sSimulating Cybersecurity Resilience in Critical Infrastructure: A Role-Based Learning Game for Water Systems

Gul Ayaz, Katherine Smith, and Rafael Diaz
Office of Enterprise Research and Innovation, Old Dominion University
Suffolk, Virginia
gayaz@odu.edu, k3smith@odu.edu, rdiaz@odu.edu

ABSTRACT

As critical infrastructure grows increasingly reliant on digital control systems, it is essential that students are introduced to the world of cybersecurity and equip them with an understanding of how cyber threats can impact real world systems. Traditional cybersecurity education often lacks interactivity, real-world relevance, and career context. Many programs emphasize abstract theory, offering limited engagement with how cyber threats affect essential systems or what actual defense roles involve. To address these gaps, this project presents an interactive, role-based simulation game that teaches students about cyber-attacks and defense strategies in the context of public water systems.

The simulation was designed using pedagogical strategies grounded in scenario-based and experiential learning frameworks. Players engage with evolving cybersecurity scenarios that mimic real-world attacks on water systems, allowing them to apply defense strategies in a safe, simulated environment. Through role-specific tasks and hands-on decision-making, the game supports "learning by doing," a core aspect of experiential learning. Gamification elements such as mini-games and feedback loops help maintain engagement while reinforcing key cybersecurity concepts. A structured narrative guides players through cyber threats, aligning game progression with learning outcomes outlined by the NIST Cybersecurity Framework.

Developed in Unity, the game supports career exploration by embedding tasks that mirror real-world job functions in cybersecurity and infrastructure protection. Players assume roles such as Network Security Engineer, ICS (Industrial Control Systems) Specialist, or Incident Response Coordinator. This paper will outline the game's learning framework, simulation architecture, and role-based mechanics to demonstrate how it supports early cybersecurity education and career engagement.

ABOUT THE AUTHORS

Gul Ayaz is a Game and Extended Reality Developer at the Virginia Modeling and Simulation Analysis Center (VMASC) at Old Dominion University (ODU). She has designed and developed serious and interactive games and immersive experiences relating to digital ship, maritime, and coastal resilience across many disciplines. Ms. Ayaz graduated with a B.S. in Computational Modeling and Simulation Engineering with a concentration in gaming from ODU and is pursuing an M.S. in Modeling and Simulation Engineering.

Katherine Smith, Ph.D., is a Research Assistant Professor in Digital Shipbuilding at ODU VMASC. Dr. Smith received her Ph.D. degree in modeling and simulation engineering, an M.S. in applied computational Mathematics, and B.S. degrees in applied mathematics and mechanical engineering from ODU. She was previously a senior lecturer in the mathematics department at ODU. Her research interests include modeling and simulation of complex systems and networks particularly involving supply chains; data analytics and machine learning especially related to competency evaluation systems and content curation; and serious games and experiences for STEM education.

Rafael Diaz, Ph.D., is a Research Associate Professor at ODU VMASC and Graduate Program Director for the School of Cybersecurity. He was previously affiliated with the MIT Center for Transportation and Logistics and MIT-Zaragoza. He directs the Advanced Analytics Lab and co-directs the Digital Maritime and Shipbuilding Lab. His research includes digital supply chains, AI/ML, prescriptive analytics, homeland security, and cybersecurity.

Simulating Cybersecurity Resilience in Critical Infrastructure: A Role-Based Learning Game for Water Systems

Gul Ayaz, Katherine Smith, and Rafael Diaz
Office of Enterprise Research and Innovation, Old Dominion University
Suffolk, Virginia
gayaz@odu.edu, k3smith@odu.edu, rdiaz@odu.edu

INTRODUCTION

Critical infrastructure systems, such as water utilities, are becoming increasingly reliant on digital technologies. This reliance makes them more susceptible to cyber threats. A report by CISA highlights the increase in pro-Russian hackers targeting industrial control systems withing in water utilities (U.S. Environmental Protection Agency, 2024). Another report by the Environmental Protection Agency (EPA) found that 97 drinking water systems had critical or high-risk vulnerabilities (U.S. Environmental Protection Agency, 2024).These reports highlight persistent vulnerabilities related to cyber threats to critical infrastructure emphasizing the importance for cybersecurity preparedness in the water sector.

