Human Factors in Cybersecurity, Vol. 127, 2024, 19–29
https://doi.org/10.54941/ahfe1004762

Interactive Virtual Learning Environment to Develop Next-Generation Cybersecurity Practitioner Competency

Rahmira Rufus[1,2], Ulku Clark[1,2], Geoffrey Stoker[1,2], Jeff Greer[1,2], and Thomas Johnston[1,2]

[1]University of North Carolina, Wilmington, NC 28403, USA
[2]University of Maryland, Adelphi, MD 20783, USA

ABSTRACT

This paper groups simulated behavioral, technical and operational elements of a 'real enterprise' for cybersecurity awareness, education and training (AET) evaluation. The research goal is developing next-generation cybersecurity practitioner competency congruent to behavioral and socioeconomic aspects of the next generation of computing. Within the cybersecurity knowledge domain, the modern digital enterprise is the system of interest (SOI) that requires enterprise cybersecurity execution to ensure security fitness based upon system state criteria. For this scope of the research, the enterprise is simulated via a web interface engineered to focus on the human entity being the key indicator to the success or failure of the enterprise's security posture. The virtual learning interface is the application domain called the Integrated Virtual Learning Environment for Cybersecurity (IVLE4C). The objective is to leverage ILVE4C as a tool to increase practitioner proficiency, as currently there is tremendous investment focused on secure enterprise digitalization for the next generation of computing. However, there is no specialized engineering workstation for this type of platform. Utilization of the ILVE4C workstation is intended to provide such a platform to enhance the development and efforts of enterprise cyber defenders to address the reduction of this learning curve and to improve this human attack surface factor within the AET space.

Keywords: Virtual learning web technologies, VR/AR systems, Enterprise cybersecurity, Awareness, Education and training (AET), Enterprise computing, Human attack surface, Cybersecurity knowledge domain, Integrated virtual learning environment (IVLE)

INTRODUCTION

Real-world training simulation has proven to be an effective approach to bridging learning gaps. Industries demonstrating transformational improvements by leveraging simulated training include healthcare, aviation, the military, etc. As a result, significant improvements in the knowledge base, intuitiveness, skills application and confidence of the practitioner were evident (Harvey, 2023). By implementing interactive training exercises, these immersive learning experiences help employ multilevel sensory learning development (Parsons, 2021). Such realistic operating environment (OE) execution is a requirement for critical infrastructure awareness, education and training (AET). Real-world training simulations for virtual application domains also incorporate multilevel sensory learning development to enhance the effectiveness of training programs. By engaging the senses, simulations can create a realistic learning environment, leading to improved retention and transfer of knowledge (Taljaard, 2016). Multisensory simulation can enhance training effectiveness by engaging learners through multiple sensory modalities (Volpe and Gori, 2019). Multisensory instruction can facilitate the transfer of training to real-world tasks and improve overall training outcomes. Additional to training outcomes, sensory modalities play a major role in virtual reality training because the integration of multiple senses can also lead to more effective learning outcomes. This approach is particularly beneficial for skills that require hands-on practice or exposure to complex scenarios.

ENCAPSULATE THE ENTERPRISE AS A DIGITAL CONSTRUCT

According to Clark et al. in the cybersecurity knowledge domain, enterprise cybersecurity stands out and requires special attention for two key reasons. Firstly, a contemporary digital enterprise constitutes a complex and expansive network of interconnected digital systems. Secondly, such enterprises rely heavily on their supply chains, making them interconnected and interdependent. Consequently, the combined digital enterprise and its supply chain present an extensive attack surface, inherently laden with risks that must be addressed to achieve security objectives. As the digital transformation nears completion, the emerging workforce tasked with developing, deploying and maintaining enterprise security faces significant challenges. Cybersecurity students and practitioners in training often struggle due to a lack of context regarding the operational intricacies, organizational structure, and control mechanisms within a modern digital enterprise. The successful discovery Clark et al. made to bridge the knowledge gaps across these complex scenarios offered insight for guidance into how to develop required knowledge, skills, and abilities (KSAs) for accelerating cyber defender practitioner success rates. This discovery provided an alternative to the limitations students face with acquiring knowledge that is primarily "accomplished with experiential learning post-graduation" (Clark et al., 2023).

