Cyber ranges - real world skills development for OT & IT cybersecurity education

39: CYBER RANGES – REAL WORLD SKILLS DEVELOPMENT FOR OT & IT CYBERSECURITY EDUCATION

Dr George D. O'Mahony [a]*, *Paudie Walsh* [b], *Killian Sanceo* [c], *Dean Brennan* [a], *Dr Muzaffar Rao* [b], *Prof. Thomas Newe* [b] *& Prof. Donna O'Shea* [a]

[a] Dept. Computer Science, Munster Technological University, Cork, Ireland,

[b] Dept. Electronic & Computer Engineering, University of Limerick, Limerick, Ireland,

c Airbus Defence and Space Cyber,

Emerging Sensing Strategies and Applications, EM010, August 14, 2024, 9:30 AM - 10:30 AM

Abstract **−** Cybersecurity has emerged as a primary concern for governments, organizations, and citizens. However, a significant deficit persists in the number of available cybersecurity professionals and the skill sets of those already in the field. This characteristic results in insufficient numbers of skilled professionals and doubts among companies regarding graduates' readiness for the workforce due to perceived inadequacies in essential skills. Additionally, cyberattacks are prevalent but the consequences mean professionals aim to prevent as many breaches as possible and reduce the impact, contain and eradicate any attack that exploit a system. The problem that arises is that cyber security professionals require realistic breach scenarios and cyberattacks to train and become sufficiently skilled but cyber professionals are consistently working hard to prevent such attacks in the real-world. The research question that this paper explores is how do we train cyber security professionals to deal with the challenging ever-changing cyber environment and ensure new technologies will not negatively impact security? This paper investigates the use of Cyber Range technology, particularly a mobile cyber range, as the identified solution in education.

Figure 1: Airbus Mobile Cyber Range

A cyber range is a secure sandbox environment designed to provide hands-on training and research and development in cybersecurity. This virtual environment is designed to mimic real-world enterprise infrastructures including Information and communications technology (ICT), operational technology (OT), mobile, software and physical systems, applications, networking systems, traffic, and threats, allowing users to interact with and respond to dynamic and challenging cybersecurity scenarios. The mobile cyber range enables the simulation/emulation of cyber-attacks, users and their activities. For this paper, an Airbus Mobile Cyber Range, Figure 1, will be utilized in the context of understanding the importance of cyber range technology for education and skill development. The mobile Cyber Range provides additional capabilities for cybersecurity skill development as it includes a physical switch that can be connected to lab environments, specific hardware and Internet of Things (IoT) networks deployed on physical assets such as monitoring and control systems. Additionally, the cyber range environment can load software applications for security skills assessment or for the gamification of cybersecurity education.

In cybersecurity education, this paper explores several critical benefits that the mobile cyber range offers for skill development across IT, OT and IoT domains, including:

- Realistic Simulation: The cyber range provide a safe, controlled environment where students can encounter the types of cyber threats they will face in real-world scenarios. This practical experience is invaluable for understanding the complexities and dynamics of enterprise security.
- Hands-on Learning: By engaging directly with the systems and tools used in cybersecurity, learners can develop practical skills that are difficult to acquire through traditional lecture-based education.
- Skill Assessment and Enhancement: Cyber ranges allow both instructors and learners to assess skills in a tangible way, through, for example, capture the flag, gamified learning scenarios where users can receive immediate feedback on their actions and decisions, helping them to improve and refine their capabilities over time.
- Projects: These environments are ideal for developing university level cybersecurity projects for additional hands-on research and skill development without the risk of affecting real networks. This encourages innovation and experimentation, leading to advancements in security practices and tools.

- Teamwork and Collaboration: Cybersecurity often requires coordinated efforts among various team members. The cyber range can simulate multi-threat scenarios that necessitate teamwork, thus helping learners to develop communication and collaboration skills crucial for effective incident response.
- Compliance and Best Practices: With cyber range technology, educators can ensure that their students are well-versed in compliance requirements and industry best practices. This is essential for maintaining security standards and protecting against legal or financial repercussions.

Overall, this paper analyses how the mobile cyber range is a requirement for modern cybersecurity education, equipping individual students with the necessary skills to protect digital assets and respond effectively to incidents. Their role in developing a skilled cybersecurity workforce with real-world applicable skills is vital as threats continue to evolve and increase in sophistication. The work will also emphasise the importance of tailoring the education learning environment using a cyber range to create a positive student experience and combat the current skills deficit in this crucial area.