Computer Security TRAINING

Mr. PATRICK, Donald

Pacific Northwest National Lab

Richland, USA

Email: drpatrick@pnnl.gov

**Abstract**

Computers and the internet have changed our lives for the good in many ways, but with change comes risk. Risk must be properly managed to ensure the safe keeping of nuclear resources. Training is one management method to reduce risk in a nuclear regime. Training when properly implemented, with an appropriate instructional strategy is a key factor to reducing risk. There are multiple ways to train personnel; however, to properly engage learners and have the key principles transferred to their work environment within their computer security programs, there are two main instructional strategies that should be used at the early stages of a computer security program. One is for basic concepts and principles that are foundational knowledge while the other is for advanced concepts that are meant to be taken away and applied in their work environment.

Staff from the International Atomic Energy Agency (IAEA), the U.S. Department of Energy’s National Nuclear Security Administration (NNSA) and subject matter experts from National Laboratories – Idaho National Laboratory, Pacific Northwest National Laboratory, and Los Alamos National Laboratory – worked together for two years to develop and design the first ever international training course (ITC) on *Protecting Computer-Based Systems in Nuclear Security Regimes*. Years of hard work created the inaugural ITC, which brought together 37 participants from 13 countries for two weeks of fully immersive training on best practices in computer security. It was hosted by the Idaho National Laboratory, in Idaho Falls, ID from 1 – 12 October. The course was intended to be the first in a series of IAEA informational computer security ITCs, focusing on raising awareness of the threat of computer attacks, and their potential impact on nuclear security. The instructional strategy and approach to the training was unique in many ways and differed from other trainings delivered in the past. It incorporated very specific instructional techniques to help the learners take away key principles and apply them to their specific situations [3].

## INTRODUCTION

This paper explores the findings of the ITC on *Protecting Computer-Based Systems in Nuclear Security Regimes* and discusses the dynamic ways of implementing proper instructional strategies for computer security training programs. It was found computer security training must change from an academic delivery to a more facilitated approach that incorporates stories, scenarios, and case-studies with hands-on exercises for more advanced topics and skills [3][5].

Computers are associated with everything we do in our personal and professional lives. With computers being a large part of not only how we communicate, but how we gain access to facilities, and are even incorporated into our vehicles. We need to take computer security training more seriously. To do so, proper training must be developed with the right instructional strategy that helps learners apply what is taught.

Computers have also become associated with everything we come in contact with. Even the machines we use on a daily basis, such as dishwashers, refrigerators, and even locks on doors. Some are connected to the internet and some are not. Even the machines that are not connected to the internet are vulnerable to malware through being serviced by computers and systems that receive equipment updates from the internet. When a maintenance person connects their scanning tool to a refrigerator to scan what may be wrong with it, a person has allowed a foreign system to gain access to the refrigerator’s computer. If the scanning tool had a bad update from the vendor, it could possibly introduce malware to an appliance used in a home. The risk associated to a refrigerator going bad is not life threatening, unless a person drinks bad milk from a refrigerator not working properly. However, for a nuclear regime, it is a different story, but comparable.

With the rise of computers, many professional fields have been created; one of the most important, being the computer security field. Computer security has grown into a specialized field. Overall computer security specialists and programs have done a good job creating training to help teach others how to reduce risk within nuclear regimes. However, within computer security programs another specialized field is needed to help nuclear regimes stay more secure by creating better training that properly engages learners and helps them apply the new information being taught.

Instructional systems design is critical to effectively create proper training and appropriate instructional strategies. A component of a matured computer security program has a clear instructional strategy within their training program. Clear instructional strategies are created by computer security subject matter experts consulting with an instructional systems designer. An effective instructional strategy has training that helps people apply what is taught. An appropriate instructional strategy aligns with a desired human performance after training has taken place. The specialized field of instructional systems design ensures not only the instructional strategy is appropriate, but training is effective and accomplishes the desired outcome of the key objective and reason for the training.

## APPROACH

The appropriate instructional strategy for entry level computer security training is a critical andragogical approach that motivates learners as well as makes the new material relevant. Relevancy is a key component to motivating adult learners by getting the adult learners to buy-into the new material [2]. Critical andragogy is when adult learners critically think about their current skills or practices within their situations and they critically think about how the new material applies to them. Taking into account, adult learners have prior relevant knowledge and can critically think about how the new information applies to their situation [5]. For computer security training the approach helps them identify ways to implement better computer security techniques within their program. For the ITC it was done through stories, scenarios, and case-studies that learners could relate to. That in-turn motivated them and helped them believe or buy-into the concepts within the training and new material.

Once learners can relate to and believe in the training, they are more committed to their learning outcomes. Then the likelihood of the learners implementing what is taught is significantly increased [2]. The ITC was successful in helping the learners feel they needed to know the principles within the curriculum. On a scale from 1 to 5 participants gave ratings of 4.57, 4.54, 4.66, and 4.3 to the respective delivery medium, finding the approach taken during the ITC helped them retain and apply what was taught [3]. Week 1 was mainly focused on presentations delivered by subject matter experts that incorporated stories, scenarios, and case-studies.

In order to validate whether a learner has implemented what they learned from the curriculum, an instructional systems designer should follow-up with the learners to see what they have implemented on the job. That can be done in a multitude of ways. The most reliable is on the job observations. Then followed up with supervisor interviews and research of extant data for a third data point of validation [4].