There is tremendous investment in securing enterprise digitalization and currently there is no specialized engineering workstation for this type of work. The research goal is developing next-generation cybersecurity practitioner competency utilizing all-encompassing and multi-disciplinary approaches to address behavioral and socioeconomic aspects for the next generation of computing. Specifically, the work needed to address why further improvements were required for enterprise cyber risk management, which specifies the need for a trusted supply chain and run time environment amongst other specifications. In this work, an interactive virtual learning environment (IVLE) training simulator for student and working practitioner use is developed as a tool for studying an enterprise cybersecurity discipline. More importantly, this work focuses on incorporating aspects of the six-sigma process improvement variation principles. We leverage this classical industrial engineering approach with pedagogy methods to demonstrate a correlation, via the People, Process and Technology (PPT) framework. This correlation is significant in assessing the effectiveness of the virtual learning environment (VLE) as being a viable tool to increase enterprise cybersecurity proficiency to balance the business operations or change management that innately occurs in the ‘real-world enterprise’.

Bringing aspects of the real-world enterprise into simulated OEs require that critical enterprise elements be encapsulated to effectively assess the behavioral, technical and operational considerations within an organization (see Table 1). A simplistic mapping amongst the enterprise elements, the six-sigma 6Ms and the PPT framework demonstrate how bridging process improvements to identify and fix process problems or variations can be modeled via a representative enterprise for training and evaluation. From a high-level viewpoint, elements of the 6Ms and PPT framework are combined to map to each enterprise element. At a more granular level, deeper inspection of these correlations is also performed to focus on each enterprise element.

Table 1. Mapping 6Ms and PPT framework to real-world application of enterprise elements.

Six-Sigma 6Ms	PPT Framework	Enterprise Elements
Manpower	People	Behavioral
Machine	Technology	Technical & Operational
Method	Process	Behavioral & Operational
Materials	Process	Behavioral & Technical
Measurements	Process & Technology	Operational
Mother Nature	Process & Technology	Technical & Operational

HIGH-LEVEL MAPPING (LEVEL 1)

The combination of six-sigma and the PPT framework involves aligning each component (see Table 2). Mapping 6Ms and PPT framework as combined components to enterprise behavioral, technical, and operational elements involves associating each combined component with aspects related to behavior, technology and operations within an organization. The alignment derived from these combinations establish the basis for how enterprise behavior, technique and operations should be approached when it comes to how an organization should work in harmony to achieve successful business operations or change management.

Table 2. 6Ms & PPT combined components to align Table 1 elements.

6Ms & PPT Aligned	Combined Components (6Ms &PPT) Description
Manpower → People	Manpower directly relates to People component; encompass human resources involved in operations, including their skills, knowledge & abilities.

(continued)

Table 2. Continued

6Ms & PPT Aligned	Combined Components (6Ms &PPT) Description
Machinery → Technology	Machinery aligns closely with Technology component; involves the equipment & physical assets used in operations.
Method → Process	Method aligns with Processes component; refers to the procedures & workflows followed in executing tasks & delivering products or services.
Materials → Process	Material management relates to Processes component; involves the procurement, storage & utilization of resources in operational processes.
Measurements → Process & Technology	Measurement relates to both Processes & Technology; involves use of performance metrics (Processes) & technology tools (Technology) to monitor & evaluate operational performance.
Mother Nature → Process & Technology	Machinery aligns closely with Technology component; involves the equipment & physical assets used in operations.

Mapping the combined components to the enterprise elements (see Table 3) describes how 6Ms and PPT elements can relate to the enterprise elements categories. In Table 3, the enterprise elements are categorized from a high-level perspective to establish the initial associations amongst the combined components of both frameworks before deeper dissection of the enterprise elements are constructed.

Table 3. Combined components alignment to enterprise categories.