Background and Motivation

Existing cybersecurity education often emphasizes theoretical knowledge over hands-on, scenario-driven. The 2024–2025 systematic reviews emphasize the rising value of serious games in cybersecurity education. A 2024 systematic review found over 50 recent games focusing on privacy/security awareness in professional settings (Chaimae Moumouh, 2025; Ng & Hasan, 2025). This gap can leave students underprepared for the types of complex, real-time decision-making required to defend critical infrastructure. A systematic review by Prümmer et al. (Prümmer, van Steen, & van den Berg, 2024) found that many cybersecurity training programs lack interactive components that mirror real-world threats or provide context for industry roles. This is particularly salient in sectors like water utilities, where operational decisions have direct consequences on public safety.

The systemic review also found that most training methods, regardless of the specific cyber topic covered, had positive effects. Among these, game-based methods were the most used. These approaches have shown promise for improving engagement and retention by providing more immersive, scenario-based experiences. However, the review also highlighted limitation in existing research, including small sample sizes.

To address these challenges, this paper introduces Cyber H_2O, a role-based simulation game developed to support teaching foundational cybersecurity concepts in the context of public water systems. The game emphasizes hands-on engagement, decision-making under pressure, and role-specific tasks that align with both the NIST Cybersecurity Framework and the NICE Workforce Framework. By blending interactive mini-games with a structured narrative and feedback-driven learning, Cyber H_2O provides students with experiential practice which will support the development of competencies aligned with cybersecurity frameworks. Although Cyber H_2O is set within the context of public water systems, the underlying design is intended to teach foundational cybersecurity concepts that are transferable across multiple sectors. Concepts such as access control, log analysis, threat detection, and network response are relevant in virtually any critical infrastructure environment, including healthcare, energy, manufacturing, and transportation. By focusing on role-based tasks aligned with the NICE Workforce Framework and emphasizing NIST Cybersecurity Framework functions, the simulation provides students with core competencies that extend beyond the specific domain of water utilities. This makes the game a valuable training tool not just for future water system specialists, but for any learners exploring cybersecurity roles or seeking to build foundational cyber resilience skills. The modular architecture of the game also supports future adaptation to additional infrastructure contexts by simply modifying scenario content or threat types without altering the core mechanics.

EDUCATIONAL FRAMEWORK

Pedagogical Foundations

The simulation game incorporates two complimentary pedagogical approaches; scenario-based learning and experiential learning. These frameworks provide a structured yet flexible way for students to develop technical and cognitive skills essential to cybersecurity defense. To ensure workforce relevance, the simulation is mapped to NICE Workforce Framework for Cybersecurity and the NIST Cybersecurity Framework. This helps align role-based tasks and learning outcomes with national standards for cybersecurity knowledge, skills, and abilities.

Scenario-based learning provides students with problems that mimic real world events. This approach helps narrow the gap between theoretical knowledge and workforce competencies (Gouveia, Lopes, & Vaz de Carvalho, 2011), especially when mapped to frameworks like NICE/NIST. In the Cyber H20 game, players face evolving cybersecurity threats that target water systems, which is a real-world issue. The scenarios reflect realistic attack patterns and have constraints such as time limits and limited attempts. By navigating through simulated crisis, students are introduced to this real-world dilemma and learn not only technical skills but also critical thinking, situational awareness, and decision-making capabilities.

Kolb's Experiential Learning Theory emphasizes a cycle of concrete experience, reflective observation, abstract conceptualization, and active experimentation (Kolb, 1984). In the Cyber H20 games, the players assume specific professional roles such as Network Security Engineer, Industrial Control Systems (ICS) specialist, or Incident Response Coordinator. They are tasked with defending the water treatment plan from cyber threats.

Gamification and Engagement

To sustain engagement and deepen learning, Cyber H_2O incorporates a variety of gamification elements that align with evidence-based practices in educational game design. Central to this are a series of mini-games that simulate key cybersecurity tasks that will be expanded upon in the Game Design and Architecture section. These interactive tasks are hands-on and role-specific, allowing players to experience the types of decisions and pressures encountered in real-world cyber defense.

Each task is supported by immediate feedback loops, which reinforce correct actions and provide real-time consequences for errors (Zhong, Kim, & Liu, 2024). For instance, delayed response to a threat may increase contamination levels within the water system, while prompt detection and intervention can restore system stability. As Whitton (Whitton, 2011) explains, the ability to see the direct consequences of a decision immediately after it's made allows learners to correct their course and reinforce successful strategies (Pramod, 2024). This tight coupling between action and consequence helps players internalize core cybersecurity concepts through repetition and reflection (Plass, D., & and Kinzer, 2015; Pramod, 2024).