However, for more advanced skills to be properly taught and transferred to the job, a more hands-on approach is necessary using a situational cognition approach as the foundation of the instructional strategy. Situational cognition or situated cognition refers to the same approach [1]. Meaning, learners get their hands-on equipment and apply some of the techniques taught within their training. They also take what they knew before the course and combine that with the new skills, then relate the new skills to their program. The most critical part of situational cognition in a learning environment is to create a safe place for learners to experiment and learn from their mistakes.

That is done by creating hands-on scenarios that are similar to their environments and their program. It lets them play in an environment and experience what happens when mistakes are made without an incident within their program. Another key component is having subject matter experts available to oversee their experiences and share their “war stories” with the learners while they practice on the equipment. The ITC was successful in incorporating subject matter experts within the curriculum delivery and included their experiences.

The data from the after-action report support’s the success. On a scale from 1 to 5, learners felt the delivery was successful in helping them retain and apply their new knowledge.

During the ITC 97% of learners said they will implement principles they learned. It was also found, through the hands-on demonstrations and capstone at the end of the training, learners not only started to master higher level skills, but enjoyed the training and had significant interactions with other learners in the class, which was a main goal for the IAEA. Through stories from the subject matter expert instructors, the scenarios, and the case-studies, learners bought into the need to learn the new material. Then from the hands-on experiences with the equipment to experience principles taught, learners were significantly more engaged and felt they could implement the new skills [3].

Below are the overall goals of the course that were not only achieved, but exceeded all expectations:

* Create awareness of cyber threats, the potential impacts to nuclear security, and identify resources and tools to meet this challenge;
* Describe IAEA guidance, international standards, and industry good practices specific to computer security for systems responsible for:
  + Nuclear safety;
  + Nuclear security;
  + Nuclear material accountancy and control;
  + Sensitive information management.
* Demonstrate approaches and share lessons learned from implementing computer security across the nuclear industry.

The IAEA and NNSA had the shared goal of developing a course that would create an awareness of computer security and allow for a collaborative learning experience. Their expected outcomes were to:

* Foster collaboration among participants;
* Develop a product that only requires minor modifications for sustainment of material;
* Create an experience that allows participants to follow the curriculum and Shapash [fictitious facility] narrative for the entire two weeks.

As quoted from the After-Action Report for the ITC, “by all accounts (observed and documented in survey responses), these expected outcomes were achieved. An unanticipated but very welcome outcome was that participants began to apply what they were learning by the fourth day [3].”

The following process is the approach that was taken to create the ITC on *Protecting Computer-Based Systems in Nuclear Security Regimes* and implement the two instructional strategies discussed earlier in this paper [3].

* Identified a team of computer security experts and an instructional designer:
  + Experts were critical to keep the stories relatable and real for the learners.
* Clearly defined the instructional strategies that aligned to adult learning behaviours;
  + Critical andragogical approach with:
    - Stories;
    - Scenarios;
    - Case studies.
  + Situational cognition with hands-on exercises.
* Reduced PowerPoint and made a more cause and effect learning environment:
  + Created a safe learning environment to make mistakes;
  + Helped learners feel and experience the principles being taught.
* Created stories, scenarios, and case-studies;
  + Ensured they were relevant;
  + Delivered by subject matter experts.
* Created life-like demonstrations with training equipment;
  + Made the exercises and demonstrations life-like and similar to the learner’s environment.

With the alignment of the instructional strategies and the goals of the stakeholder’s success was achieved, but not without a lot of hard work to ensure the strategy was throughout the curriculum. The oversight of the instructional systems designer played a critical path for the overall curriculum. There were many reviews and touch points throughout the process. The instructional systems designer created instructor guides to help the instructors stay on task during the facilitation of the curriculum. The guides were not meant to constrain the subject matter expert instructors, but rather to remind them of key strategies such as the story telling of “war stories” during their delivery.

## conclusion

With the appropriate instructional strategy optimal learning and improved human performance will take place. The ITC on *Protecting Computer-Based Systems in Nuclear Security Regimes* is an example of effective training delivered to improve computer security. The ITC significantly exceeded all expectations by implementing the appropriate instructional strategies and exceeded all expectations according to participants, facilitators, observers, and sponsors.

Going forward it was recommended to always include an instructional systems designer to collaborate with subject matter experts to ensure an appropriate instructional strategy is implemented to properly engage learners. It was also recommended to include interactive discussions with the subject matter expert instructors and the learners to allow for more focussed stories to be shared that the learners could relate to [3].

References

1. DRISCOLL, M., PSYCHOLOGY OF LEARNING FOR INSTRUCTION, Second Edition, Allyn and Bacon, A Pearson Education Co., Needham Heights, Massachusetts (2000).
2. KELLER, J. M., Strategies for Stimulating the Motivation to Learn, Performance and Instruction Journal, Wiley Periodicals, Inc., A Wiley Company, Hoboken, New Jersey (1987).
3. PATRICK, D.R., GEHRIG, L.K., IAEA Computer Security ITC 1.0 After Action Report, Pacific Northwest National Laboratory (2018).
4. PHILLIPS, J.J., Investing in Your Company’s Human Capital, American Management Association, 1601 Broadway New York, NY (2005).
5. MERRIAM, S.B., Learning in Adulthood, Josey Bass A Wiley Imprint, 989 Market St, San Fransisco, Ca (1999).