6Ms & PPT	Enterprise Category Alignment
Manpower → People	**Behavioral** - relates to behavioral aspect of the enterprise by encompassing aspects such as employee skills, teamwork, leadership & organizational culture.
Machinery → Technology	**Technical & Operational** - primarily falls under the technical & operational aspects of the enterprise by involving technology infrastructure, equipment, maintenance procedures & operational processes.
Method → Process	**Operational & Behavioral** - relates to both operational & behavioral, which involves operational processes, procedures & workflows (Operational). Also, employee behaviors, attitudes toward change & adherence to standardized methods (Behavioral).
Materials → Process	**Operational** - primarily an operational element, involving procurement, inventory management, supply chain logistics & production scheduling.
Measurements → Process & Technology	**Behavioral & Technical** - involves both behavioral & technical to include use of performance metrics, key performance indicators (KPIs) & data analytics (Technical). Also, organizational practices related to performance appraisal, feedback mechanisms &managerial decision-making (Behavioral).
Mother Nature → Process & Technology	**Operational & Technical** - primarily affects operational & technical to include risk management, contingency planning & resilience strategies to mitigate the impact of external environmental factors such as natural disasters, weather events & geopolitical instability.

Managing Enterprise Risk via the Elements (Level 2)

Some aspects of process improvement for fluid operations that can contribute to risk at the high level are, but not limited to following:

- Managing behavioral risk involves 1st understanding and addressing factors such as organizational culture, employee conduct, leadership practices, and ethical considerations. Enterprise behavioral risk refers to the potential for loss or harm arising from human behavior, attitudes, actions or decision-making within an organization.
- Managing technical risk is essential for ensuring the reliability, security and resilience of technological infrastructure and systems. This type of enterprise risk refers to the potential for loss or harm arising from failures or vulnerabilities in technology-related assets, systems, or processes within an organization.
- Managing operational risk is crucial for organizations to safeguard their reputation, financial stability and compliance with regulations. This risk refers to the potential for loss arising from inadequate or failed internal processes, people, systems or external events.

Specifically in operations management, there are some aspects to consider when analyzing various factors that affect improving operational processes at the high level:

- **Behavioral** refers to the human resources involved in executing tasks and managing processes. This includes aspects such as workforce skills, training, allocation, and productivity. Understanding manpower-related risks can help in workforce planning, skill development and ensuring adequate staffing levels.
- **Technical and operational** elements encompass the equipment, technology and physical assets used in production or service delivery. It involves assessing the reliability, maintenance requirements, capacity and efficiency of machinery. Some risks involved are preventive maintenance, technology upgrades, and contingency planning for equipment failure.
- **Operational and behavioral** refers to the processes, procedures and workflows followed in executing tasks and delivering products or services. Operations managers focus on optimizing methods to enhance efficiency, minimize waste and ensure consistency in output quality. Risks related to this category include process bottlenecks, inefficiencies, lack of standardization and resistance to change.
- **Behavioral and Technical** involves the quantification and analysis of key performance indicators (KPIs) to monitor and evaluate operational performance. This includes metrics related to productivity, quality, lead times and customer satisfaction. Risks associated with this category include inadequate data collection, unreliable metrics, and misinterpretation of performance data. Effective measurement systems incorporate clear KPIs, data validation processes and performance benchmarking against industry standards.

MODEL THE ENTERPRISE ATTACK SURFACE CONDITION

The digital enterprise is multifaceted, requiring a balanced approach to the behavioral, technical and operational elements. In the previous section, the elements were mapped (see Tables 1-3) to align with other enterprise process, business operations and change management components to better address the broad scope categorized in the behavioral, technical and operational elements. Nevertheless, the elements play a crucial role in transforming a traditional organization into a digitally mature entity capable of adapting to rapidly changing market dynamics and leveraging digital technologies, such as the focus in this paper. In this section we model the enterprise attack surface as a condition representative of the following risk criteria: insecure, secure and at-risk states. Each risk state is also assigned a status for construction and utilization of risk reduction methods, capabilities, etc. as a risk treatment plan (RTP), where the status determines each state (see Table 4).