These gamification elements serve as instructional scaffolds offering students opportunities to engage with complex, abstract topics through tangible, goal-oriented tasks. Prior research has shown that such strategies not only enhance motivation but also improve knowledge retention and transferability to real-world applications (Hamari, Koivisto, & Sarsa, 2014; Whitton, 2011). In the context of cybersecurity education, they help bridge the gap between conceptual understanding and operational readiness.

GAME DESIGN AND ARCHITECTURE

Simulation Overview

Research shows that game-based cybersecurity training such as the GenCyber immersive workshops can significantly improve both student awareness and motivation by placing learners in realistic, scenario-driven environments (Jin, Tu, Kim, Heffron, & White, 2018). A broader review by Batzos et al. further reinforces this approach, highlighting how serious games and gamified simulations are increasingly being adopted to train cybersecurity professionals and first responders (Batzos et al., 2023). Building on this approach, Cyber H_2O is a role-based simulation game developed to support teaching foundational cybersecurity principles within the context of critical infrastructure specifically, digitally controlled public water systems. The simulation immerses players in the high-stakes environment of a digitally controlled water treatment plant under threat from various cyberattacks. This branching design mirrors current best practices in serious game development, which promote narrative-driven decision structures to reinforce applied learning (Costa & Ribaudo, 2023).

The game is structured around a progressive narrative in which the system comes under increasing levels of threat. Players begin in a relatively stable system environment, completing a system audit and engaging with basic security tasks. As the simulation advances, increasingly sophisticated attacks are introduced, ranging from unauthorized access attempts to ICS manipulation and contamination risk events. Players must work both independently and in their assigned roles to detect, mitigate, and recover from these incidents.

Gameplay is broken into a series of missions and interactive modules, including mini-games and decision-based challenges, that simulate real-world cybersecurity tasks. Each action the player takes contributes to the simulated outcome—for example, how well the player responds to a threat affects the resulting water contamination level. This dynamic cause-effect structure promotes systems thinking and reinforces the importance of timely, coordinated responses in cybersecurity operations. There are also visuals to show the virus spreading.

The simulation is built in Unity and designed for classroom use with 1 to 3 players. It supports both individual learning and collaborative decision-making, offering students a realistic and engaging way to explore the intersection of cybersecurity, infrastructure protection, and professional roles in the field.

System Architecture and Code Design

The Cyber H_2O simulation was developed in Unity using a modular node-based architecture that dynamically adapts game progression based on player choices. This approach enables flexible scenario sequencing and branching logic while maintaining consistent alignment with pedagogical objectives.

At the core of the system is a custom GameFlowManager that manages a queue of scripted events using a hierarchy of node classes. Each node represents a different game state or interactive module, such as a mini-game, decision prompt, or alert message. Nodes can trigger other nodes based on player actions or predefined conditions, allowing for an event based system. This structure supports extensibility where new scenarios or modules can be inserted without rewriting existing logic, making it easy to expand the game.

Mini-games are handled by a MiniGameManager that maintains a list of mini-game prefabs and triggers the appropriate game based on the current event. Mini-games are activated sequentially or conditionally, depending on the decision path selected by the player. Once completed, each mini-game reports its outcome (success or failure) back to the GameFlowManager, which updates the system state and determines the next node to activate. This architecture allows each mini-game to function independently while still contributing to a unified gameplay experience.

Game outcomes such as successful threat mitigation or access control failures impact global variables like water contamination and virus spread level. These variables are managed centrally by the GameManager and reflected visually through the UI. For example, if a player fails to block malware, the GameFlowManager invokes TriggerVirusSpread(), which increases the infection level and updates the virus visualization. A contamination meter similarly reflects the effects of player performance. This real-time feedback system creates a clear link between player decisions, their consequences, and opportunities for reflection, reinforcing key lessons through experiential learning.

Scenario Progression and Pre-Game Audit

Before players begin the main game scenarios in Cyber H_2O, they complete an interactive pre-game audit module establishes foundational cybersecurity awareness and align with the NIST Cybersecurity Framework (CSF) (Figure 1). This initial experience introduces players to the structural and procedural expectations of a secure water system, reinforcing the importance of readiness and planning before an attack occurs. Auditing is a standard practice in critical infrastructure security. Water treatment facilities, like other essential services, must routinely assess system vulnerabilities, validate access controls, and ensure that policies are in place to detect and respond to cyber threats. By incorporating an audit simulation, Cyber H_2O mirrors this real-world process and helps players understand its significance as the first line of defense against attacks.

