ASTROGUARD: A GAMIFIED APPROACH TO TEACHING CMMC COMPLIANCE

Michaela Pierce

A Capstone Project (or Thesis) Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Congdon School of Supply Chain, Business Analytics, and Information Systems

University of North Carolina Wilmington

2023

Approved by

Advisory Committee

Minoo Modaresnezhad | Elham Ebrahimi | Ulku Clark

Geoff Stoker, Chair

Accepted By

_____

Dean, Graduate School

Table of Contents

ABSTRACT

AstroGuard: A Gamified Approach to Teaching CMMC Compliance. Pierce, Michaela, 2023. Capstone Paper, University of North Carolina Wilmington.

This paper explores the essential need for heightened cybersecurity measures, particularly for entities engaged with the Department of Defense (DOD). Emphasizing the critical role of the Cybersecurity Maturity Model Certification (CMMC), the paper proposes the development of an engaging educational game to simplify its complexities. In the context of increasing cyber threats, especially for small businesses, the significance of prioritizing CMMC for robust defense against evolving cyber threats is highlighted. The paper also delves into the challenges associated with the implementation of CMMC, offering insights into navigating this crucial cybersecurity framework.

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

ABBREVIATIONS

CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DIB	Defense Industrial Base
DOD	Department of Defense
NIST	National Institute of Standards and Technology
SSP	System Security Plan
NARA	National Archives and Records Administration

CHAPTER 1: INTRODUCTION

This paper delves into the gamification of CMMC (Cybersecurity Maturity Model Certification), emphasizing the critical need for heightened cybersecurity measures, particularly for entities engaged with the Department of Defense (DOD). The escalating frequency of cyber threats highlights vulnerabilities faced by small businesses, making the prioritization of cybersecurity imperative. The Cybersecurity Maturity Model Certification (CMMC) emerges as a key framework, ensuring secure defense contracts by mandating stringent cybersecurity standards. In response to this urgency, the paper proposes the development of an engaging educational game designed to demystify the complexities of the CMMC model. The human factor's vulnerability and the ever-present threat of cyber attacks underscore the significance of prioritizing CMMC for comprehensive defense against evolving cyber threats.

1.1 Background and Context

This paper explores the reality illuminated by compelling statistics, emphasizing the crucial need to prioritize cybersecurity, especially for entities involved in contracts with the Department of Defense (DOD). Small businesses, constituting 43% of cyber attack targets, grapple with vulnerabilities, with only 26% acknowledging cybersecurity as a top priority (Palatty, 2023). These businesses, irrespective of size, may find themselves mandated to adhere to the Cybersecurity Maturity Model Certification (CMMC) due to their connections with the DOD. The escalating frequency of cyber attacks, such as the 95% surge observed in the last six months of 2022, the staggering financial implications of breaches, and the prevailing cybersecurity landscape magnify the urgency for businesses to fortify their defenses (Palatty, 2023).

Within this context, the development of an educational game geared toward teaching the CMMC Model assumes heightened significance. The game's mission is to render the often-complex CMMC model engaging and accessible to a broader audience. Notably, the human factor, identified as the "weakest link" in cybersecurity, is evident in statistics revealing that 85% of breaches involve a human insider, and 61% involve weak passwords or compromised credentials (Ninja, 2023). Moreover, the urgency for robust cybersecurity measures is encapsulated in the forthcoming exploration of the game development process, which endeavors to acquire CMMC knowledge as engaging and indispensable learning experience.

In the realm of cyber-attacks, the statistics are concerning: an attack happens every 39 seconds, with an average cost of $9.44 million per data breach. The cumulative impact of cybercrime has reached unprecedented levels, with an estimated 33 billion

account breaches anticipated in 2023 alone. The severity of these threats is further compounded by the prediction that cybercrime will cost a staggering $8 trillion by the end of 2023 (Ninja, 2023).

In addressing the aftermath of cyber attacks, the escalating costs are reflected in the rise of cyber insurance premiums by an average of 28% in the first quarter of 2022. Currently, 55% of businesses hold cyber insurance, yet 85% have witnessed an increase in their premiums. Notably, the largest ransom payouts by insurers in the last two years averaged $3.52 million in the U.S. (Ninja, 2023). These statistics illuminate the multifaceted challenges and financial ramifications associated with cybersecurity breaches, further underscoring the need for proactive measures and comprehensive educational initiatives such as the development of the CMMC-focused game.

1.2 Contextualizing CMMC Challenges

Implementing the Cybersecurity Maturity Model Certification (CMMC) is crucial for enhancing security, but it is not without its set of challenges. There are several common challenges to be found when working with firms to achieve CMMC 2.0 compliance.

The first challenge organizations often face is assuming they have time. It is a frequent misconception that compliance can be postponed and dealt with at any time before the designated "deadline." Organizations tend to assume they will be able to easily achieve compliance, “…because they have an IT provider helping them and some cybersecurity policies in place could lull them into a false sense of security” (Cohen, 2023). It should be noted “…that even the most advanced organizations can take months to achieve and document compliance” (Cohen, 2023). CMMC 2.0 entails a

comprehensive framework comprising more than 110 distinct controls and necessitates the meticulous formulation, implementation, and enforcement of 34 discrete policies, all requiring tangible evidence of compliance (Cohen, 2023). Beyond these policies and control specifications, the certification mandates an integrated approach that includes the training of all employees and the establishment of new processes and procedures to supersede outdated practices. The multifaceted nature of these requirements underscores the depth and complexity involved in achieving and maintaining CMMC 2.0 compliance.

The second challenge organizations often face is having an incomplete security plan. The System Security Plan (SSP) plays a pivotal role in CMMC compliance, serving as a formal, written document that meticulously details the organizational infrastructure, associated risks, and the security controls currently in operation or planned to mitigate those risks (Cohen, 2023). Auditors commence their evaluation by scrutinizing the SSP, emphasizing the critical importance of comprehensive documentation. This entails the inclusion of boundary diagrams, network architectures, details about services, data flows for Controlled Unclassified Information (CUI), as well as documented processes and procedures for its proper handling. The completeness of the SSP documentation is paramount, acting as a foundational element for a successful CMMC compliance audit.

Many smaller and medium-sized businesses frequently lack the depth and intricacy in their current documentation necessary for CMMC compliance, presenting a common hurdle in the certification process. Conversely, larger enterprises might have the required personnel and documentation internally, but these resources are often dispersed across various IT teams (Cohen, 2023). Regardless of organizational size, creating a thorough inventory that precisely outlines the scope of CMMC compliance is essential.

This ensures a comprehensive understanding of the compliance landscape, enabling a more efficient and effective approach to meeting the stringent certification requirements.

The third challenge organizations often face is inadequate continuous monitoring. Numerous entities exert significant efforts to overcome the hurdles essential for achieving CMMC compliance, only to encounter a potential pitfall—carelessness post-compliance. It is crucial to emphasize that CMMC imposes a continuous requirement for assessment, monitoring, and improvement. Enhancing efficiency in this regard involves the adoption of technologies and frameworks that automate monitoring and maintenance processes. This strategic approach not only streamlines the compliance procedures but also ensures a sustained commitment to the ongoing requirements of CMMC (Cohen, 2023).

The fourth challenge organizations often face is the failure to locate controlled unclassified information (CUI). Contractors within the Defense Industrial Base (DIB) are obligated to manage CUI which, although not classified, remains government-owned and necessitates protection.

Identifying and locating the CUI stored by companies frequently emerges as a common obstacle. This lack of precision often leads to the imposition of broad controls for CUI protection, resulting in unnecessary costs and added complexities. The challenge lies in the failure to precisely pinpoint and recognize stored CUI, posing a substantial risk to the efficiency and cost-effectiveness of protective measures. This underscores the critical need for accurate CUI management within the DIB (Cohen, 2023).

The fifth challenge organizations often face is perceiving the CMMC Compliance Journey as a basic checklist. It is essential to dispel the misconception that CMMC

compliance is a one-time task confined to a checklist; rather, it exerts a profound influence on individuals, processes, and technology. The impact can be substantial, necessitating intensive training for employees, adjustments to business processes, and technological updates to align with new standards.

Furthermore, acknowledging that the risk profile and potential attack surface of a business evolve, coupled with the dynamic nature of the cybersecurity landscape, emphasizes the necessity for frequent updates to the SSP. Staying proactive in addressing emerging security risks is crucial, prompting the Department of Defense (DoD) to advocate for regular CMMC audits instead of a singular assessment (Cohen, 2023).

Given the introduction of the updated version (2.0) of certification requirements, there exists a potential for confusion regarding the necessary actions for compliance. Companies must ensure a thorough understanding of these requirements, covering essential aspects such as data encryption, access log tracking, personnel training in cybersecurity best practices, and the secure storage of all documents related to CUI (Common NIST and CMMC 2.0 compliance challenges, 2023).

Businesses are obligated to meticulously track their progress in meeting these updated requirements, facilitating accurate reporting during audits and reviews conducted by DoD officials. While an abundance of online resources is available to aid in comprehending various facets of compliance, a level of uncertainty persists in interpreting how specific rules may apply in distinct situations or industries. Therefore, companies must navigate these complexities to ensure adherence to the latest CMMC 2.0 standard. (Doubleday, 2023).

1.3 Evolution of Cybersecurity Standards

The evolution from the National Institute of Standards and Technology (NIST) cybersecurity standards to the Cybersecurity Maturity Model Certification (CMMC) is a journey shaped by the need for enhanced cybersecurity in the Defense Industrial Base (DIB). It all began with NIST, a pivotal force in establishing cybersecurity standards. NIST's Special Publication 800-171 (NIST SP 800-171), created in response to Executive Order 13556 in 2010, laid the groundwork by setting security requirements for protecting CUI in federal contractor systems (Bjorklund, 2023).

Executive Order 13556, signed by President Barack Obama in 2010, was a catalyst for change. Acknowledging the shortcomings of ad hoc policies, the order aimed to streamline the safeguarding and control of CUI across the executive branch. It assigned the National Archives and Records Administration (NARA) the responsibility of ensuring compliance and consistency in safeguarding sensitive government information.

Enter CMMC, introduced by the DoD to fortify defense contractors against evolving cyber threats. While NIST SP 800-171 laid out critical security practices, CMMC represents a strategic leap forward. CMMC builds upon NIST's foundation, incorporating a comprehensive framework with five maturity levels. This model addresses the shortcomings of self-attestation and introduces a more rigorous certification process, aligning with the goals set by Executive Order 13556 (Bjorklund, 2023).

The journey from CMMC 1.0 to CMMC 2.0 reflects an ongoing commitment to cybersecurity excellence. In November 2021, the DoD announced the transition to CMMC 2.0, signaling a refined framework. CMMC 2.0 streamlines certification levels from five to three, focusing on Foundational, Advanced, and Expert tiers. This shift is

accompanied by a restructuring of security domains, introducing new elements like Incident Response, Anomaly Detection, and Supply Chain Risk Management for a more holistic view of contractors' operations (CMMC 1.0 vs. CMMC 2.0, 2023). Figure 1 shows CMMC Version 1.0 and 2.0 for reference.

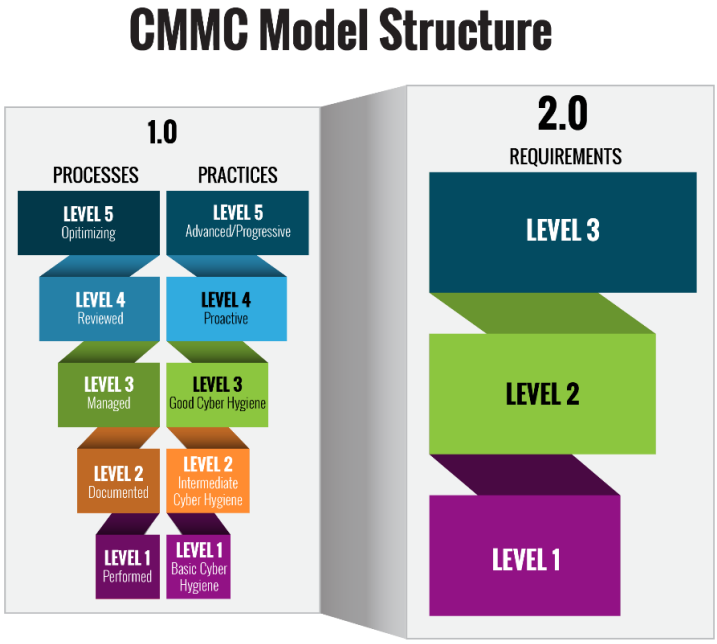

Figure 1 CMMC Model Structure (CMMC Model, n.d.)

Despite the planned transition to CMMC 2.0, a delay until 2024 has raised questions and redirected attention to NIST SP 800-171 compliance. The delay emphasizes the importance of adhering to existing regulations, and defense contractors are urged to focus on NIST 800-171 as a crucial step in safeguarding CUI. The delay underscores the significance of a proactive approach to cybersecurity, emphasizing the "trust but verify" principle through independent assessments of NIST SP 800-171 controls (CMMC is delayed, 2023).

As of early 2023, questions linger about the finalization of CMMC's rulemaking and its effectiveness in the coming year. Delays in sending the rule package to the White House Office of Management and Budget (OMB) suggest internal disagreements on the way forward. Anticipation surrounds whether CMMC will be implemented through an "interim final" rule or a "proposed rule," with the latter potentially pushing full implementation into 2024. The rollout strategy is expected to be phased, considering the readiness of Third-Party Assessment Organizations (C3PAOs) and assessors to meet the demand (Doubleday, 2023).

As CMMC inches closer to reality, defense contractors face the challenge of readiness. Awareness of cyber threats has grown significantly, but the evolving nature of cybersecurity requires continuous vigilance. The defense industrial base remains a prime target for adversarial actors, emphasizing the need for a renewed focus on cybersecurity. The ongoing conflict in Ukraine further underscores the potential impact of cyber intrusions on the defense industrial base, making readiness a top priority (Doubleday, 2023).

The journey from NIST standards to CMMC represents a strategic evolution in response to cybersecurity challenges. From NIST's foundational standards to the comprehensive approach of CMMC, the transition reflects a commitment to adapt and fortify against evolving threats, grounded in executive orders and a continuous pursuit of cybersecurity excellence. As CMMC navigates delays and uncertainties, defense contractors are urged to prioritize NIST compliance and maintain a proactive stance in the face of dynamic cyber landscapes.

1.4 Objectives of the Study

The primary objective of this study is to design and develop a proof-of-concept interactive educational game aimed at instructing individuals on the CMMC. Recognizing the critical importance of cybersecurity in contemporary digital landscapes, the game seeks to engage users in an immersive learning experience that effectively conveys the principles and requirements outlined in the CMMC framework. Through a carefully crafted combination of gamification elements, simulations, and instructional content, the goal is to enhance the accessibility and comprehensibility of CMMC concepts, catering to a diverse audience ranging from cybersecurity professionals to individuals with limited technical backgrounds.

The study will prioritize the timely development of the proof-of-concept game, streamlining the process to meet project deadlines. While the absence of testing and feedback collection limits real-time assessment, the project's success will be gauged through adherence to predefined design criteria, functionality benchmarks, and the fulfillment of learning objectives. This streamlined approach aims to lay the groundwork for delivering a comprehensive educational tool that equips users with a foundational understanding of CMMC, contributing to broader cybersecurity awareness and providing a more engaging experience dedicated to learning cybersecurity standards.