Table 4. Enterprise attack surface risk state criteria.

System State	RTP Status	Description
Insecure	No RTP Present	There is currently no RTP in effect or to reference
Secure	RTP Deployed	There is a RTP currently being deployed & in use
At Risk	RTP Modified	There has been a modification to RTP

The inclusion of the system state classification to model the enterprise's attack surface condition as a state machine, helps to conceptualize the various states where the enterprise's digital assets, services, networks, etc. can exist. Additionally, this occurs along with the transitions between these states triggered by potential security events or attacks. This approach helps in understanding and mapping out potential vulnerabilities, threat vectors and the dynamics of how an attack progresses through a system. For the cyber defender, there is now the opportunity to be nestled within the construct specified for the simulated enterprise (see Figure 1). The nexus amongst modeling the enterprise via its elements, virtualizing the application domain, ability to manage the control plane and reduce the enterprise attack surface are illustrated via the diagram and are the basis for the VLE constructed.

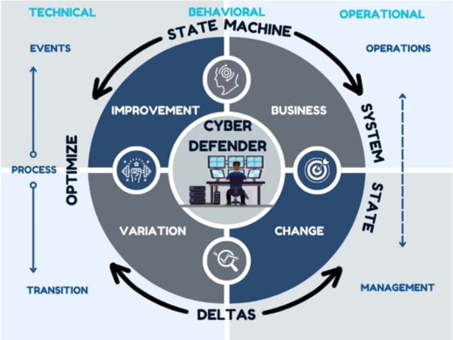


Figure 1: Enterprise components digital model for cyber defender learning.

In essence, the relationship between state machines and system states is foundational to understanding and modeling the dynamic behavior of complex systems. State machines provide a formal framework for describing the sequences of states a system goes through in response to events, including the conditions under which transitions occur and the actions performed during each state (IBM, 2021). This modeling approach is essential to designing, analyzing and implementing systems with predictable and manageable behaviors like what is necessary for controlled learning environments in this instance.

Enterprise Attack Surface as a State Machine

The enterprise attack surface is treated as a state machine where it's modeled via defining states, identifying transitions, mapping attack vectors, incorporating mitigation strategies and by continually updating and performing analysis. The first step is to define the states in which the enterprise's digital assets can exist. These states could range from secure, compromised, under investigation, to being restored, etc. For this paper the system states are specified via the RTP status (see Table 4). Each state represents a condition of the system's security posture. Second, transitions are identified. Transitions are the events or actions that cause the system to change from one state to another. This could include unauthorized access, detection of a vulnerability, the application of a security patch or the occurrence of a security breach. Third is mapping attack vectors, which involves outlining how an attack can move the system from one state to another. For example, exploiting a vulnerability could move a system from a secure state to a compromised state. Fourth, is incorporating mitigation strategies. For each transition that represents a potential security threat, mitigation strategies should be identified. This might involve transitioning to a state of increased security monitoring or applying specific security controls. In this case, the strategies are represented as the RTPs (see Table 4). The final measure is to continually update and perform analysis. As the enterprise evolves and new threats emerge, the state machine modeled should be updated. This ongoing process ensures the model accurately reflects the current attack surface and security posture.

DESIGN THE IVLE4C VIRTUAL LEARNING WORKSTATION

Integrated virtual learning environments (IVLE) involve a complex process that requires a multidisciplinary approach where technology development skills and educational expertise are coupled together. This approach employs best practices in educational technology, user experience design and content strategy to create an engaging and effective online learning experience (Encyclopedia.com, 2023). IVLE4C is a virtual learning platform that focuses on cybersecurity AET. The user interface has the cyber defender working in a virtualized enterprise security operations center (ESOC) as the defender's workstation (see Figure 1). Within this user-centric design, the focus is on usability factors centered around design aspects for accessibility, responsiveness, the visual and auditory sensory modalities, etc. to ensure the operating environment (OE) is effective across different device requirements and user needs. The elements incorporate interaction and engagement to enhance learning that can leverage a multitude of pedagogy tools to manipulate the real-world simulation. Interactive quizzes, videos, discussion forums, skills specific training scenarios, etc. can be utilized via application domains such as IVLE4C. Additionally, on the backend of this web interface is the ability to ingress enterprise risk management and cyber security AET capabilities that support the integration of server-side logic development, distributed repositories, API services, etc. An API service specific to effective operability for learning management systems (LMS) integration is xAPI, as some development use cases have reported that standards like SCORM does not capture the full spectrum of e-learning (xAPI.com, 2023).