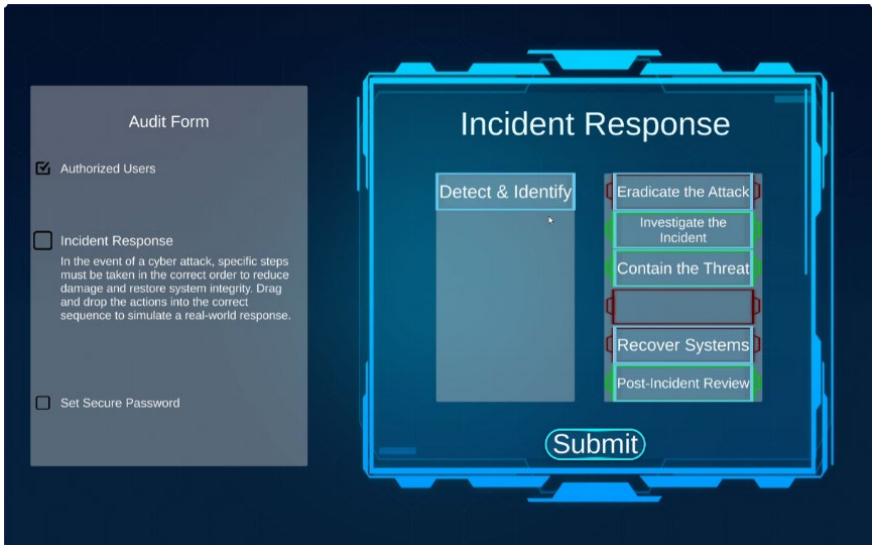

Figure 1: Audit portion of H2O water game

The audit consists of a series of checklist tasks, such as verifying authorized users and setting secure passwords that prompt players to consider the "Identify" and "Protect" functions of the NIST CSF. These tasks are intentionally low-stakes but conceptually important, serving as an instructional primer on system vulnerabilities and preventative controls. This task list ties into the mini games where they'll have to employ some of the concepts that were learned. For example, in the drag and drop game below they learn the order in which cyber threats should be handled. Throughout the minigames, employing the same steps will help them succeed in the games.

Together, the pre-game audit and scenario sequencing establish a foundation for the escalating challenges that follow in Cyber H_2O, reinforcing how preparation, organization, and procedural accuracy can reduce system damage and restore operational stability in critical infrastructure.

Mini-Games and Interactive Mechanics

Cyber H_2O integrates a series of mini-games simulates realistic cybersecurity challenges tied to the protection of critical infrastructure. As players progress through the game narrative, they encounter different decision points that guide them to one or more of these mini-games (Figure 2). While players will ultimately experience all mini-games, their order and context may vary depending on earlier actions and system conditions. These choices influence branching consequences such as the spread of malware, delayed response time, and increasing water contamination levels—visible through an in-game contamination meter that provides continuous feedback.

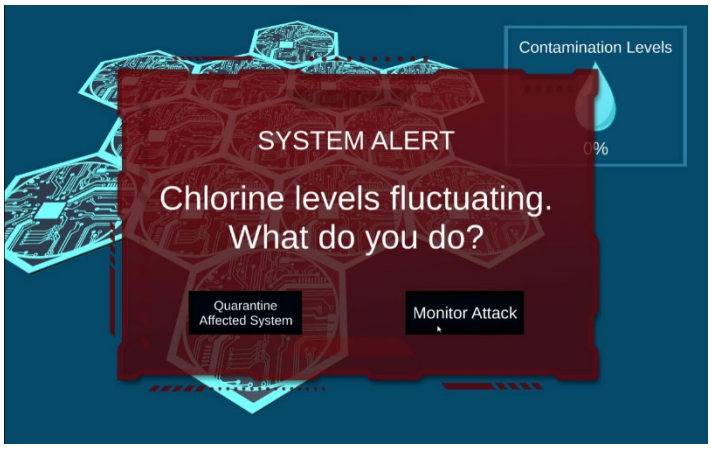

Figure 2: Decision point in H2O water game

Each mini-game corresponds to cybersecurity skills while aligning with NIST CSF functions and NICE role-based competencies:

Log Analysis and Threat Detection

In this mini-game, players examine a scrolling log of system events and must identify suspicious entries related to malware, intrusion attempts, or abnormal system behavior (see Figure 3). Entries are color-coded by severity—INFO, WARN, CRITICAL, ERROR and mimic real log output from SCADA systems, firewalls, and authentication platforms. This exercise supports the "Detect" function of the NIST CSF and builds pattern-recognition and analytical thinking skills essential for roles like Cyber Defense Analyst.