1.5 Assessing the Need for CMMC Gamification

The exploration of gamification as a solution to address challenges in CMMC training is grounded in the well-documented benefits of this approach in the realm of corporate learning and development. Gamification, far from being a mere buzzword, has

demonstrated its effectiveness in making corporate training more dynamic and significantly increasing learner engagement (Mulkeen, 2018). The application of gamification principles capitalizes on the inherent motivation derived from competitive elements, a concept exemplified by the universal appeal of sports such as football, which draws individuals to a muddy field on a rainy day for the sheer desire to win (Mulkeen, 2018)

One of the fundamental advantages of gamification is its capacity to make learning fun and interactive, leveraging psychological drivers that stimulate human engagement. By incorporating role-play and competitive elements, gamification creates an immersive learning experience that not only informs but also entertains, making the educational content exciting and enjoyable (Mulkeen, 2018). Furthermore, the addictive nature of gamification contributes to knowledge retention by triggering the release of dopamine, a neurotransmitter associated with reward and pleasure, reinforcing the learning experience (Mulkeen, 2018). In the context of CMMC training, where the material can be complex and technical, the gamification approach offers a promising avenue to enhance learner engagement and knowledge retention. Additionally, the real-world application aspect of gamification aligns with the third benefit, providing learners with the opportunity to see practical applications of CMMC principles and witness the consequences or rewards of their choices within the game (Mulkeen, 2018).

Moreover, gamification offers real-time feedback, a critical component often lacking in traditional training methods. Learners engaged in gamified training scenarios can receive immediate, measurable feedback as they work towards meaningful targets, fostering continuous improvement and skill development (Mulkeen, 2018). This aspect is

particularly pertinent to CMMC training, where the evolving nature of cybersecurity threats demands agile and adaptive learning strategies. In summary, the exploration of gamification in CMMC training is supported by its proven ability to make learning engaging, addictive, application-oriented, and conducive to real-time feedback, enhancing the overall learning experience (Mulkeen, 2018).

1.6 Defining the Scope of Gamification in CMMC Training

The implementation of gamification in CMMC training seeks to address challenges faced by individuals with limited technical experience by making the learning process more accessible and engaging (Top 7 Benefits, 2023). By incorporating game-like elements such as progress bars, achievements, and interactive scenarios, gamification transforms the complex landscape of cybersecurity standards into an approachable and enjoyable educational experience. This approach aims to bridge the gap for learners who may find traditional training methods less engaging. Moreover, gamification in CMMC training focuses on enhancing learner engagement and productivity by creating an immersive learning experience with features like points, badges, and leaderboards. This not only imparts knowledge but also sustains learner interest throughout the training process, contributing to improved retention and application of CMMC principles.

Additionally, gamification encourages social interaction among learners, fostering healthy competition and collaboration through features like leaderboards and points (Top 7 Benefits, 2023). This social aspect is particularly beneficial for individuals who may feel isolated or overwhelmed by the technical nature of cybersecurity standards. The sense of community and shared objectives created through gamification provide

additional support and motivation for learners, enhancing their overall training experience.

Furthermore, the gamification of CMMC training contributes to an improved corporate image by creating a positive and engaging learning environment (Top 7 Benefits, 2023). As employees connect with coworkers and engage in a sense of community through gamified training, it reflects positively on the organization's culture, extending beyond the training realm to enhance the overall image of the company as one that values employee development and fosters a collaborative learning atmosphere.

Moreover, gamification in CMMC training provides a clear call to action by creating scenarios that require learners to complete specific tasks, coupled with immediate feedback and rewards (Top 7 Benefits, 2023). This streamlined approach ensures that employees understand and follow correct processes efficiently, promoting effective and timely skill acquisition in the complex field of cybersecurity standards. In conclusion, the exploration of gamification in CMMC training demonstrates its potential to make the learning experience more accessible, engaging, and enjoyable for individuals with limited technical experience, contributing to improved understanding, retention, and application of cybersecurity principles (Top 7 Benefits, 2023).

CHAPTER 2: REVIEW OF LITERATURE REVIEW AND ANALYSIS

This section critically examines the existing body of knowledge and research related to cybersecurity, educational games, and the CMMC. This comprehensive review is structured to provide a foundation for understanding the broader context surrounding cybersecurity challenges, the efficacy of educational games in fostering learning, and the specific requirements and implications of the CMMC framework. By synthesizing insights from diverse sources, this section aims to identify gaps, trends, and key findings in the literature, laying the groundwork for the subsequent discussion on the development and implementation of an educational game for CMMC.

2.1 Historical Overview of Gamification

The evolution of gamification traces a rich history, from its humble beginnings to its pervasive presence in contemporary applications. The term "gamification" itself was only coined in 2002 by Nick Pelling, reflecting a time when the concept had yet to permeate the lexicon (The history of gamification, 2019). However, the roots of gamification extend much further back.

In 1896, Sperry and Hutchinson Co. pioneered a form of gamification through a loyalty program involving Green Stamps, rewarding customers for specific spending thresholds (Andreev, 2023). The Boy Scouts of America introduced a badge system in 1908, a precursor to contemporary gamified achievement systems (The history of gamification, 2019). American Airlines further embraced gamification in 1981 with the AAdvantage frequent flier program, a testament to early recognition of the potential for game-like structures to foster customer loyalty (The history of gamification, 2019).

The advent of video games in the late 20th century catalyzed a shift in thinking, with developers recognizing the intrinsic engagement potential of gaming elements. In 2005, Bunchball emerged as the first modern gamification platform, dedicated to enhancing website engagement through game mechanics (Andreev, 2023). This period also saw the introduction of Microsoft's Xbox 360 Gamerscore system in 2005, standardizing in-game achievements and contributing to the gamification landscape (The history of gamification, 2019).

The term "gamification" gained formal recognition in 2002 when Nick Pelling coined the phrase while designing game-like user interfaces for electronic devices (The history of gamification, 2019). This year also witnessed the release of America's Army,

an educational first-person shooter game developed by the U.S. Army, exemplifying the diverse applications of gamification (The history of gamification, 2019).

The 2010s marked a pivotal era for gamification. Jane McGonigal's TED Talk in 2010, titled "Gaming Can Make a Better World," provided a groundbreaking perspective on the potential positive impact of games (The history of gamification, 2019). The inaugural Gsummit in 2011, hosted by Gamification Co., marked a turning point, with around 400 attendees and the official release of Jane McGonigal's influential book, "Reality is Broken" (Andreev, 2023). The year 2012 saw increased hype and attention as Gartner predicted that by 2014, 70% of Global 2000 organizations would have at least one gamified application (The history of gamification, 2019).

In 2016, the release of Pokémon Go demonstrated the viral success of gamification, amassing over 800 million downloads and breaking several records (Andreev, 2023). This success underscored the addictive nature of game mechanics and their potential to captivate diverse audiences.

As of 2018, gamification had become ubiquitous, integrated into various apps spanning education, health, and daily activities (Andreev, 2023). The term has evolved, with alternative descriptors such as "behavioral design" and "engagement-focused experience" reflecting the broader application of gamified principles.

In summary, the evolution of gamification highlights a trajectory from early loyalty programs to widespread integration across diverse sectors. The timeline reflects not only technological advancements but also a paradigm shift in recognizing the profound impact of game elements on user engagement and behavior.

2.2 Existing CMMC Training Methods

Traditional CMMC training methods encompass a variety of approaches aimed at equipping individuals with the necessary skills and knowledge to navigate the certification process's intricacies. These methods include courses, videos, and guides/manuals. While these approaches are instrumental in delivering foundational information, they are often characterized as routine and, at times, less engaging.

One widely recognized avenue for CMMC training is through courses offered by Licensed Training Providers (LTPs). These providers, as part of the CMMC-AB Marketplace, deliver Certified Professional (CP) courses, preparing individuals for the CP certification. The CP certification allows professionals to participate as assessment team members and be listed in the CMMC-AB Marketplace (Cybersecurity Maturity, 2022).

However, the process of acquiring CMMC knowledge extends beyond formal courses. A comprehensive review of the CMMC training landscape reveals that only a subset of Licensed Training Providers offers specific Certified CMMC Professional (CCP) courses. Prices for these courses vary, ranging from $1,995 to $4,935, and often support Virtual Instructor-Led Training (VILT) with some also offering in-person courses (Stanton, 2021). This diversity in training options underscores the evolving nature of CMMC training methodologies.

Moreover, individual roles within the CMMC ecosystem necessitate distinct training paths. Registered Practitioners (RPs), for instance, play a crucial role in helping organizations prepare for certification. The training for RPs, delivered through a web-based platform, covers 12 modules with quizzes at the end of each module. However, the

focus of this training is on the broader goals of CMMC and the participants in the process, rather than delving into detailed practice or assessment objectives (Stanton, 2021).

Registered Provider Organizations (RPOs) and Certified Third-Party Assessor Organizations (C3PAOs) represent organizational entities in the CMMC ecosystem, each requiring specific training and accreditation. RPOs, much like RPs, undergo business background checks, while C3PAOs face a more rigorous process, including interviews, assessments, and adherence to a Code of Professional Conduct (Stanton, 2021).

Certified CMMC Professionals (CCPs) and Certified CMMC Assessors (CCAs) form the backbone of C3PAOs' assessment teams. The distinction between registered and certified designations lies in the rigor of training and evaluation. The CMMC Body of Knowledge (BOK) serves as a foundational resource available to registered and certified members of the CMMC ecosystem. It encompasses the CMMC Model, assessment criteria, methodologies, learning objectives, and other relevant resources (Stanton, 2021).

Licensed Publishing Partners (LPPs) and Licensed Training Partners (LTPs) contribute to the training landscape by developing courses and curricula based on the BOK. Certified Instructors, crucial for delivering training, must pass certification as assessors before achieving instructor certification. Notably, the certification process involves achieving at least the same maturity level they teach (Stanton, 2021).

While training is available, delays and adjustments are anticipated due to the release of CMMC 2.0. The Certified Professional (CCP) certification, a prerequisite for Certified CMMC Assessors (CCAs), requires a college degree or two years of IT experience, among other criteria. The examination for CCPs, initially scheduled for

February 2021, faced delays, and the revised schedule is yet to be issued (Stanton, 2021)

In conclusion, the landscape of CMMC training is multifaceted, with various roles and entities requiring distinct training paths. While traditional methods such as courses play a vital role, the evolving nature of CMMC necessitates adaptability and continuous updates to training methodologies. Engaging with Licensed Training Providers and staying informed about the evolving requirements is a key aspect of navigating the CMMC training landscape.

2.3 Gamification in Cybersecurity Training

The integration of gamification, particularly exemplified by platforms such as Hack the Box (HTB), presents a promising avenue for enhancing cybersecurity education. Trombino's study underscores the efficacy of HTB in imparting secure software development skills, outperforming traditional laboratory methods. Participants reported heightened engagement and confidence levels in secure software development practices post-HTB engagement, highlighting its efficacy as an instructional tool (Trombino, n.d.). Additionally, HTB was perceived as more stimulating and demanding compared to conventional approaches, catering to students who found the latter uninspiring or challenging (Trombino, n.d.). Significantly, HTB bolstered students' confidence, with the majority feeling adequately prepared for real-world scenarios (Trombino, n.d.)

Expanding upon this, serious games within cybersecurity training have demonstrated tangible benefits. Research by Steen and Deeleman emphasizes the positive impact of theory-informed serious games on participants' attitudes, subjective norms,

perceived behavioral control, intentions, and behavior in cybersecurity (Steen & Deeleman, 2021). This aligns with the growing recognition of serious games as a potent tool for enhancing end-users' cybersecurity behaviors (Steen & Deeleman, 2021). However, further exploration of objective behavioral outcomes and team-focused offline game formats is warranted to fully harness the potential of serious games in cybersecurity training (Steen & Deeleman, 2021).

In summary, the literature strongly advocates for the effectiveness of gamification, notably through platforms like HTB and serious games, in cybersecurity education. These innovative approaches enhance engagement, confidence, and readiness for real-world challenges. Ongoing research endeavors are imperative to refine these methodologies and ensure their widespread integration into educational curricula.

2.4 Successful Gamification Implementation Cases

CybAR, a Mobile Augmented Reality (MAR) serious game developed by Alqahtani and Kavakli-Thorne in 2020, represents an innovative approach to cybersecurity education. Grounded in the Technology Threat Avoidance Theory (TTAT), the game leverages gamification and situated learning principles to create an engaging and immersive environment for users.

The game is designed to increase awareness of safe cybersecurity practices through a competitive and interactive interface. It incorporates 20 tasks that simulate real-life cybersecurity challenges, covering a spectrum of threats such as phishing, ransomware, Wi-Fi security, password creation, and social media practices. Users earn

points by making informed decisions in response to these challenges, fostering a deeper understanding of cybersecurity concepts.

In an experimental study involving 91 participants, university students, CybAR demonstrated notable success. The participants, comprising 59% males and 41% females, primarily consisted of bachelor's (45%) and master's (37%) students. Despite 44% of participants self-reporting poor prior knowledge of cybersecurity, 88% reported an improved understanding after engaging with CybAR.

The feedback from the study participants was overwhelmingly positive. Key statistics include an 84% agreement that CybAR motivated them to learn more about cybersecurity. Additionally, 82% agreed that the game effectively simulated real-life cybersecurity scenarios. Importantly, more than 90% of participants found CybAR to be clear, enjoyable, and easy to understand, indicating a prominent level of user satisfaction.

These statistics highlight the success of CybAR in engaging users and enhancing their awareness and understanding of cybersecurity concepts. The positive reception underscores the efficacy of the gamified approach, motivating users to actively participate in cybersecurity education. As part of future endeavors, the developers aim to refine the game for enhanced enjoyment and conduct long-term evaluations to assess knowledge retention. The overarching goal is to expand CybAR into a comprehensive cybersecurity awareness application suitable for diverse age groups (Alqahtani, 2020).

2.5 Cognitive and Behavioral Aspects of Gamification

Gamification extends beyond mere technology; it's deeply intertwined with psychology, particularly in understanding motivation. "Gamification is more psychology than technology and the development of motivation is an important factor to consider

(AlMarshedi, Wanick, Wills, & Ranchhod, 2017). AlMarshedi et al.'s chapter delves into this intersection of gamification and behavior, stressing the significance of psychological insights for effective implementation.

The chapter defines gamification as a process integrating play and user experience elements into non-gaming contexts. However, it emphasizes the need to grasp psychological aspects beyond superficial gaming elements for successful implementation. Cultural influences emerge as pivotal in shaping the effectiveness of gamification, influencing perceptions and usage patterns. Cultural influences refer to the societal norms, values, beliefs, and practices that shape individuals' behaviors and attitudes. Understanding the nuances of cultural context, including individual and collective attributes, emotional attachments, and decision-making processes, is crucial for effective behavioral interventions.

Various psychological theories underpin gamification strategies, illuminating the mechanisms of motivation and behavior change. Motivation, whether intrinsic or extrinsic, is identified as a key driver of behavior. While specific cultural dimensions are not discussed, the chapter explores the broader concept of cultural influences, highlighting their importance in gamification design.

These cultural influences impact consumer behavior and necessitate consideration in gamification design to ensure resonance with diverse audiences. Additionally, the chapter underscores the role of social influences, particularly through social norms, in shaping behavior within gamified contexts.

Recognizing the intricate interplay between psychology, culture, and behavior is essential in leveraging gamification effectively for behavioral change. By understanding

the motivations driving individuals and the cultural influences shaping their perceptions, gamification strategies can be tailored to resonate with diverse audiences. As gamification continues to evolve, integrating insights from psychology and cultural studies will be imperative for refining strategies and maximizing their impact on behavior. Through an integrated approach that considers psychological principles and cultural nuances, gamification can truly unlock its potential as a powerful tool for promoting positive behavioral change in various contexts.

CHAPTER 3: METHODOLOGY

This chapter will delineate the intricacies of the gamification process, with a specific focus on the development of a serious game designed for instructing on the CMMC. A serious game, in this context, is distinguished from conventional games by its educational and informative objectives.