Figure 2: IVLE4C enterprise security operations center (ESOC) workstation.

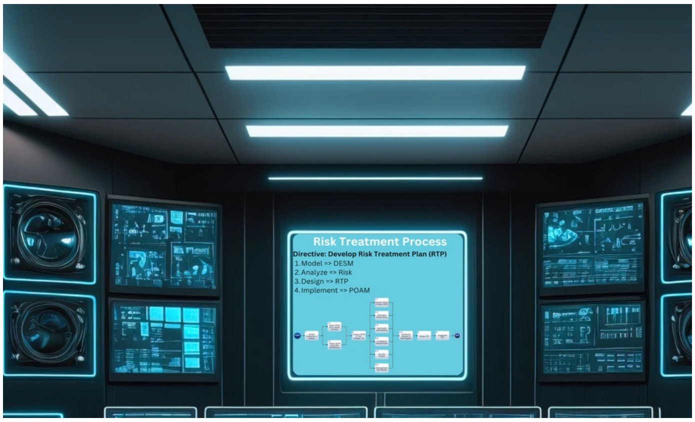
Risk Reduction Learning Tool for the Enterprise Attack Surface

The learning curve objective orchestrated within the IVLE4C workstation is that the primary output of the risk treatment process be a RTP that converts an attack surface into a trust boundary at a level sufficient for enterprise security objective achievement. At a high-level, the process directives are for the cyber defender (end-user) to model aspects of the enterprise via the enterprise elements and progress through the treatment steps to eventually implement a plan satisfying reduction of the attack surface condition (see Table 5).

Table 5. Risk treatment work process high-level view (Clark et al., 2008).

Risk Treatment Process	End-User Directives
1. Model => DESM	User will create, in a database, through parametric definition, an artifact known as a descriptive enterprise system model (DESM)
2. Analyze => RISK	User will create a risk register for a descriptive enterprise system model based on multiple reported factors
3. Design => RTP	User will create a risk treatment plan (RTP) for risks identified in the risk register
4. Implement => POAM	User will create a plan of action and milestones (POAM) for implementing the risk treatment plan

In execution the process steps are divided and represented as an activity diagram within IVLE4C dashboard (see Figure 2). Step 1: model the enterprise of interest, is divided in (1.1), selecting a DESM development template from the model library. After selecting a template to work with, (1.2) creates the DESM using the relative reference architecture (RA) for the DESM specifications. Step 2: performing contextual DESM analysis, divides this step to analyze the DESM in the context for identifying the following aspects of the enterprise via sub steps (2.1-2.6): the desired assets of value (AOV), motivated threat actors, exploitable vulnerabilities, compliance requirements, security scope and the risk management appetite (Clark et al., 2023). Steps 3–4 are where emphasis on both the technical aspects of web development and the pedagogical considerations for effective online learning were heavily scrutinized. The reason is cyber defender competency analysis is the overall research goal but not the direct focus of this paper. However, determining if this approach to IVLEs is an effective method, are within the scope of this work and will influence outcomes for the overall research goals.



Risk Treatment Process

Directive: Develop Risk Treatment Plan (RTP)

1. Model => DESM
2. Analyze => Risk
3. Design => RTP
4. Implement => POAM

Figure 3: Risk treatment process via IVLE4C workstation.

IVLE4C needed to combine best practices in educational technology, user experience (UX) design and content strategy to create an engaging and effective online learning experience. Constructing a web interface involved extensive planning, technology selection, UX design and content creation to ensure an effective and engaging online learning experience. Specific UX and interface design requirements for IVLE4C were identifying the learning goals of the end-user and determining features and functionalities for the virtualized workstation. This meant understanding the educational objectives and needs of the learners.