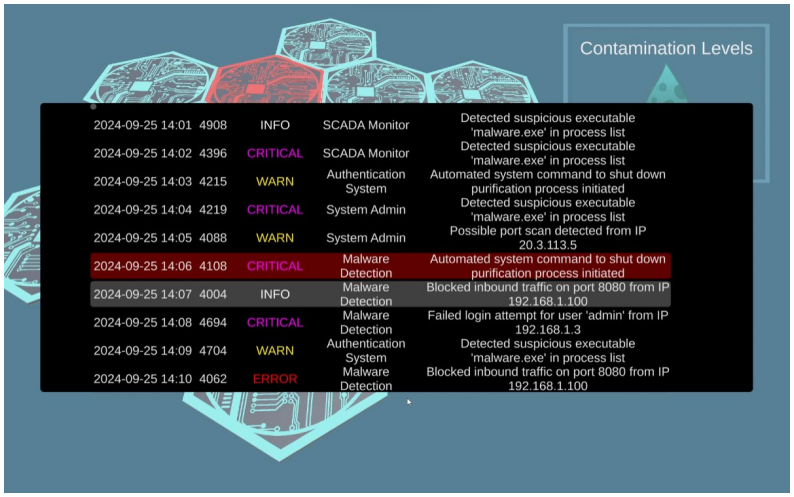

Figure 3: Players scan and investigate security logs to identify cyber threats such as system shutdowns, failed login attempts, or blocked traffic.

Access Control Decision Making

In this access-based mini-game (see Figure 3), players review user requests for access to system components such as the chlorine dispenser, pressure regulator, or SCADA terminals. Each request includes contextual information like name, role, time, and location. Players must use this information to approve, flag, or deny access, cross-referencing it with a system diagram that reveals which roles are authorized for each asset. This activity emphasizes **"Protect"** functions, particularly access control and identity management, and closely mirrors responsibilities of an Identity & Access Management Analyst.

Figure 4: The player evaluates a request by "Quinn," a technician, and must decide whether their location and role justify access to critical components like the pressure regulator.

Network Traffic Management and Anomaly Response

In this system health mini-game (see Figure 5), players monitor network traffic across routers and IP addresses. Alerts are triggered when suspicious patterns emerge such as excessive bandwidth usage or traffic spikes on vulnerable ports. Players must respond by selecting appropriate defensive actions: block traffic, deploy a patch, update the firewall, or increase monitoring. This real-time puzzle challenges players to assess risk quickly and deploy resources effectively, supporting both **"Detect"** and **"Respond"** functions of the NIST CSF.

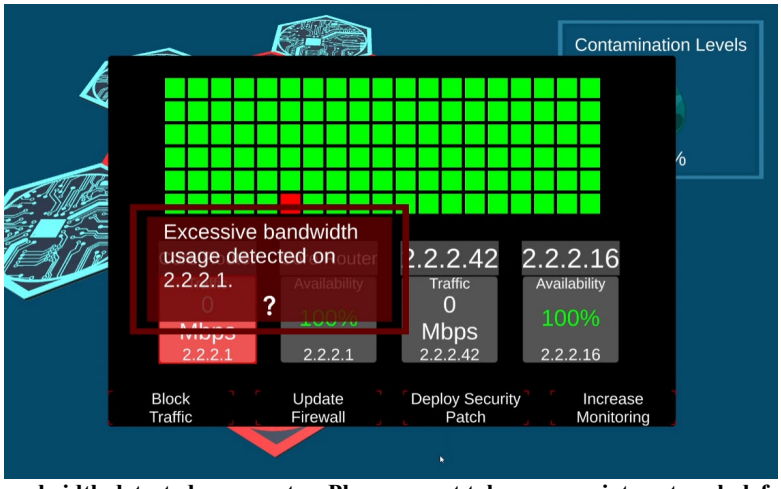

Figure 5: Excessive bandwidth detected on a router. Players must take appropriate network defense action to prevent further compromise.