3.1 Research Method

The chosen methodological approach for this project is qualitative, emphasizing textual analysis. Specifically, the examination will revolve around dissecting the textual descriptions of CMMC practices to extract pivotal elements for game implementation. This involves a comprehensive investigation into themes, patterns, and the specific language employed within the CMMC model.

3.2 Project Overview

Introducing an educational initiative, the forthcoming game is crafted to dynamically explore the nuances of the CMMC. Employing a 3D framework, the game will be structured across three levels, aligning seamlessly with the distinctive tiers of the CMMC model. The incorporation of Levels 1 and 2 will involve the selection of specific security practices, while Level 3 remains a consideration for a potential future project. Acknowledging time constraints, the integration of CMMC practices into the game will be purposeful and selective. Emphasizing accessibility, the game is intended to be readily available online, offering a workplace-appropriate and captivating platform for users seeking a comprehensive grasp of the CMMC Model. It is crucial to underscore that, due

to time constraints, comprehensive research and extensive feedback collection will be streamlined, prioritizing an efficient approach to game development.

3.2.1 Project Description

This project involves the development of an online, 3D educational game focused on the Cybersecurity Maturity Model Certification (CMMC). Structured into three levels corresponding to CMMC tiers, the game imparts knowledge of selected security practices. With a workplace-appropriate theme and emphasis on accessibility, the game is planned to be created using JavaScript/HTML/CSS and Babylon.JS, adopting an Agile project management approach.

3.2.2 Audience

In determining the target audience for the educational game centered on the CMMC, careful consideration was given to various demographic groups. Children were deemed less likely to benefit from the model or engage with it, given its specialized nature. College students, whose interests are contingent upon their major and career path, were recognized as a diverse group with varying levels of relevance to CMMC. It was acknowledged that not every college student would use or require knowledge of the CMMC model.

Conversely, the focus was on employees as a primary audience. The rationale behind this choice lies in the growing trend of CMMC becoming a job requirement for numerous companies and their workforce. This strategic decision is underpinned by the recognition that making CMMC compliant with a job requirement serves as a robust

motivator for employees. By linking job security and performance to proficiency in this critical cybersecurity model, the approach aims to impart a tangible and immediate significance to the learning process.

The final choice, therefore, is to prioritize general employees, emphasizing the teaching of the CMMC model over the game elements. Within this framework, employees will be afforded the flexibility to choose between reading a manual or engaging with the game to learn about CMMC. This approach acknowledges the diverse learning preferences and requirements of the target audience.

The decision not to focus on a specific company or certain employees is grounded in the acknowledgment of differences in age and the distinct security needs prevalent across various organizations. It is recognized that certain companies may choose to emphasize specific security controls tailored to their requirements and goals. Consequently, a training option such as the game may prove advantageous to a single company, catering to its specific needs, but may lack universal applicability. The chosen approach, therefore, is to prioritize a broader teaching of the CMMC model, ensuring relevance across diverse organizational contexts.

3.2.3 Theme Selection

In determining the thematic backdrop for the educational game focused on the CMMC, various considerations were explored to ensure both engagement and relevance.
One option considered was a space theme. This choice was motivated by its distinctiveness, offering a departure from more common themes. The inclusion of "cyberspace" adds a playful element, and the technological context of space stations

aligns with the cybersecurity theme. Despite uncertainties about spaceship design and specific limitations, the space theme was deemed promising for its unique appeal and potential for creative application. The name would be “Astro Guard.” Considerations for this idea are in the tables below.

Theme: Space	
Proposed Name: AstroGuard	
Description:	Embark on a cosmic journey, shield your vessel, conquer escalating mini levels within stages, and fortify your craft with collected coins, all while mastering the CMMC 2.0 model for seamless progression.
Environment	• Cyber “Space” • Some levels may have asteroids, comets, galaxies, etc.
Characters	• First person viewpoint • The character will be in a spaceship. • Character will not be visible; hands will be visible to complete tasks. • Inside of ship will be shown, outside of ship may be shown for specific situations/mini levels
Gameplay	• Fly through space. • Avoid obstacles and respond to threats properly. • Collect coins to purchase different powers for your ship.

Table 1 Space Theme Considerations

Astro Guard Game Play Examples (Level 1)			
Security Family	Security Control	Implementation	Gameplay Elements
Limiting Information System Access	Security Clearance	The player must manage access to the spaceship's systems, ensuring that only authorized users, processes, and devices can interact with sensitive components.	The player encounters puzzles that need to be solved to gain access to critical areas, mimicking the process of cracking encryption to gain access.
Limiting Access to Authorized Functions	Tactical Decision-Making	The player needs to ensure that the spaceship's systems can only perform functions permitted for the user's role.	The player needs to make strategic decisions about which systems to activate, deactivate, or modify to fulfill mission objectives while adhering to security protocols.
Verifying and Controlling External Connections	Network Monitoring Console	The player monitors and manages connections between the spaceship and external systems, ensuring they are secure and authorized.	The player oversees incoming and outgoing network traffic, identifying suspicious connections and taking action to block unauthorized access attempts.

Table 2 Space Theme Game Play Examples

Contrastingly, a beach theme was also contemplated. The idea was to create an atmosphere of relaxation while undergoing training, catering to individuals who find enjoyment in ocean-related environments. However, this choice posed limitations, particularly concerning inappropriate content such as blood effects and potential negative associations with shark attacks. The ocean's movement, a challenging aspect to mimic accurately, also factored into the decision-making process.

Theme: Ocean	
Proposed Name: CyberTide	
Description:	Dive into the ocean, get to know the CMMC 2.0 model, and have a blast taking in the awesome views. Grab coins to give your diver cool special powers!
Environment	• Ocean • Some levels may have underwater tunnels, treasure chest/safe, sunken ships, cages, underwater data storage, etc.
Characters	• First person viewpoint • Diver may be visible in some instances. • Diver's hands will be visible to complete tasks.
Gameplay	• Swim in the sea • Avoid obstacles and respond to threats properly. • Collect coins to purchase special powers for your diver.
Additional Considerations	Options to consider (need to choose one) • Explore the ocean freely and complete quests (free play) • Quests are provided for the user to complete during gameplay. • Protect an area in the ocean from predators (Atlantis, etc.) * Need to consider what happens when diver is attacked /harmed (blood or just black screen then back to level menu) * Need to consider the depth that divers can go to and what they can explore.

Table 3 Ocean Theme Considerations

CyberTide Game Play Examples (Level 1)			
Security Family	Security Control	Implementation	Gameplay Elements
Limiting Information System Access	Bio-Lock Mechanisms	Players must manage access to underwater systems and structures, ensuring that only authorized organisms, devices, or processes can interact with sensitive components.	Players need to solve puzzles involving coral patterns, bioluminescent organisms, or other underwater elements to grant access to restricted areas.
Limiting Access to Authorized Functions	Ecosystem Interactions	The player needs to ensure that the spaceship's systems can only perform functions permitted for the user's role.	Players interact with different marine species that have unique abilities. Using these abilities strategically, they can unlock new areas and advance through the game.

Verifying and Controlling External Connections	Sonar Network Monitoring	Players monitor and manage connections between underwater systems and external entities to ensure security and integrity.	Use virtual sonar technology to detect unauthorized activities and connections from marine creatures or artificial devices.

Table 4 Ocean Theme Game Play Examples

A detective theme, centered on mysteries and detective stories, was another option considered. Despite the theme's popularity, personal unfamiliarity with storytelling in this genre presented challenges in creating an engaging narrative. Furthermore, concerns about the inappropriateness of murder and crime-related content posed constraints on this thematic choice.

Theme: Detective	
Proposed Name: CyberSleuth	
Description:	CyberSleuth is an immersive game fusing mystery solving with CMMC 2.0 learning. As a cyber detective, explore digital realms, crack complex cybersecurity puzzles, and uncover a captivating narrative.
Environment	• Futuristic City • Virtual Spaces represent different aspects of the cyber world (Dark web, social media platforms, corporate networks, etc.) • Secret underground hideouts or digital cafes where hackers and others meet to gather information
Characters	• The user will be a Detective – visible, may have a first-person perspective. • There will be other characters the detective can interact with to gather information.
Gameplay	• Digital Forensics: Allow players to analyze digital evidence, such as logs, emails, and code snippets, to piece together the mystery. • Social Engineering Include scenarios where players use social engineering techniques to gain information from characters or manipulate events. • Develop puzzles and challenges related to real-world cybersecurity problems that players must solve to progress.

Table 5 Detective Theme Considerations

CyberSleuth Game Play Examples (Level 1)			
Security Family	Security Control	Implementation	Gameplay Elements
Limiting Information System Access	Social Engineering Scenarios	Players must manage access to virtual systems, databases, and digital infrastructure, ensuring only authorized entities can interact with sensitive data.	Incorporate scenarios where players must engage in dialogue with NPCs (non-player characters) to gain access, highlighting the importance of human factors in cybersecurity.
Limiting Access to Authorized Functions	Digital Artifact Manipulation	Players enforce permissions and control what digital entities can do, just as in the cybersecurity principle of granting limited access.	Players manipulate digital artifacts or symbols in the environment to unlock different functions, reflecting the concept of authorization.
Verifying and Controlling External Connections	Phishing Awareness Training	Players monitor and manage the connections between the cyber city's systems and the external digital environment, guarding against unauthorized access.	Introduce "phishing" scenarios where players must identify suspicious communication requests and block them, emphasizing the importance of verifying external connections.

Table 6 Detective Theme Game Play Examples

The final choice settled on the space theme. The decision was influenced by the theme's uniqueness, the potential for creative exploration, and its applicability to the technological aspects of cybersecurity. Importantly, the space theme avoids the mundane nature of an office setting, ensuring a more exciting and engaging user experience. To provide a comprehensive overview, tables will be included below each theme, outlining the considered options, associated drawbacks, and planned strategies for implementation.

This meticulous approach aims to facilitate an informed understanding of the thematic decision-making process and the subsequent development plans.

3.2.4 Dimensional Format

Both 2D and 3D formats were evaluated for the game development. Considering the audience and the core aim of conveying complex communication concepts effectively, the decision was made to opt for a 3D format. The rationale behind this choice lies in the belief that the immersive nature of a 3D environment better mirrors real-world scenarios, enhancing the learning experience. The target demographic for this game primarily comprises average everyday employees, typically aged 20 and above. However, its design is intentionally inclusive, welcoming players aged 11 and older, thus ensuring accessibility across diverse age groups. The appeal of 3D gameplay is particularly pronounced among individuals aged 20 and above, as it offers heightened interactivity and user engagement, delivering a more compelling and immersive experience.

3.2.5 Technology and Tools

Throughout the project planning process, careful consideration was given to selecting tools crucial for ensuring efficiency and organization. In the initial plan, SharePoint was identified as the central platform for sharing updates and consolidating resources conveniently. GitHub, recognized for its importance in code management, was chosen to maintain code organization and facilitate version control. IntelliJ IDEA, renowned for its robust code-editing capabilities, was designated as the primary

integrated development environment (IDE) due to its alignment with project requirements. To streamline GitHub interaction, GitHub Desktop was utilized, providing an accessible interface for repository management. Supplementary tools were anticipated for asset integration as needed, ensuring a tailored approach to dynamic project demands. The strategic integration of these tools aimed to optimize workflow, collaboration, and resource management throughout the developmental stages of the educational game.

In actual execution, the project primarily relied on Unreal Engine for development, supported by email and SharePoint for communication and resource coordination. Video updates were leveraged to document progress effectively. Additionally, Adobe Photoshop played a significant role in asset creation and modification. This adaptation of tools ensured flexibility and responsiveness to the evolving needs of the project, aligning with the overarching goal of efficient project management and execution.

3.2.6 Game Prototype – Main / Dashboard Screen

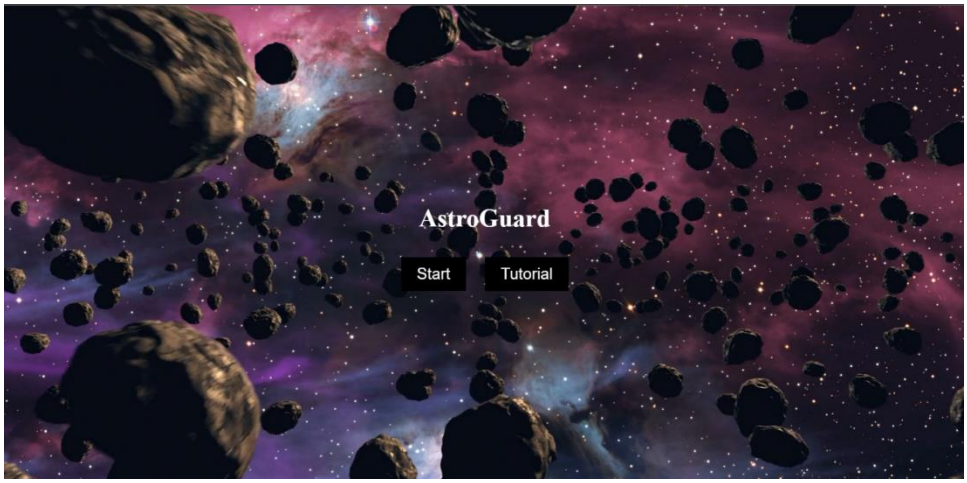

Figure 2 Main Screen

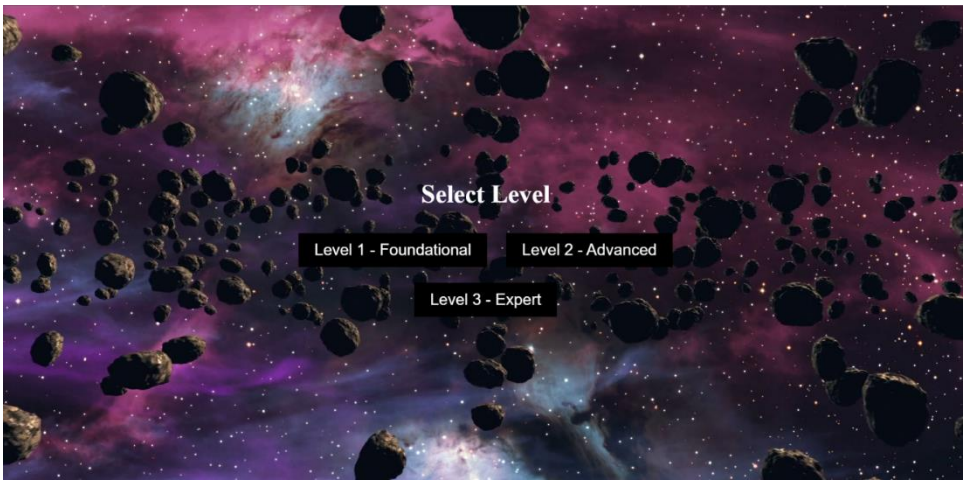

Figure 3 Level Screen

3.2.7 Game Development

In considering the appropriate development framework for the educational game, several options were evaluated, each with its set of advantages and challenges. Unity, although widely used and versatile, was deemed less feasible due to a lack of familiarity and potential difficulties with the export process, especially concerning accessibility through web browsers without additional application downloads. A similar challenge arose with Unreal, which, while known for its professional capabilities, presented a steeper learning curve and posed similar issues with web browser accessibility.

Conversely, the JavaScript/HTML/CSS combination emerged as a promising choice. With a moderate level of familiarity with JavaScript and proficiency in HTML/CSS, this option offered the advantage of easy accessibility via web browsers. Given the emphasis on widespread availability and user-friendly access, this became the preferred choice for the game's development.