CONCLUSION

This paper emphasizes that an interactive virtual learning environment (IVLE) can develop next-generation cybersecurity practitioner competency for representative enterprises as the critical infrastructure operating environment (OE). This virtual learning interface is the application domain called the Integrated Virtual Learning Environment for Cybersecurity (IVLE4C). The goal is to leverage ILVE4C as a tool to increase practitioner proficiency. This develops a capability for the practitioner to work vertically and horizontally across the enterprise. As the practitioner uses the IVLE4C workstation, three conditions are observed:

(1) An insecure system state, where no cyber risk management strategy is implemented,
(2) A secure system state, where there is a cyber risk management strategy developed and deployed and
(3) An at-risk system state, which indicates a change in information is used to develop or modify strategy.

The risk management strategies are expressed as treatment plans to mitigate and reduce the effects of the infractions. The practitioner is the cyber defender at the IVLE4C workstation and utilization of the workstation is intended to increase proficiency in enterprise cyber risk management. Within this cybersecurity engineering workstation, which is specifically built for enterprise cyber risk management, we create the nexus and fidelity between the training and work environment. Utilization of the workstation is intended to enhance the development and efforts of enterprise cyber defenders.

Next Steps

The objective in this paper was to encapsulate the real-world enterprise as a digital construct based upon key enterprise elements: behavior, technique and operation, then model the enterprise's attack surface to execute in the application domain. The next phase of the research is to evaluate IVLE4C's effectiveness at converting the attack surface into a trust boundary at a level sufficient for enterprise security objective achievement. Analyses directed at system state transitions, process variation and practitioner proficiency will be conducted.

REFERENCES

Clark, Ulku, Jeff Greer, Rahmira Rufus, and Geoff Stoker. (2023). "A Descriptive Enterprise System Model (DESM) Optimized for Cybersecurity Student and Practitioner Use", Cham: Springer Nature Switzerland. in: International Conference on Human-Computer Interaction, pp. 610–621.

Encyclopedia.com (March 19, 2023) "The Virtual Integrated Teaching and Learning Environment (VITLE): A Cyberspace Innovation." Problem-based Learning in eLearning Breakthroughs. Encyclopedia.com Website: https://www.encyclopedia.com/telecommunications/educational-magazines/virtual-integrated-teaching-and-learning-environment-vitle-cyberspace-innovation.

Harvey, S. (June 13, 2023) "The Importance of Effective Training Programs with Realistic Simulations," Instancy Website: https://www.instancy.com/the-importance-of-effective-training-programs-with-realistic simulations/#:∼: text=Realistic%20simulations%20have%20proven%20transformational, of%20professionals%20in%20these%20sectors.

International Business Machines (IBM) (March 05, 2021) "States, regions, and transitions", IBM Website: https://www.ibm.com/docs/en/rsas/7.5.0?topic=machines-states-regions-transitions.

Parsons, K. A. (April 06, 2021) "How Multilevel Sensory Experience Enhances the Learning Process," Bethatspark Website: https://www.instancy.com/the-importance-of-effective-training-programs-with-realistic-simulations/#: ∼: text=Realistic%20simulations%20have%20proven%20transformational, of%20professionals%20in%20these%20sectors.

Taljaard, J. (2016). A review of multi-sensory technologies in a Science, Technology, Engineering, Arts and Mathematics (STEAM) classroom, Journal of Learning Design Volume 09, No. 2.

Volpe, G., Gori, M. (2019). Multisensory Interactive Technologies for Primary Education: From Science to Technology. *Frontiers in psychology*, *10*, 1076. https: //doi.org/10.3389/fpsyg.2019.01076

xAPI.com (October 23, 2023) "SCORM vs xAPI", xAPI.com Website: https://xapi.com/scorm-vs-the-experience-api-xapi/?utm_source=google&utm_medium=natural_search.