Feedback Systems and Progression

To reinforce learning and simulate real-world consequences, Cyber H_2O integrates layered feedback systems that respond dynamically to player decisions. Throughout the game, players receive immediate visual and textual cues that reflect the impact of their actions, providing both short-term reinforcement and long-term performance assessment.

One of the primary mechanisms is the **virus spread visualization**. When players fail to contain a cybersecurity threat, such as granting improper access or delaying detection, the virus begins to propagate across a network map. This is displayed through an expanding red overlay on system nodes (see Figure 6), serving as a clear, real-time indication of system compromise. Simultaneously, a contamination meter in the top-right corner of the interface updates to reflect how these failures affect water safety. This coupling of visual feedback and environmental consequence provides an intuitive way for learners to associate errors with tangible outcomes

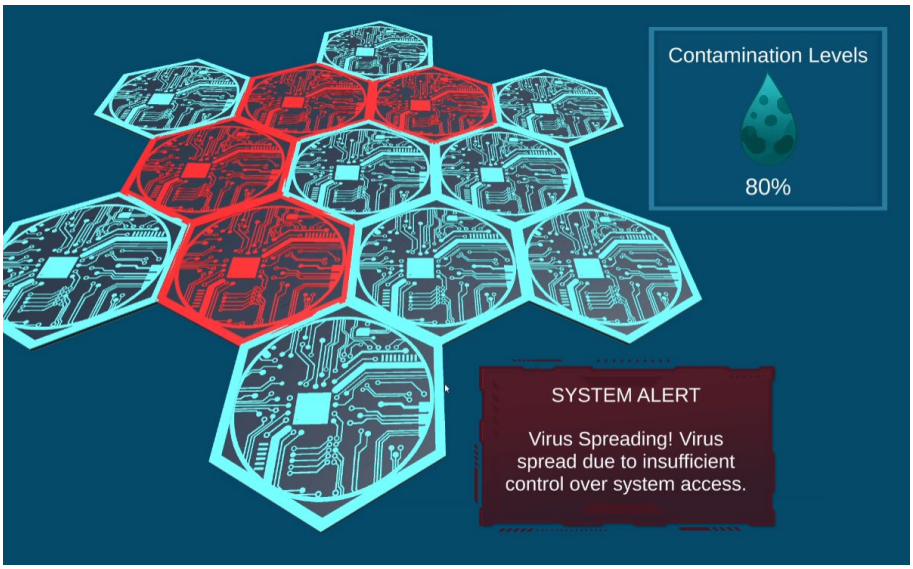

Figure 6: The virus spread visualization and contamination level gauge give players real-time feedback as threats escalate across the system.

At the end of each session, players are presented with a mission summary screen that quantifies their performance. Metrics such as Virus Spread Level and Contamination Level are displayed alongside a message indicating the severity of the incident (see Figure 2). This encourages reflection and replayability, prompting players to consider what actions could have improved the outcome.

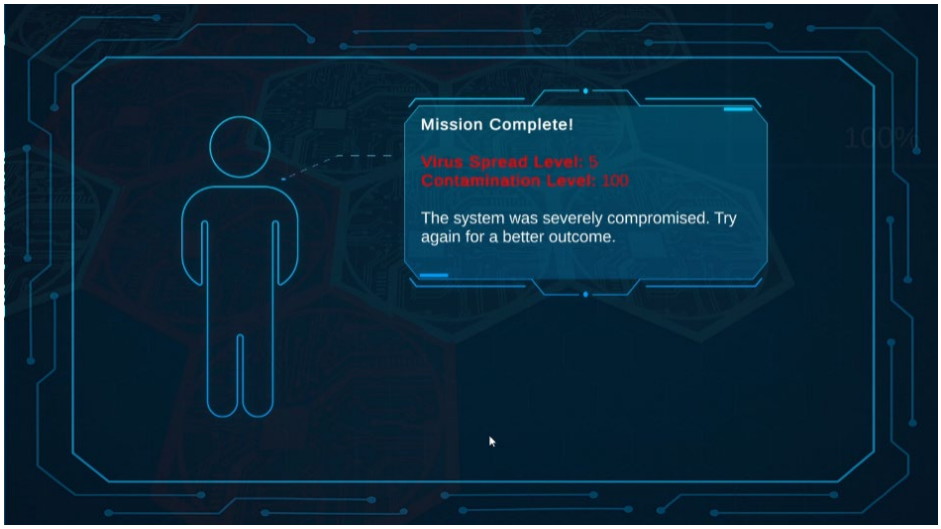

Figure 7: Post-game summary screen showing the final impact of player decisions on system security and water safety.