Furthermore, the decision was made to utilize Babylon.JS, a JavaScript framework for building 3D games. While other options such as three.js were considered, Babylon.JS stood out for its focus on rendering photorealistic images. This aligns with the vision of creating a game with a realistic feel, enhancing the overall user experience by immersing them in a visually compelling and authentic environment. Notably, Babylon.JS not only serves as a rendering engine but also functions as a game engine, providing a comprehensive solution for the envisioned educational game. This thoughtful selection aims to elevate the gaming experience and contribute to the game's effectiveness as an educational tool.

However, after establishing the environment in Babylon, the absence of prior experience in game development prompted a thorough reassessment of the available tools. Recognizing the need for a platform with substantial potential, despite its steep learning curve, the options between Unity and Unreal Engine were weighed.

Ultimately, Unreal Engine was chosen, fully aware of its complexity and the challenges it posed to beginners. While Unity is renowned for its beginner-friendly interface, Unreal Engine's extensive use by professional game developers and its capacity to deliver higher-quality environments and experiences were compelling factors. Despite the anticipated difficulties in learning the intricacies of Unreal Engine, it was seen as an opportunity to push the boundaries of the educational game project.

One particularly challenging aspect initially was the packaging process in Unreal Engine. However, further investigation revealed that Unreal Engine offers an option to package the game as a Windows executable (EXE) application, eliminating the need for additional software downloads and simplifying the distribution process.

Understanding that Unreal Engine demands more time and effort to master, the challenge was embraced in pursuit of unlocking its full potential. It was recognized that this decision would require dedication not only to learning the software but also to refining skills in game design, implementation, and development.

While Unity may have offered a gentler learning curve, Unreal Engine was chosen because it was believed to provide the project with the greatest scope for growth and sophistication, even if it meant navigating a more complex path to proficiency.

3.3 Limitations and Constraints

Navigating the landscape of educational game development, various limitations and constraints demand careful consideration. Primarily, the limited prior experience in game development poses a potential challenge, as the learning curve associated with this unfamiliar territory may impact the efficiency and speed of the development process. Additionally, the learning curve associated with game development plays a crucial role in shaping the project's trajectory.

An additional constraint arises from the incomplete specifications of CMMC. Given that the CMMC is not fully finalized, potential changes or updates to its specifications may occur during the project, necessitating adaptability in the development process. Technological compatibility issues, especially concerning the integration of different technologies or frameworks, may pose challenges and impact the overall functionality of the game.

Ensuring accessibility for users with diverse needs and platforms adds another layer of complexity, potentially posing challenges in providing a seamless experience

across different environments. The creation and integration of assets, such as 3D models or graphics, present challenges that may be influenced by constraints in skill sets or access to suitable resources. Testing, a critical aspect of the development process, may be constrained by factors such as time limitations or the availability of diverse testing environments, potentially impacting the identification and resolution of bugs.

Furthermore, the adoption of Babylon.JS or other tools introduces a learning curve that may impact the efficiency of the development process until a proficient level is achieved. There's a need to remain vigilant against potential scope creep as the project progresses, guarding against the temptation to expand the project's scope beyond the initial vision, which could lead to time and resource overruns. Lastly, due to time constraints, collecting and incorporating user feedback may be limited, impacting the refinement of the game based on user experience. Despite these challenges, a proactive and adaptable approach is crucial to navigating and mitigating the impact of these limitations throughout the project's lifecycle.

The initial time constraint was a significant limitation, as the asset (3D spaceship) was received on January 29th, following a request made on January 16th. This shortened time limit posed challenges in both asset integration and familiarization with the development platform. Additionally, encountering frequent crashes and freezing issues with Unreal Engine, particularly after updates, hindered the development process. The necessity to close other software while working in Unreal Engine to prevent freezing further compounded the time-consuming nature of troubleshooting and researching solutions.

Utilizing a gaming-oriented laptop ensured the device could effectively handle running heavier software. Additionally, encountering an issue with Unreal Engine freezing upon using the "Save All" function required manually saving individual files, resulting in additional time expenditure and occasional loss of progress due to Unreal Engine crashes failing to restore previous work.

Troubleshooting errors in Unreal Engine proved challenging due to the software's limited error reporting, requiring extensive research and trial-and-error to identify and resolve issues. This further extended the development timeline and added complexity to the process. Despite these constraints, perseverance and adaptability were crucial in overcoming challenges and progressing towards project completion.

3.4 Timeline

Originally, the project's timeline was strategically designed to coincide with the academic calendar. The proposal phase took place in December, with active efforts to secure a timeline for this crucial stage. With a projected graduation date in Spring 2024, the capstone project was divided into two semesters, spanning Fall 2023 and Spring 2024. This intentional division allowed for a methodical and comprehensive approach to the development of the educational game, ensuring that each stage received the necessary attention and diligence for a successful outcome.

However, adjustments were made to the plan as the project progressed. The creation of the space skybox took place in December, and the actual game development began in February after receiving the spaceship asset at the end of January. Despite these

changes, the project remained on track, and considerable progress was made. The project was completed by mid-April, meeting the established timeline and project requirements.

CHAPTER 4: OUTLINE OF COMPLETED PROJECT

This chapter offers a thorough overview of the finalized project, focused on the creation of a 3D game aimed at educating ordinary employees about Cybersecurity Maturity Model Certification (CMMC) principles. It provides detailed insights into the game's structure, mechanics, and adherence to CMMC standards, highlighting its innovative strategy in bolstering cybersecurity awareness among non-technical staff.

4.1 Overview of CMMC Gamification Components

The gamified approach developed for teaching CMMC concepts focuses specifically on four controls within Level 1 of the CMMC framework: Identification, Authentication, Authorized Access Control, and Limited Physical Access. Within the game, various components are utilized to present scenarios requiring the user to complete tasks to progress or gain access to different areas.

Identification is illustrated through a scenario where the player is prompted to fill out a form at Computer A with their credentials, displayed within a collapsible button on the screen. Feedback is provided based on the values entered, and upon successful submission, an identification card appears on the player's screen. This card grants access to the cargo room, showcasing both Authorized Access Control and Limited Physical Access.

Upon obtaining a glowing hex orb, signifying a promotion, the player can request access to door 2. They return to the cargo room and fill out a form at Computer B, highlighting the increased security measures required for higher-level access. Successful submission results in an access card appearing alongside the identification card. Access to door 2 is granted, demonstrating Authorized Access Control, yet the player encounters limited physical access when attempting to retrieve a file in the cargo room.

Additionally, the game features colored 'i' icon objects disseminated throughout the environment, each providing information about one of the controls. Furthermore, glowing Aztec coin objects are strategically placed to engage users and present facts or statistics related to cybersecurity.

To maintain focus and prevent overcrowding, objects disappear after the player interacts with them. The game incorporates prompts to familiarize players with movement controls and emphasizes the importance of following numbered objects strategically placed throughout the environment. This design choice is intended to guide player progression in the absence of a formal task or quest system, which may be subject to future refinement.

4.2 Integration with Traditional Training Models

The gamification approach complements traditional CMMC training models by offering an engaging and interactive learning experience. Unlike conventional methods that typically involve reading manuals or attending lectures, gamification immerses users in a virtual environment where they actively participate in scenarios related to CMMC concepts.

By presenting CMMC principles in the form of challenges, decision-making scenarios, and interactive tasks, the gamification approach stimulates users' cognitive engagement and fosters a deeper understanding of the material. This hands-on approach is particularly effective in reinforcing learning retention as users are more likely to remember information when it is presented in the context of meaningful experiences or interactions.

Furthermore, gamification provides an opportunity for users to apply theoretical knowledge in practical situations, thus bridging the gap between theory and real-world application. Through gameplay, users can explore different scenarios, experiment with various strategies, and observe the consequences of their actions in a risk-free

environment. This active learning process not only enhances comprehension but also promotes critical thinking and problem-solving skills.

Overall, by integrating gamification with traditional models of CMMC training, organizations can create a more dynamic and effective learning experience that resonates with a broader audience. By leveraging the engaging nature of games, users are more motivated to actively participate in the learning process, leading to improved knowledge retention and proficiency in CMMC concepts.

4.3 User Interface and Experience Design

During development, meticulous attention was paid to design principles and user interface considerations to ensure an engaging and effective learning experience. One key aspect was the strategic use of colors and objects within the interface design.

The choice of colors was deliberate, aiming to create a visually stimulating environment conducive to learning. Vibrant and contrasting colors were employed to draw the users' attention to important elements while maintaining coherence and accessibility throughout the interface. This thoughtful selection of colors not only enhanced the aesthetic appeal but also contributed to the overall usability and user experience.

In addition to colors, careful consideration was given to the selection of objects within the gamified environment. Emphasis was placed on simplicity and clarity, opting for easily recognizable objects such as labeled computer screens and coin collectibles. These objects served as visual cues and interactive elements that reinforced key concepts and encouraged user engagement.

To streamline information delivery and prevent overwhelming users with text, iconography played a crucial role. Instead of relying solely on textual explanations, intuitive icons were strategically integrated into the interface to convey information concisely and efficiently. This icon-based approach not only minimized cognitive load but also catered to diverse learning preferences, ensuring accessibility for all users.

Furthermore, the incorporation of gamification elements such as numbers and a spaceship motif added layers of enjoyment and immersion to the learning experience. By introducing numerical challenges and a thematic narrative, the training program transcended mere instruction and transformed into an interactive adventure. The spaceship served as a captivating focal point, injecting fantasy into the educational context and fostering a sense of excitement and curiosity among users.

Overall, the design principles and user interface considerations employed in the gamified CMMC training were meticulously crafted to optimize engagement, comprehension, and retention. Through the strategic use of colors, objects, icons, and gamification elements, the training program succeeded in creating an immersive and enjoyable learning environment that effectively conveyed complex concepts while motivating users to actively participate and progress.

4.3.1 Game Walkthrough

Upon initiation, the game interface displays a main menu, prominently featuring options for initiating gameplay or exiting the application, as depicted in Figure 4. The "Quit" button will terminate the game session when selected. Upon selection of the "play" button, the user is transitioned to a secondary screen denominated as the "level menu," wherein three distinct levels, constituting integral components of the CMMC Model, are

presented for potential engagement, as illustrated in Figure 5. Notably, Level 1 stands as the sole implemented segment, showcasing a preliminary array of controls, with ample scope for further augmentation in subsequent iterations. Conversely, Levels 2 and 3 remain as unimplemented entities within the current framework; however, they are accompanied by on-screen notifications intimating the prospect of their prospective integration in forthcoming developmental phases, as exemplified in Figure 6.

Figure 4 Main Menu

Figure 5 Level Menu

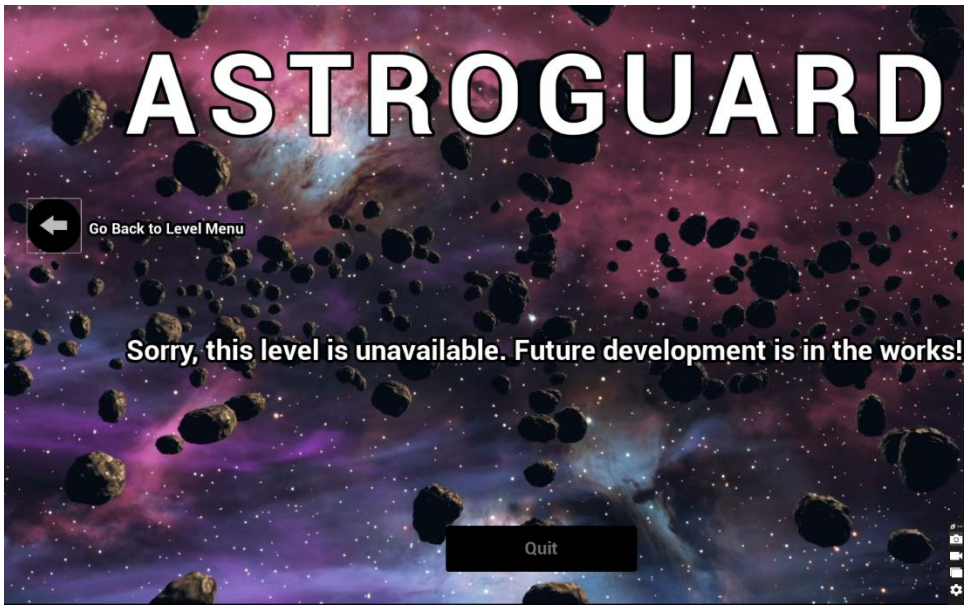

Figure 6 Level 2 and Level 3 Screens

At the initiation of gameplay, users are presented with game movement instructions, elucidating the methods for maneuvering within the virtual environment, including the utilization of the WASD or arrow keys for character movement, as well as mouse interactions for camera manipulation, as detailed in Figure 7.

Following this, upon the player's activation of the "next" prompt, the game initiates instructional prompts directing sequential engagement, emphasizing the crucial adherence to numerical sequences. Within Level 1, as delineated under the CMMC framework, elucidation is provided through informative icons concerning controls such as Identification, Authentication, Authorized Access Control, and Physical Access Controls. Supplementary elucidation is offered through interactive elements such as coins, disseminating pertinent insights into the realm of cybersecurity. Subsequently, upon player interaction with environmental objects, they are either absorbed into the

player's inventory or prompt the emergence of guidance on subsequent actions, elucidation on control functionalities, or the provision of cybersecurity knowledge. The game instructions are shown in Figure 8.

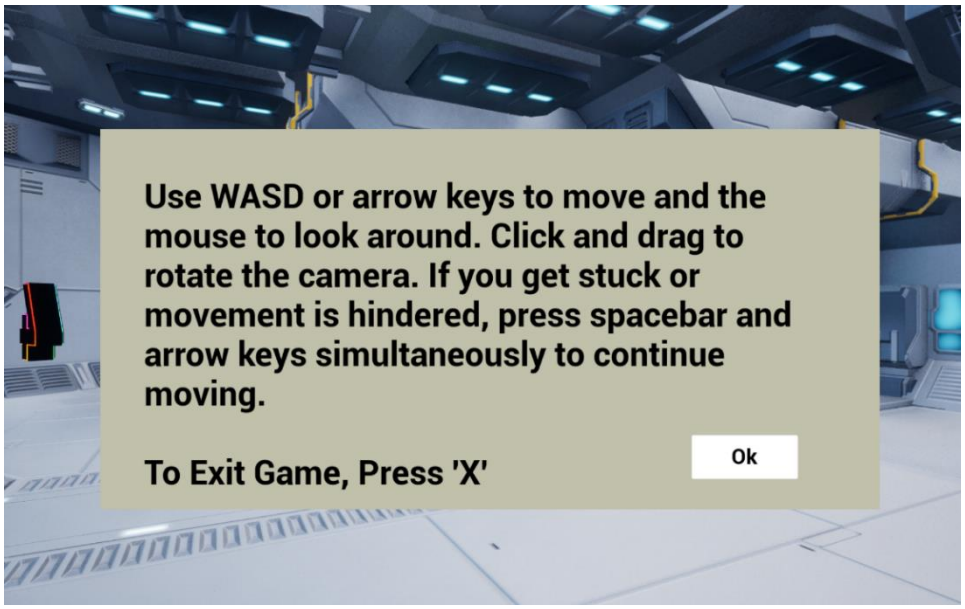

Figure 7 Game Movement Instructions

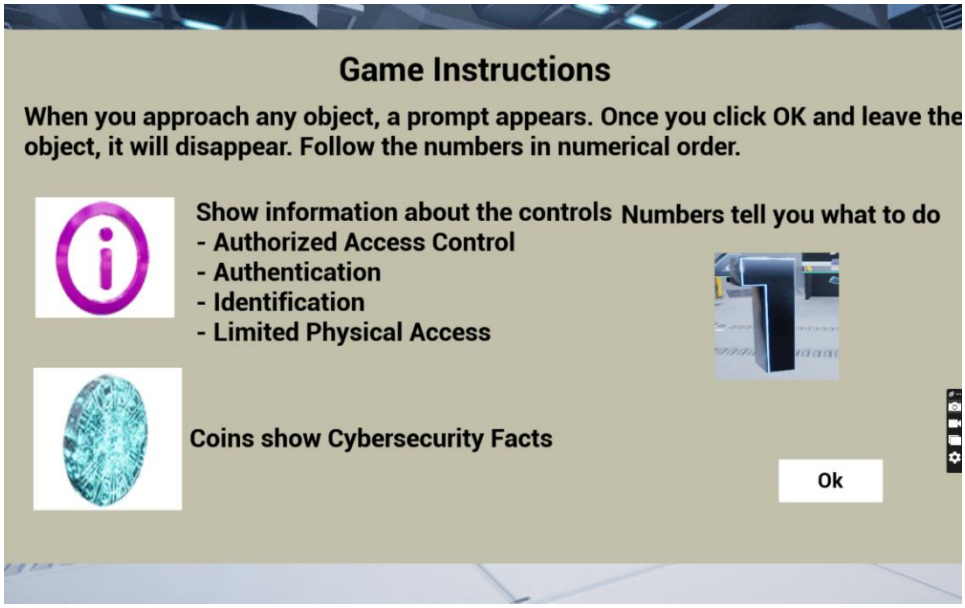

Figure 8 Game Instructions

Figure 9 shows the starting point for Level 1.

