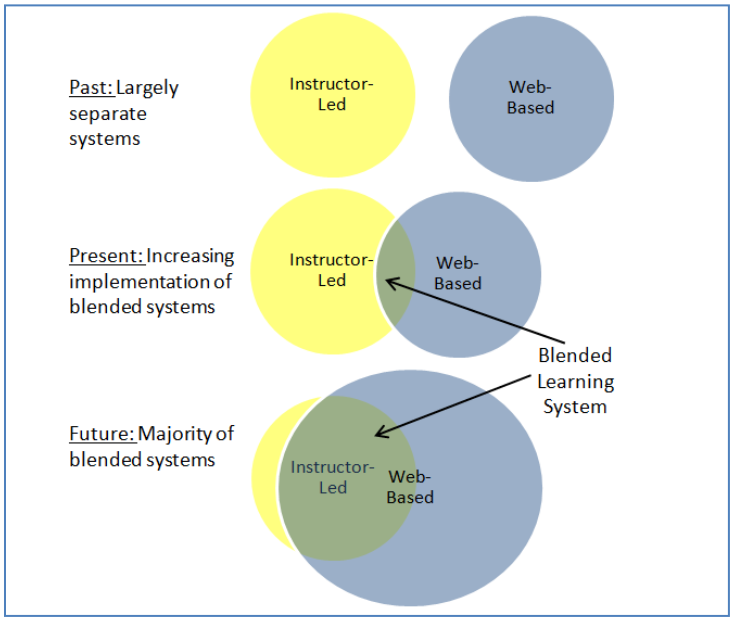

Figure 1. Progressive Convergence of Traditional Instructor-Led and Web-Based Environments Allowing Development of Blended Learning Systems.

One of the most commonly cited reasons for blended learning is more effective pedagogical practices (developing curriculum that provides multiple opportunities for trainees to engage in intellectual and real-world learning experiences).

One example of this is a learning model developed by IBM where learners go through three phases: (1) online, self-paced learning to acquire background information; (2) instructor-led learning lab focused on application experiences rather than lecture; and (3) online learning that supports transfer of knowledge into the workforce.[7]

A similar strategy developed by Brigham Young University uses online modules to help trainees acquire tool-related skills and technical information. Then, uses instructor-led class time to focus on application, case studies, and develop decision-making skills.[8]

Offering a blended approach makes materials available to trainees in situations where they were not previously available. Trainees are given flexibility and convenience as more mature trainees often balance learning with outside commitments such as work and family.

Lastly, blended learning provides an opportunity for reaching a large, globally dispersed audience in a short period of time with consistent content delivery. Adopting this type of approach can cut the costs associated with attending training. As well as affording the opportunity for trainees to participate in training they might not be able to otherwise.

In order to fully adopt a blended learning approach, the training team uses a learning management system (LMS). An LMS is a software application for the administration, documentation, tracking, reporting, and delivery of training courses. It was necessary to have a place to house the web-based training and associated materials that trainees could access internationally. The benefits of using the LMS include:

- Creating a unique user ID that provides for user status tracking and credit for course completion;
- Providing training courses using varied multimedia approaches;
- Facilitating interoperability between eLearning software products through compliance with Sharable Content Object Reference Mode (SCORM);
- Enabling live training events, training invitations, self-registration, and attendance tracking; and
- Assisting in tracking, analyzing and reporting course statistics, and ensuring course availability on desktop or mobile devices – iPads, iPhones, or Android devices.

Since March of 2014 (when the LMS was implemented), over 11,000 trainees have registered for at least one course. The trainees are from all 16 identified CI sectors, including owners and operators of control systems in the Federal government sector, and from multiple states and countries. Many trainees are completing web-based modules prior to attending instructor-led courses. In addition, the training team has offered over 25 instructor-led training sessions with over 1,200 in attendance in the last year. A recent impact evaluation found that over 90 percent of trainees are using the control system cyber security principles and concepts learned in class.

Training is a critical component in the effort to strengthen and maintain secure, functioning, and resilient CI. INL's HSD training group performs outreach activities through

training and education programs to help CI sectors and the control systems community better understand the risks associated with ICSs. The team has had great success in aiding this mission using a systems approach to developing training and blended learning methods.

---

[1] Robert K. Ackerman, "Destructive Cyber Attacks Increase in Frequency, Sophistication," *SIGNAL*, July 1, 2015, accessed November 13, 2015, http://www.afcea.org/content/?q=Article-destructive-cyber-attacks-increase-frequency-sophistication

[2] Darren Pauli, "Black Hat 2015: 32 SCADA, mobile zero-day vulns will drop," *The Register*, July 21, 2015, accessed November 13, 2015, http://www.theregister.co.uk/2015/07/21/black_hat_2015_32_scada_mobile_zerodays_will_drop/

[3] "Presidential Policy Directive – Critical Infrastructure Security and Resilience," The White House, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[4] "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity," The White House, February 12, 2013, accessed July 15, 2015, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[5] Summary of ADDIE Phases: DOE-STD-1077-94, "Training Accreditation Program Standard: Requirements and Guidelines," June 13, 1996, http://energy.gov/sites/prod/files/2013/07/f2/std1077.pdf

[6] Curtis J. Bonk and Charles R. Graham, *The Handbook of Blended Learning: Global Perspectives, Local Designs.* (San Francisco: Pfeiffer, 2006), 5-6.

[7] Curtis J. Bonk and Charles R. Graham, *The Handbook of Blended Learning: Global Perspectives, Local Designs.* (San Francisco: Pfeiffer, 2006), 61-74.

[8] D.M. Cottrell and R.A. Robinson. "Blended Learning in an Accounting Course," *The Quarterly Review of Distance Education* (2003): 261-269.