These feedback mechanisms align with best practices in educational game design, where immediate, contextualized feedback improves decision-making and helps players internalize lessons through reflection and iteration (Hamari et al., 2014; Whitton, 2011). In Cyber H_2O, feedback is not limited to points or scores—it is embedded directly in the

game environment, tying player performance to real-world cybersecurity outcomes and reinforcing the value of vigilance, timing, and role-specific expertise.

CONCLUSION

There are complex challenges facing future cybersecurity professionals especially with respect to cyber threats targeting critical infrastructure. Traditional instruction methods have been shown to fail to adequately prepare students for these challenges from both a technical and contextual standpoint. To address this gap, this work introduces a role-based simulation that integrates scenario-based gameplay and experiential learning approaches. The simulation offers a structured environment by mapping gameplay to established cybersecurity frameworks. The inclusion of branching consequences, mini-games, collaboration, and feedback mechanisms supports student development of critical thinking and role-specific competencies.

While this preliminary implementation is promising, integration of the simulation's impact on knowledge retention and workforce readiness. The team plans to continue to refine the simulation based on learner feedback and evolving cybersecurity threats. As the simulation is refined, maintaining the pedagogically grounded, interactive principles that were implemented in the first version of this work will allow it to continue to bridge the divide between cybersecurity theory and practice.

Acknowledgements

This work is funded by the Commonwealth Cyber Initiative under grant number HC-4Q24-074.

REFERENCES

Batzos, Z., Saoulidis, T., Margounakis, D., Fountoukidis, E., Grigoriou, E., Moukoulis, A., . . . Mouratidis, H. (2023). *Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview*.

Chaimae Moumouh, J. A. G.-B., Mohamed Y. Chkouri, José L. Fernández-Alemán. (2025). Serious Games to Improve Privacy and Security Knowledge for Professionals: a Systematic Literature Review. *International Journal of Serious Games, 12*(1), 3-24. doi:10.17083/ijsg.v12i1.825

Costa, G., & Ribaudo, M. (2023). Designing a Serious Game for Cybersecurity Education. In K. M. L. Cooper & A. Bucchiarone (Eds.), *Software Engineering for Games in Serious Contexts: Theories, Methods, Tools, and Experiences* (pp. 265-290). Cham: Springer Nature Switzerland.

Gouveia, D., Lopes, D., & Vaz de Carvalho, C. (2011). *Serious gaming for experiential learning*.

Hamari, J., Koivisto, J., & Sarsa, H. (2014). *Does Gamification Work? — A Literature Review of Empirical Studies on Gamification*.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn), 12*, 150. doi:10.11591/edulearn.v12i1.7736

Kolb, D. (1984). *Experiential Learning: Experience As The Source Of Learning And Development* (Vol. 1).

Ng, C. Y., & Hasan, M. K. B. (2025). Cybersecurity serious games development: A systematic review. *Computers & Security, 150*, 104307. doi:https://doi.org/10.1016/j.cose.2024.104307

Plass, J. L., D., H. B., & and Kinzer, C. K. (2015). Foundations of Game-Based Learning. *Educational Psychologist, 50*(4), 258-283. doi:10.1080/00461520.2015.1122533

Pramod, D. (2024). Gamification in cybersecurity education; a state of the art review and research agenda. *Journal of Applied Research in Higher Education, 17*(4), 1162-1180. doi:https://doi.org/10.1108/JARHE-02-2024-0072

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585. doi:https://doi.org/10.1016/j.cose.2023.103585

U.S. Environmental Protection Agency, O. o. I. G. (2024). *Cybersecurity concerns related to drinking water systems: Management implication report*. Retrieved from Washington, DC:

Whitton, N. (2011). Encouraging Engagement in Game-Based Learning. *IJGBL, 1*, 75-84. doi:10.4018/ijgbl.2011010106

Zhong, C., Kim, J. B. J. B., & Liu, H. (2024). The Art of Inclusive Gamification in Cybersecurity Training. *IEEE Security & Privacy, 22*(05), 40-51. doi:10.1109/MSEC.2024.3427666