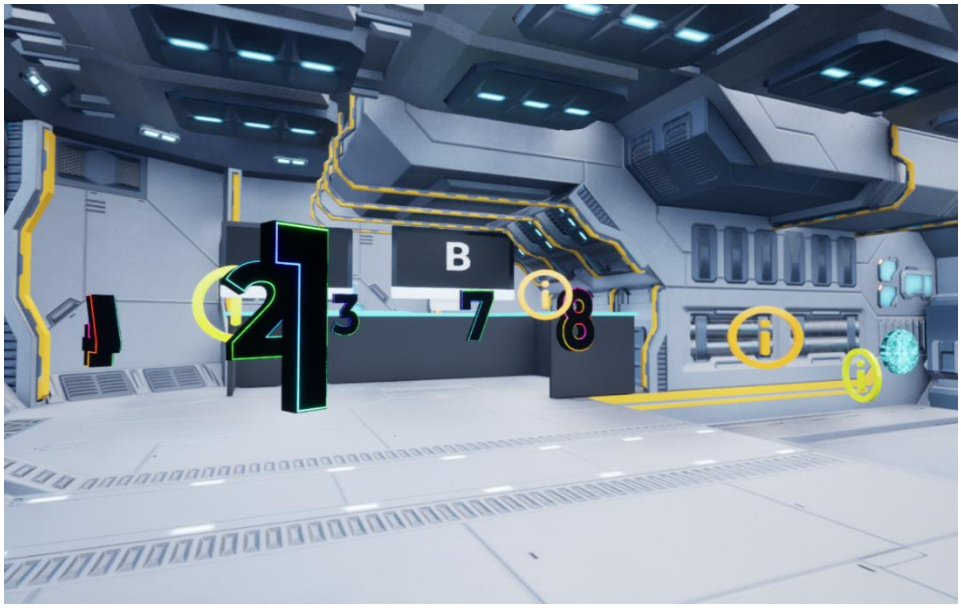

Figure 9 Level 1

Following the initial game instructions, the player progresses to step number 1, wherein they are presented with essential information regarding their character, including the character's name and their role within the game environment, as depicted in Figure 10. This segment serves to provide the player with a brief introductory narrative, elucidating the character's background and objectives.

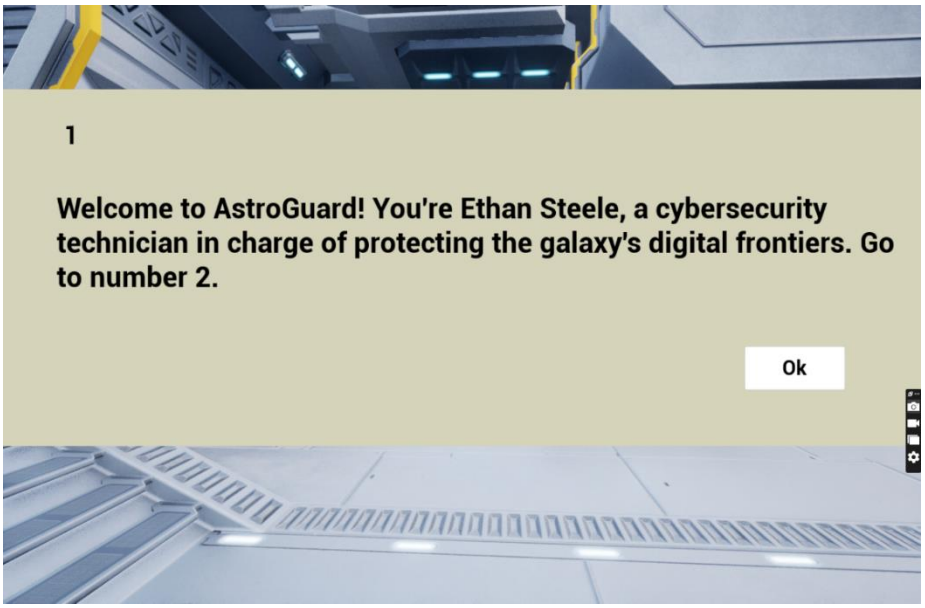

Figure 10 First Prompt

Following this, the player progresses to step number 2, as depicted in Figure 11, where they are instructed to proceed to step number 3 for additional guidance on acquiring the ID Card. Within step number 3, explicit instructions are provided, directing the player to navigate to Computer A to complete a form to acquire the ID Card. Emphasis is placed on the imperative exclusion of personal information and the utilization of player information from the top left corner when the form is displayed. These instructions are visually represented in Figure 12, which illustrates the guidance associated with step number 3.

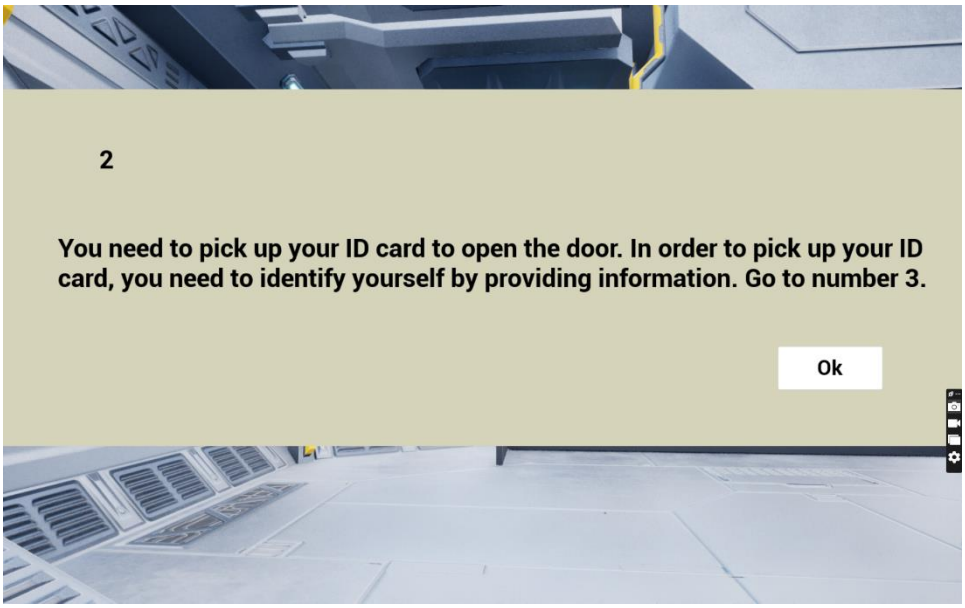

Figure 11 Second Prompt

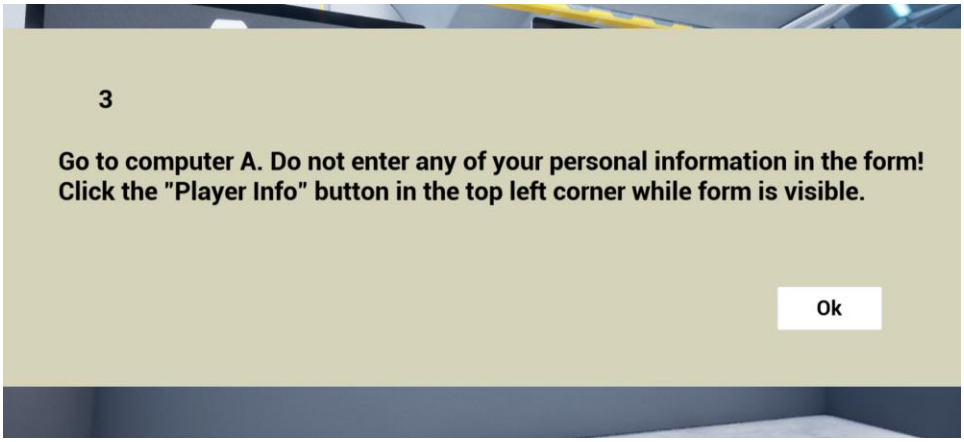

Figure 12 Third Prompt

Additionally, in the event of the player inputting incorrect information, corresponding error messages are promptly displayed adjacent to the respective input fields, as demonstrated in Figure 14. Upon successful entry of the correct information and subsequent submission of the form, a prompt promptly materializes, guiding the user to proceed to step number 4. At this pivotal juncture, the player is directed to employ the ID card, which promptly materializes on-screen after the accurate submission of the form.

This sequence of events is visually illustrated in the following figures: Figure 13 showcases the ID Pickup Form alongside Player Info; Figure 15 depicts the form after it has been submitted with the correct information, along with the prompt to proceed to step number 4; finally, Figure 16 showcases the ID Card displayed on the screen, indicative of its acquisition after the correct form submission.

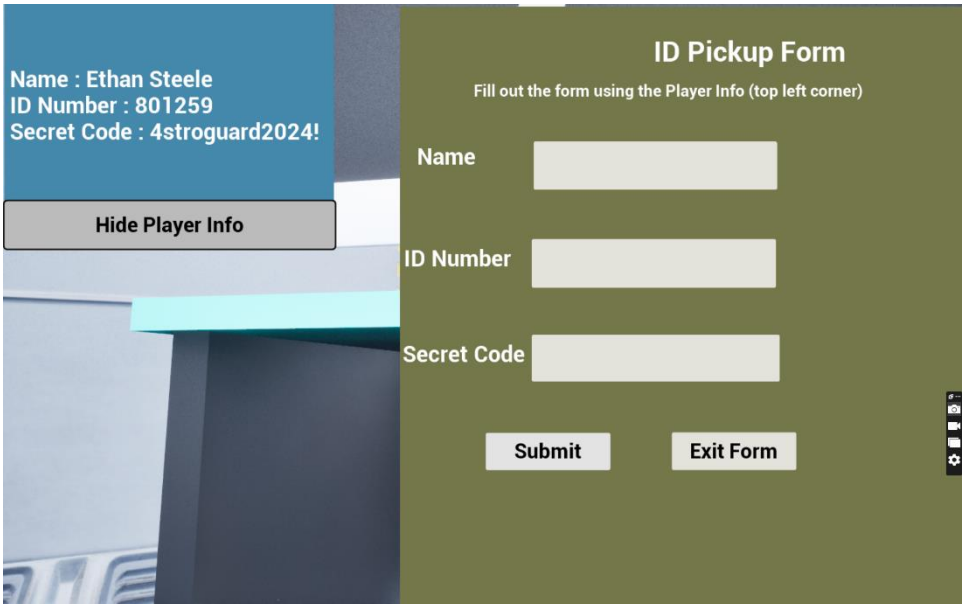

Figure 13 ID Pickup Form

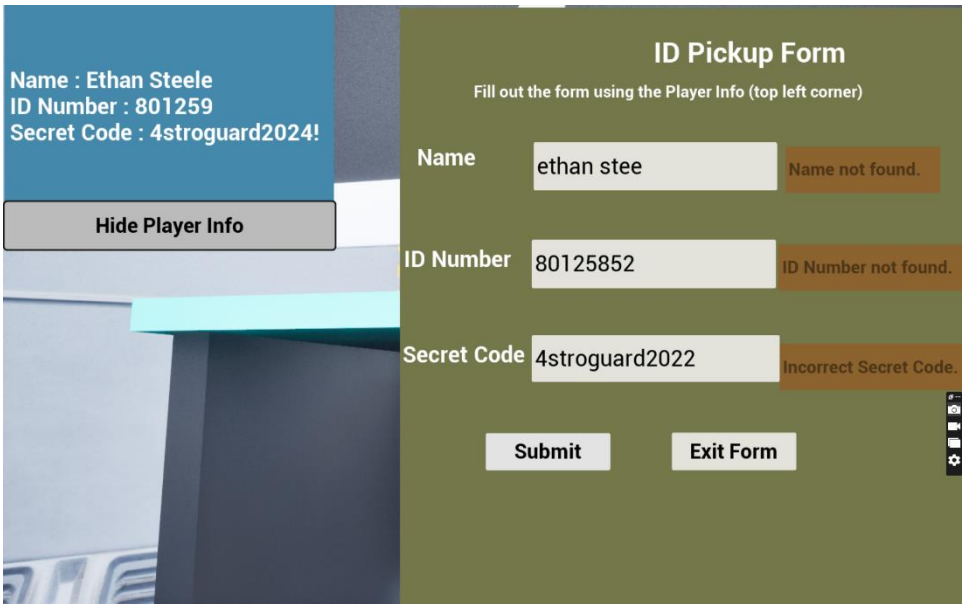

Figure 14 ID Pickup Form showing Input Validation

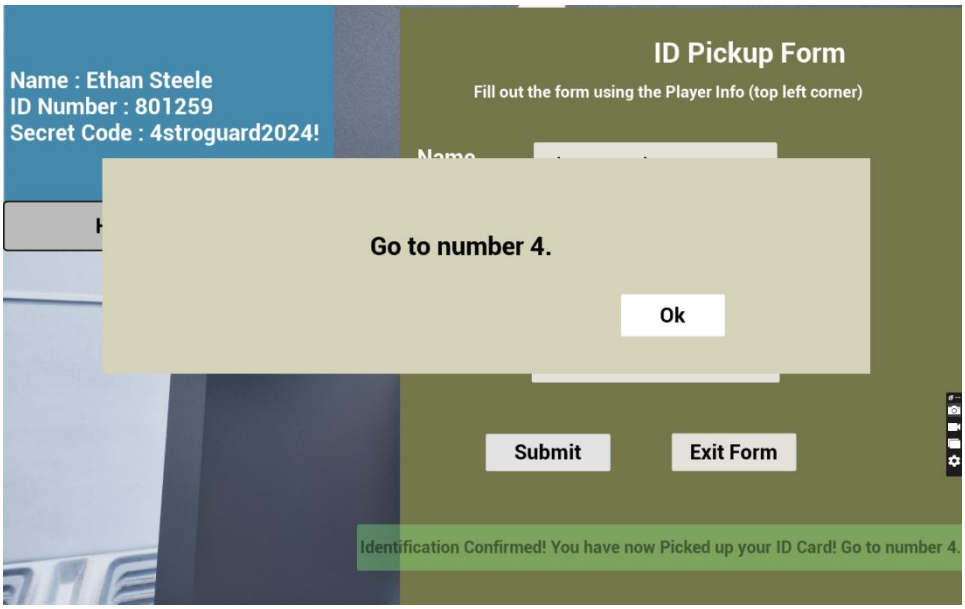

Figure 15 After Submit Prompt

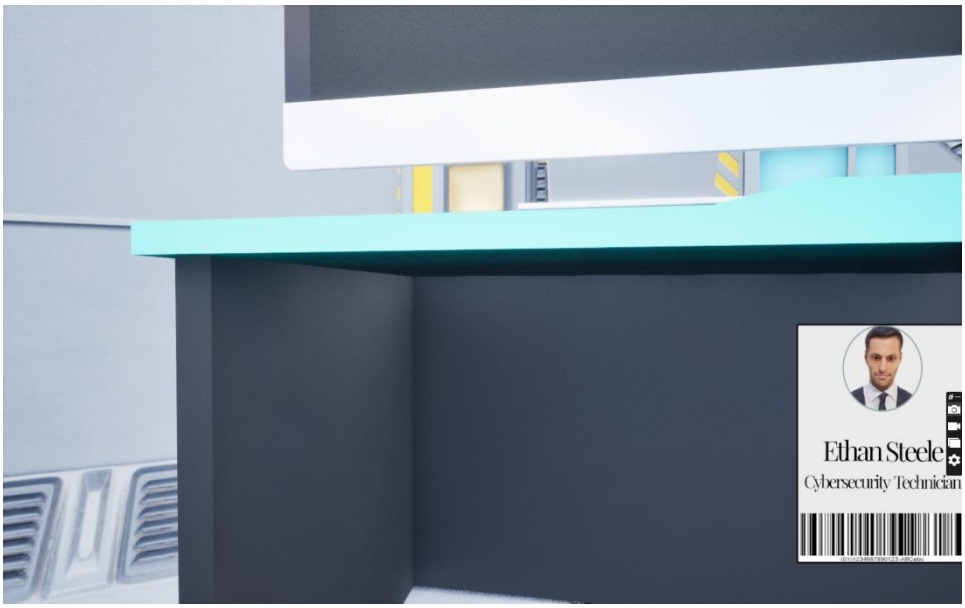

Figure 16 ID Card on Screen

Figure 17 illustrates one of the information icon prompts, specifically focusing on identification. This prompt elucidates to the player the concept of identification, elucidating its definition and providing an illustrative example, such as providing one's name. This icon is found near Computer B in the Cargo Area.

