

Computer Security Training

Computers and the internet have changed our lives for the good in many ways, but with the change comes risk. In a nuclear regime, risk must be managed appropriately, and to do so, personnel must be properly trained.

1. INTRODUCTION

This paper explores the findings of the first-ever international training course (ITC) on Protecting Computer-Based Systems in Nuclear Security Regimes, and discusses dynamic ways of implementing a proper instructional strategy for a computer security training program. Computer security training must shift from a less academic feel to a facilitated approach with a more hands-on delivery technique that incorporates, stories, case studies, and scenarios.

Computer security has grown into a specialized field to help nuclear regimes stay secure. A good computer security training program has training that helps people apply what is taught. An appropriate instructional strategy aligns with a desired human performance after training has taken place.

2. APPROACH

The appropriate instructional strategy for entry level computer security training is a critical andragogical approach. Meaning, it has adult learners critically thinking about their current practices and helps them identify ways to implement better computer security techniques. This is done through case studies, scenarios, and stories that learners can relate to; that helps learners believe in the training. Once learners believe in the training, they will be more committed to their learning and will feel they need to know the principles taught. Then the likelihood of the learners implementing what is taught increases .

However, for more advanced skills a more hands-on approach is necessary using a situational cognition approach as the foundation of the instructional strategy. Meaning, learners get their hands-on equipment and apply some of the techniques taught within the training. 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.

During the first ever ITC on Protecting Computer-Based Systems in Nuclear Security Regimes, 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. The following 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.

- Identified a team of cyber security experts and an instructional designer
- Clearly defined the instructional strategies that aligned to adult learning behaviours
- Reduced PowerPoint and made a more cause and effect learning environment
- Created case-studies, stories, and scenarios
- Created life-like demonstrations with training equipment

3. 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 delivery to improve computer security.

Gender

State

United States

Author: PATRICK, Donald (Pacific Northwest National Laboratory)

Presenter: PATRICK, Donald (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security