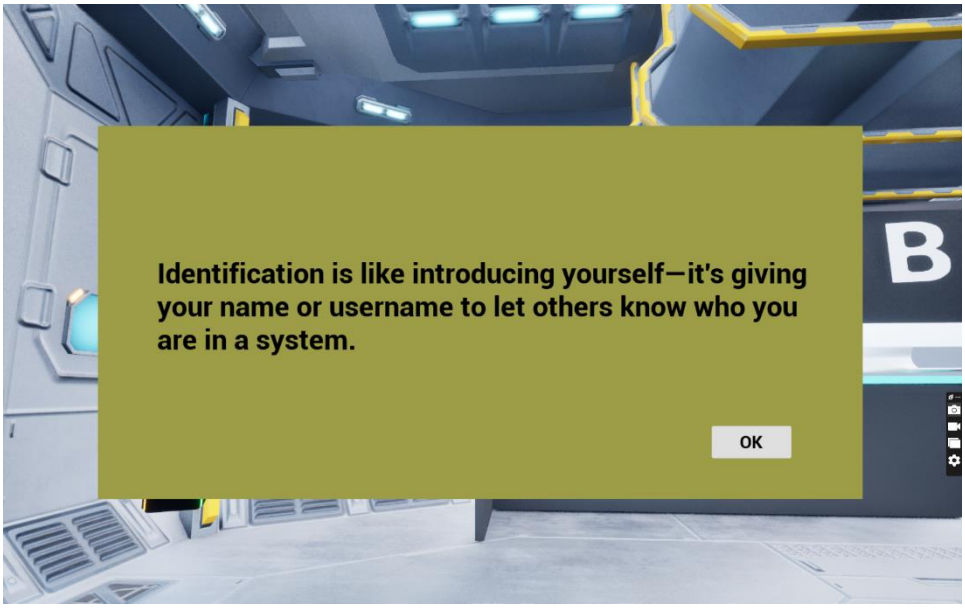

Figure 17 Identification Information

Upon reaching the doors, the player clicks the ID Card on the screen, prompting the doors to open. Within the corridor, number 5 stands before another set of doors, informing the player that higher access is required to proceed through these doors and explore the living quarters. Figure 18 illustrates this fifth prompt about needing higher access for the second set of doors.

Additionally, the corridor and living quarters contain fact coins and information coins for the player to collect. Notably, a promotion ball or hex ball is also present, and upon collection, it notifies the player of their promotion and directs them to proceed to number 7, located in front of Computer B within the Cargo Bay.

Upon returning to the Cargo Bay and utilizing the ID Card to access the doors, the player encounters number 7, which provides information about authentication while also representing authorized access control, as the player gains authorized access to the Cargo Bay. Figure 19 showcases an icon information prompt detailing common authentication factor, while Figure 20 displays an icon information prompt outlining examples of authorized access control. Moreover, Figure 21 illustrates the hex ball, and upon collection, it displays the promotion message depicted in Figure 22.

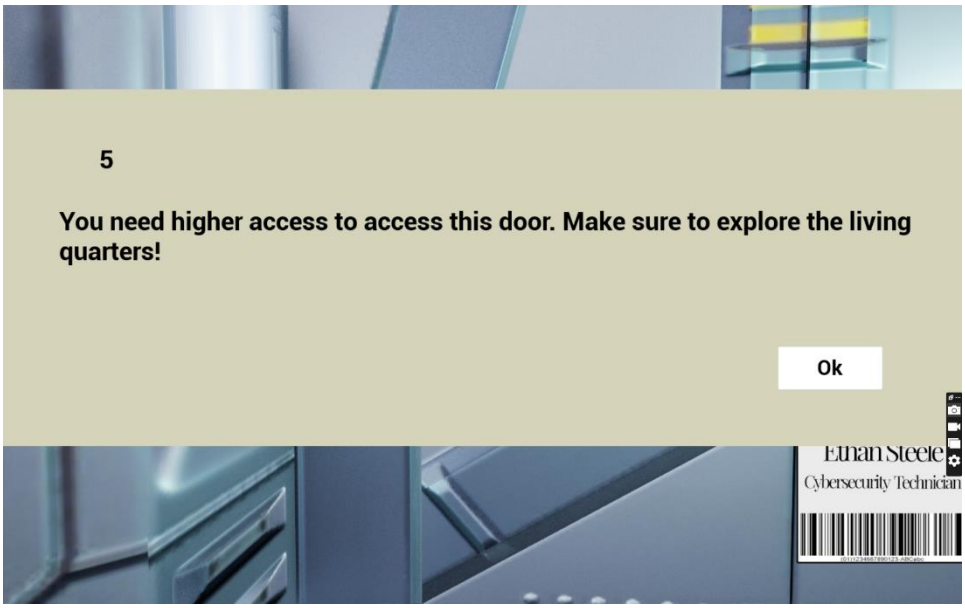

Figure 18 Fifth Prompt

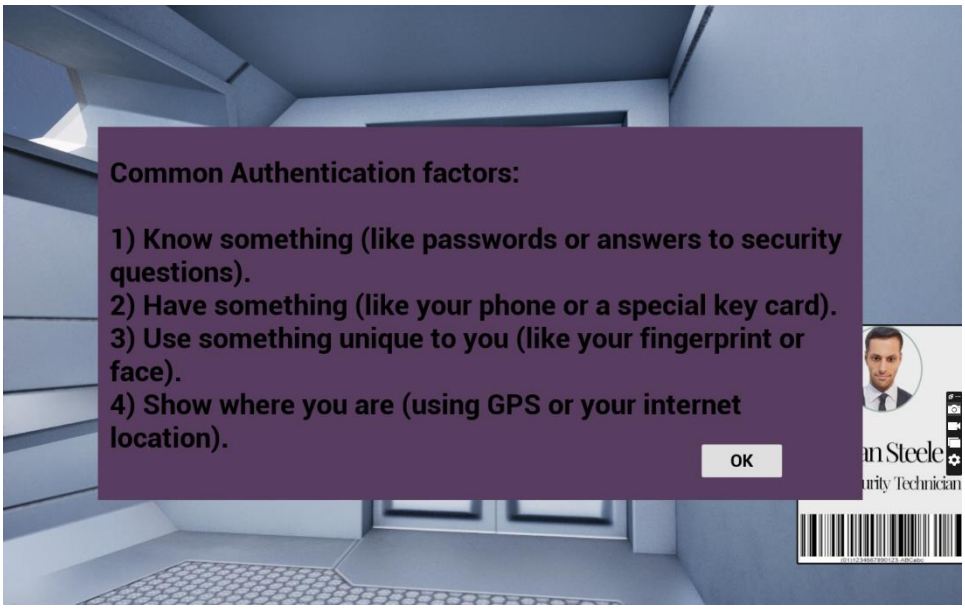

Figure 19 Common Authentication Factors

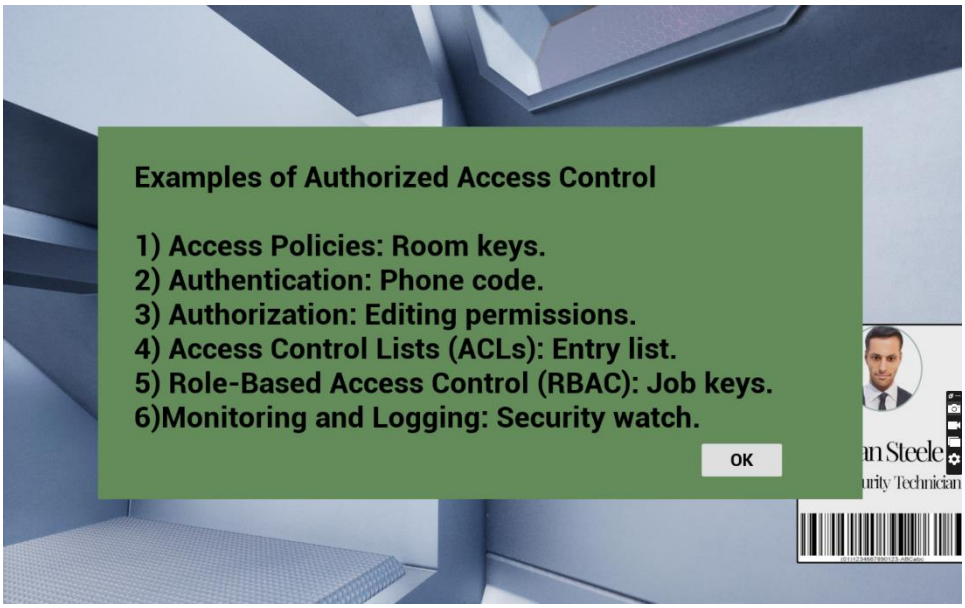

Figure 20 Examples of Authorized Access Control

Figure 21 Promotion / Hex Ball

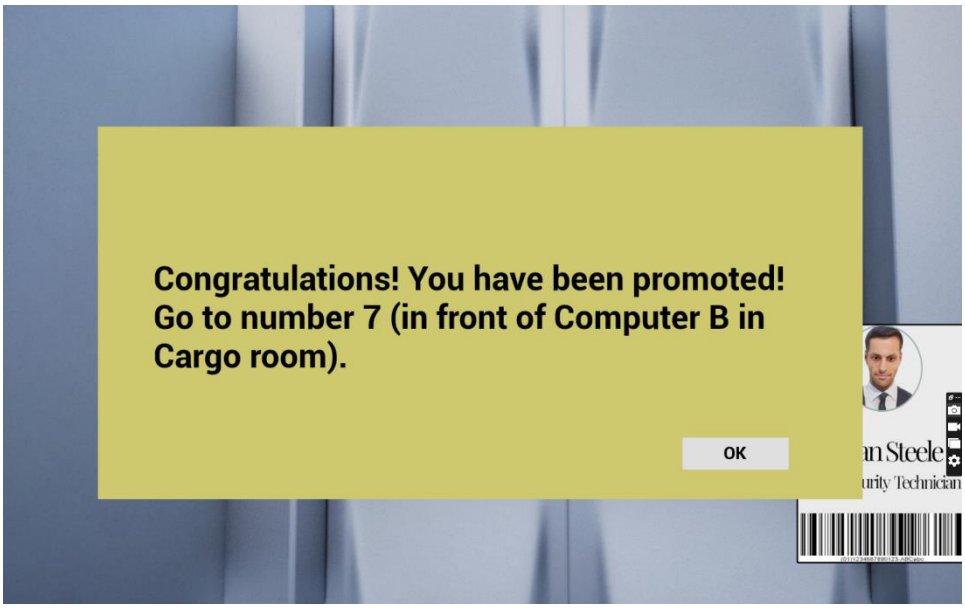

Figure 22 Promotion Prompt

Upon returning to the Cargo Bay using the ID Card to open the doors, the player proceeds to number 7, which not only provides authentication information but also symbolizes authorized access control, as the player receives authorized access. The prompt informs the player of an additional field on the form, necessitating a promotion code to be sent to their phone as a form of 2FA. At Computer B, the player encounters the form alongside a phone and their player information, as shown in Figure 23.

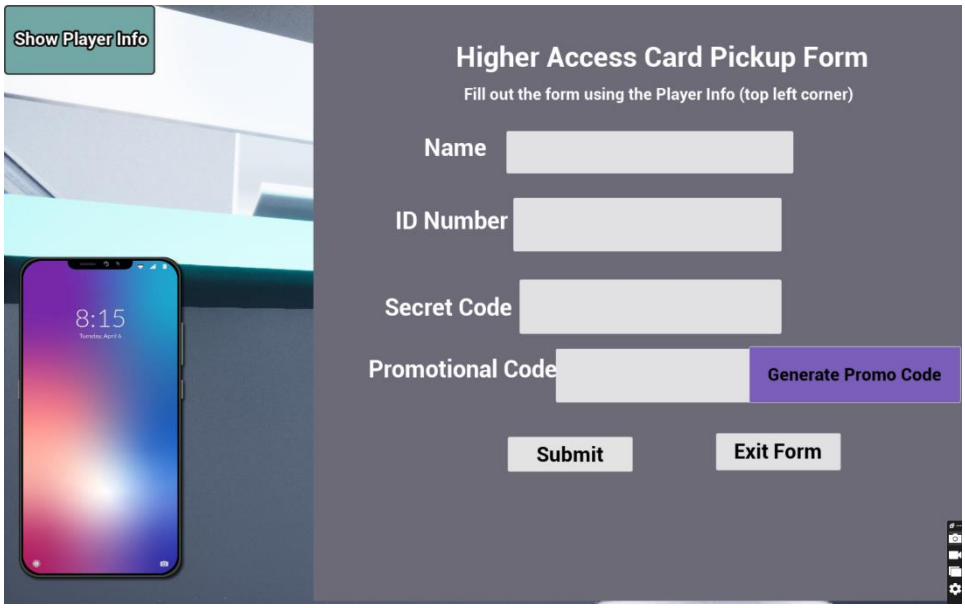

Figure 23 Access Card Pickup Form

Subsequently, the player fills out the form for the higher access card, clicking on the "generate promotion code" button to display the promotion code on the phone screen. The form includes input validation, ensuring the player inputs correct information to obtain the access card. Upon entering the correct information and clicking "submit," a prompt appears instructing the player to proceed to number 8. Clicking "OK," the player observes an access card above the ID card on the screen. The player then goes to number 8, receiving instructions to use their new access card to access the second set of doors. This process exemplifies authorized access control, emphasizing the necessity of using the correct cards for each set of doors, as the ID card does not grant access to the Cockpit/Control Room, and the access card does not grant access to the Cargo Bay.

Additionally, Figure 24 displays the form after clicking the "generate promo code" button, Figure 25 illustrates the screen after submitting the form correctly, and Figure 26 shows the higher access card displayed on the screen above the ID card.

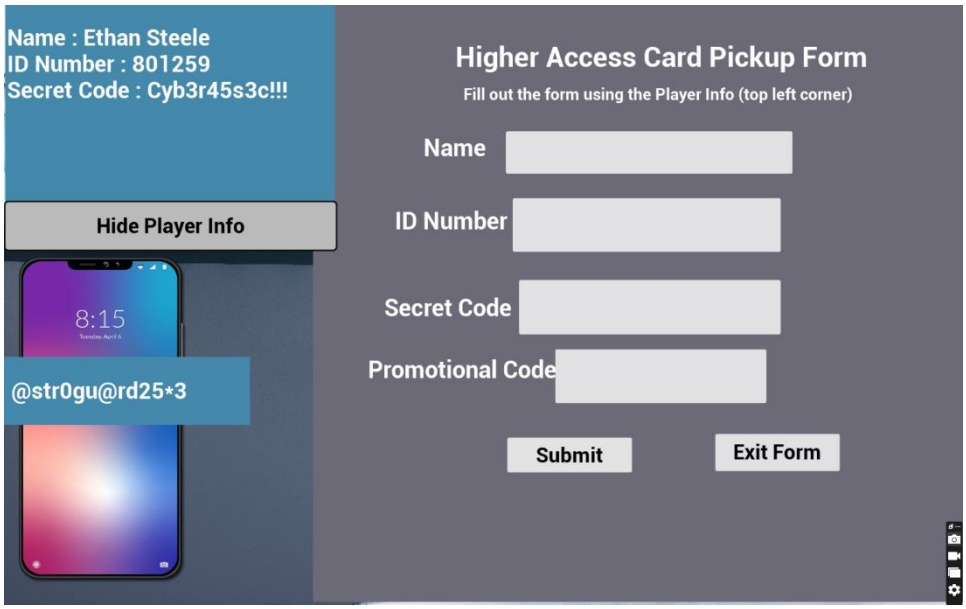

Figure 24 Access Card Pickup Form After Clicking Generate Promo Code

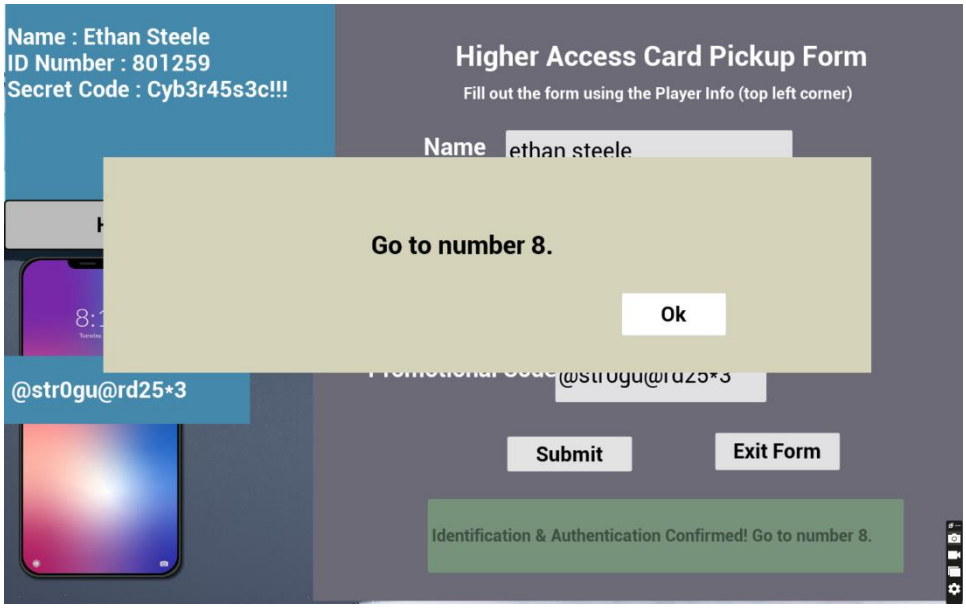

Figure 25 After Submitting Access Card Form Prompt

Figure 26 Access Card and ID Card on Screen

After successfully using the correct cards to open both sets of doors, the player gains access to the Cockpit/Control Room, exemplifying authorized access control in action. This serves as one illustrative example of how such control mechanisms are implemented within the game world. Figure 27 visually depicts the Cockpit/Control Room after gaining access.

Figure 27 Cockpit / Control Room Granted Access Using Access Card

Once in the Cockpit/Control Room, the player collects number 9, which prompts them to retrieve a file named "Cybersecurity_Audit_2023" from the filing cabinets in Cargo Bay. This file appears to require special permissions, suggesting that only approved individuals should have access to it. As the player collects facts and information coins, they become aware of the importance of these access restrictions. Figure 28 illustrates the number 9 prompt instructing the player to retrieve the "Cybersecurity_Audit_2023" file.

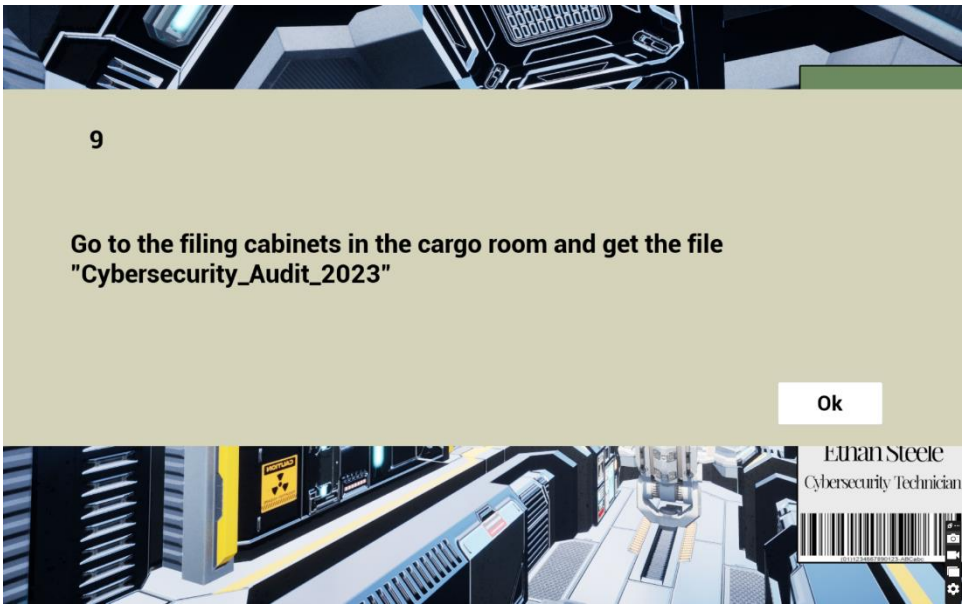

Figure 28 Physical Access Prompt

Returning to the Cargo Bay and nearing the filing cabinet area, the player receives a message indicating that they do not have access. This scenario exemplifies physically limited access, emphasizing that only individuals with proper authorization can enter these areas. Without the necessary access permissions, the player is unable to interact with or access these restricted areas.

Additionally, Figure 29 showcases the space skybox visible through the front windows of the cockpit, providing a visual context for the player's surroundings.

Figure 29 Skybox View Inside Cockpit

Figure 30 shows the filing cabinets area, and Figure 31 illustrates the message that appears, indicating that the player cannot access this area due to a lack of authorization.

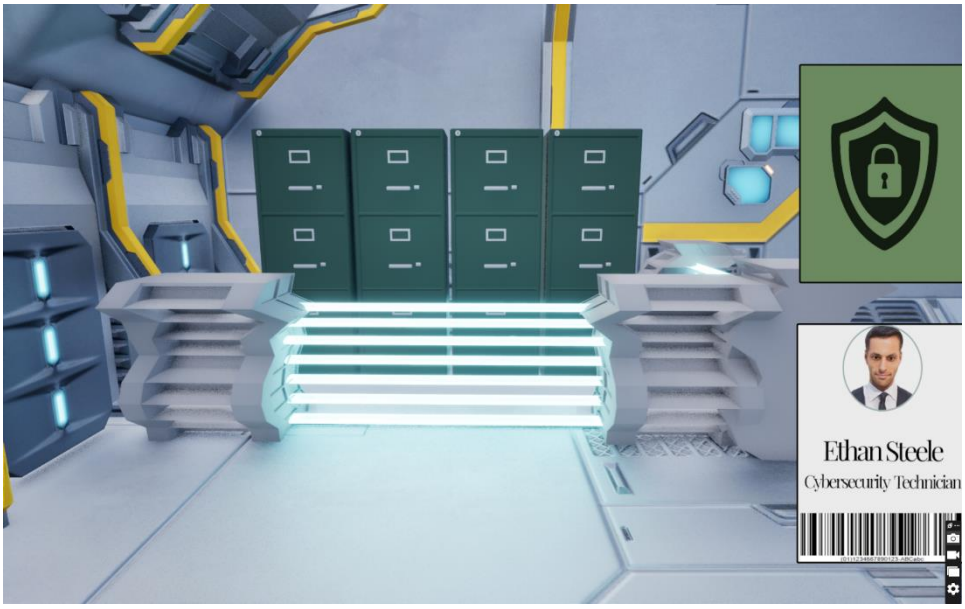

Figure 30 Filing Cabinet in Cargo Bay

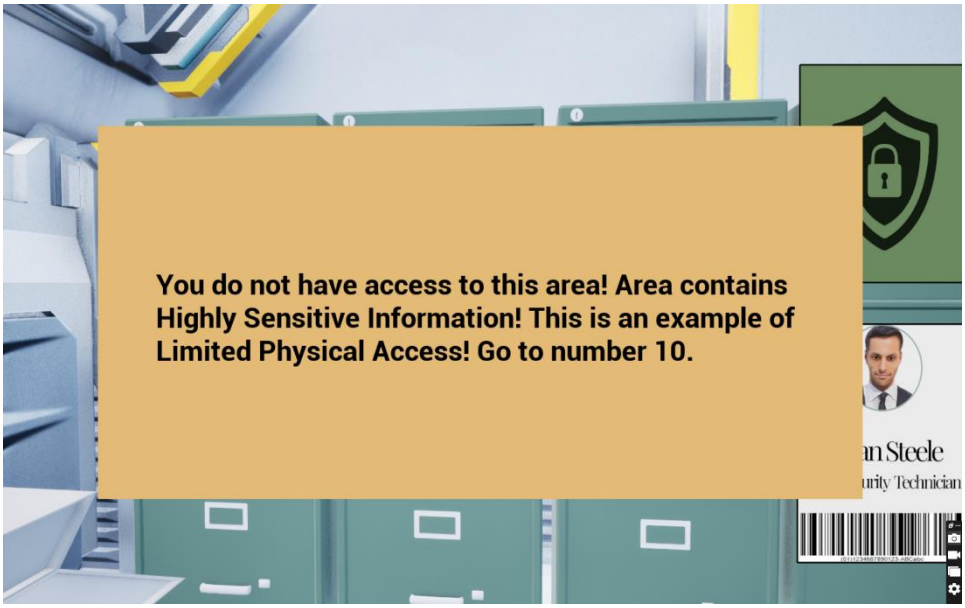

Figure 31 Prompt which appears when the player gets close to filing cabinets

The player proceeds to number 10, where they are introduced to the concept of limited physical access, as illustrated in Figure 32. Upon acknowledging this prompt, the player receives a notification indicating the conclusion of the game, with instructions to press X to exit, as depicted in Figure 33.

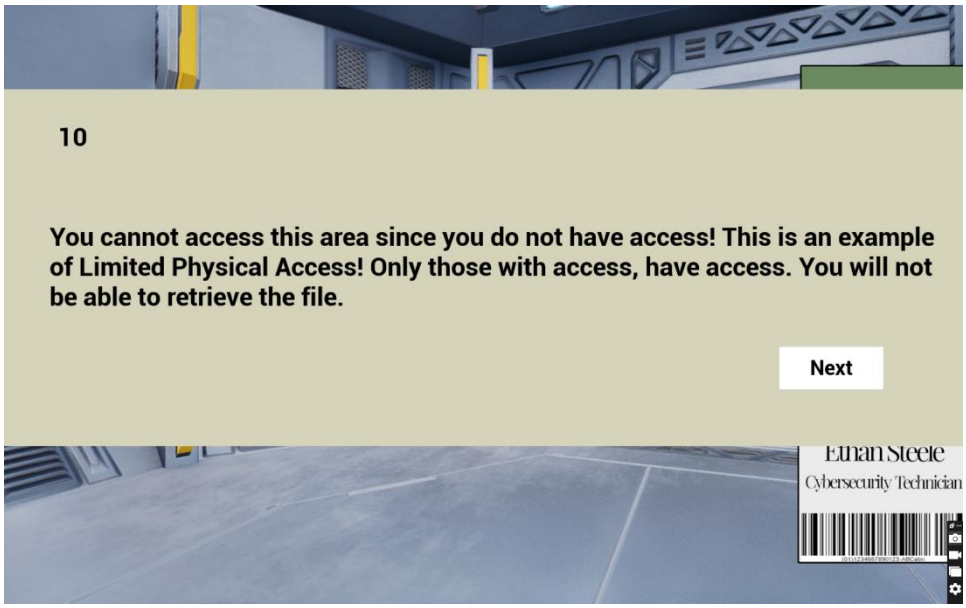

Figure 32 Prompt for Number 10

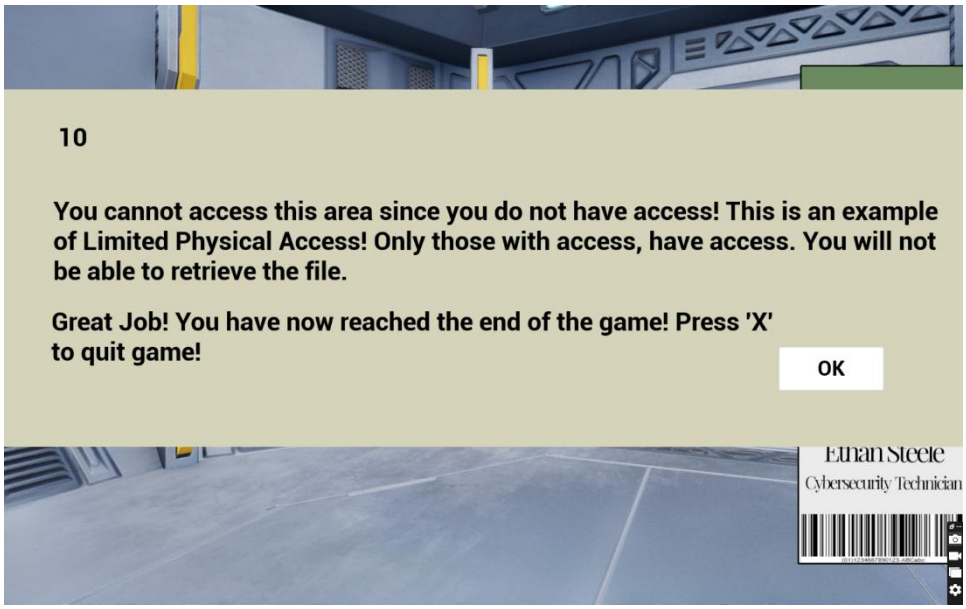

Figure 33 End of Game Prompt

Players have the option to continue exploring the ship at their leisure, collecting any remaining coins or information icons. Figure 34 showcases information regarding authorized access control, obtained from an information icon, while Figure 35 displays details on physical access control from another information icon. Additionally, Figure 36 presents information on identification from yet another collected information icon.

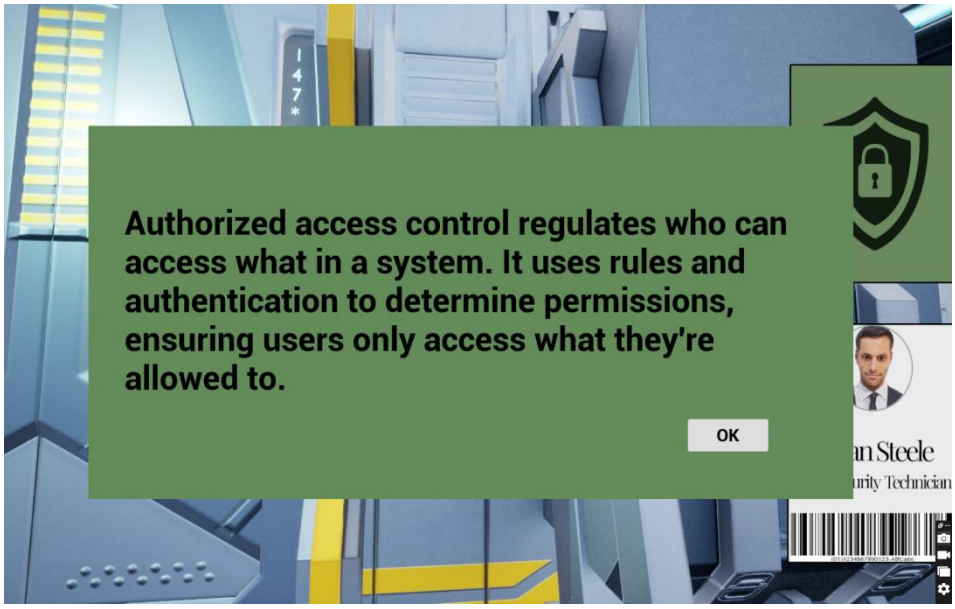

Figure 34 Authorized Access Control Information

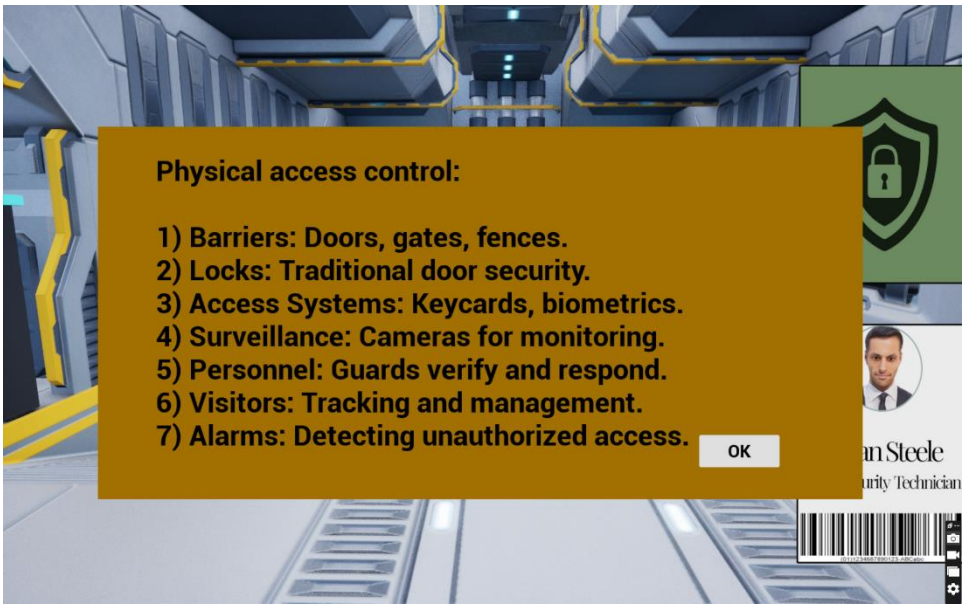

Figure 35 Physical Access Control Information

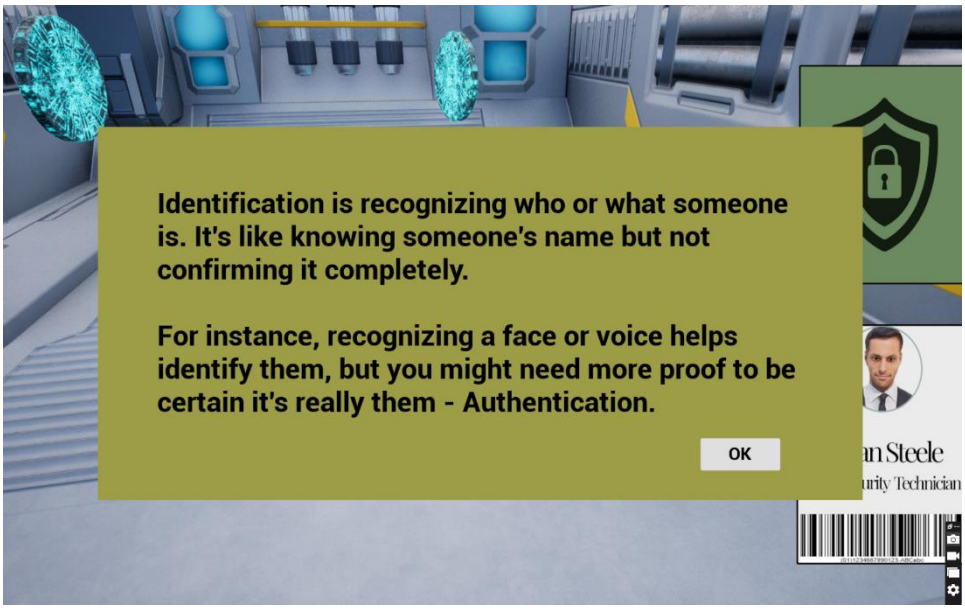

Figure 36 Identification Information

Figures 37 to 39 offer insights into various cybersecurity facts. Once all collectibles have been gathered, the environment is depicted in Figure 40.

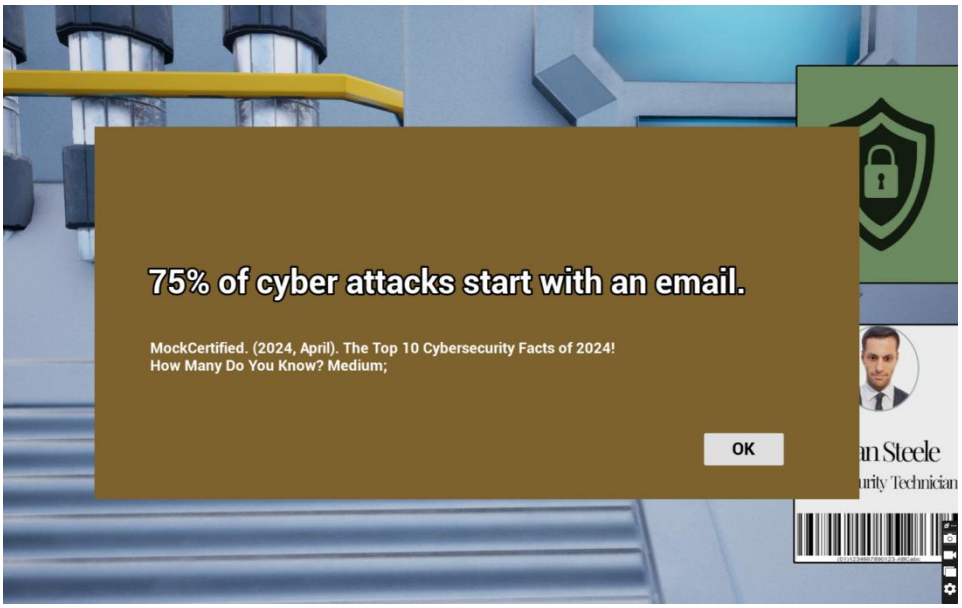

Figure 37 Fact About Cyber Attacks

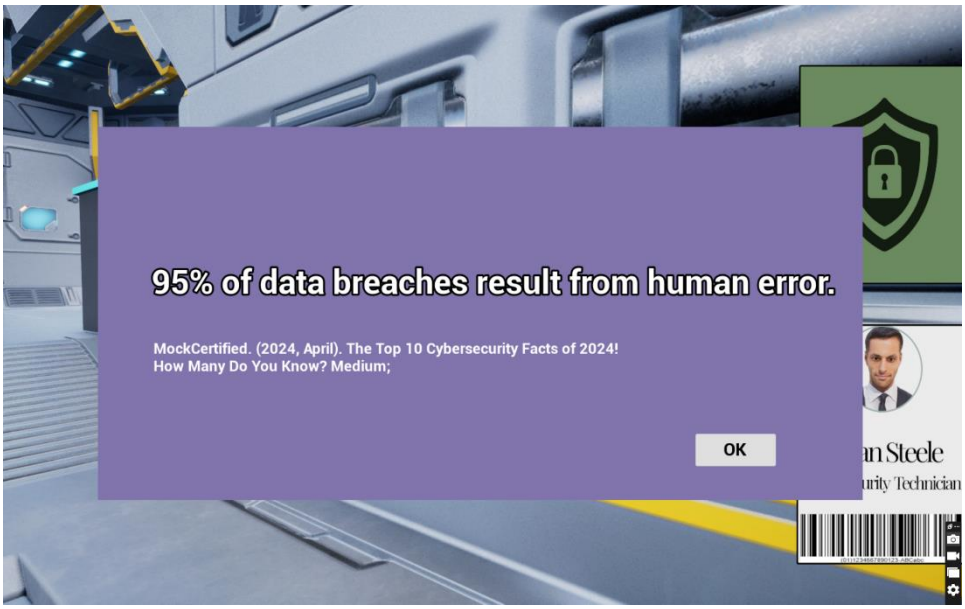

Figure 38 Data Breach Fact

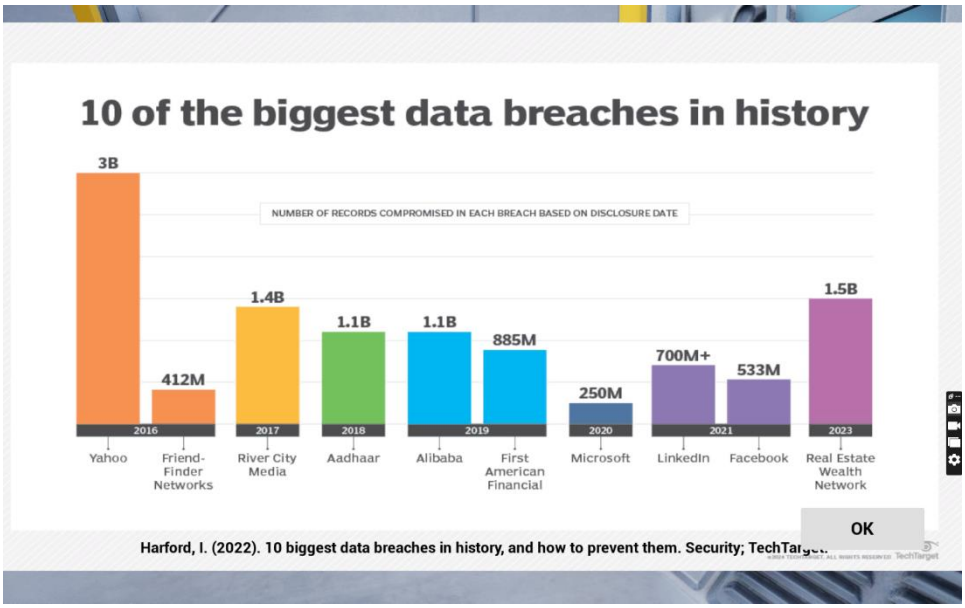

Figure 39 Breach Fact

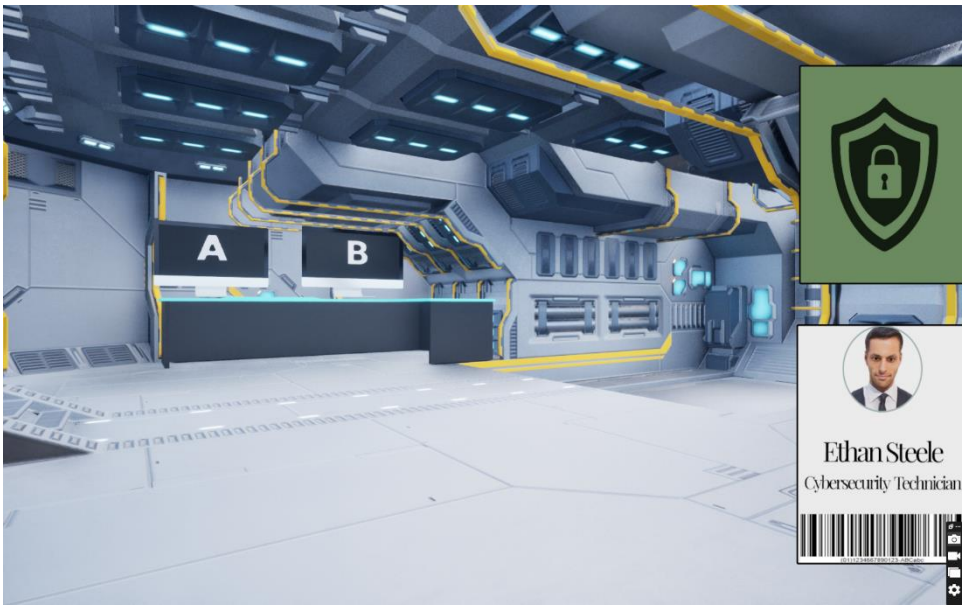

Figure 40 In-Game Environment After Collecting All the Objects

Figure 41 exhibits the exterior of the spaceship with a space skybox illuminated by lit lighting. Despite the vibrancy of the space skybox under unlit lighting, as shown in Figure 42, this option was not feasible due to its adverse impact on the spaceship's appearance. Hence, lit lighting was selected to maintain the spaceship's visual integrity.

Figure 41 Exterior of Spaceship with Space Skybox Lit

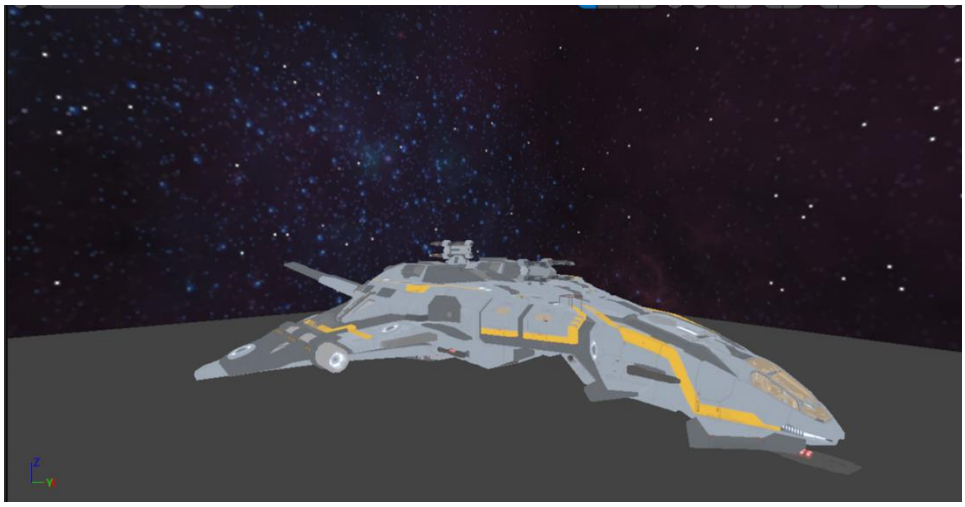

Figure 42 Exterior of Spaceship with Space Skybox Unlit

4.4 Pilot Testing and Iterative Refinement

During the pilot testing phase, the evaluation was somewhat limited due to time constraints and technical issues such as Unreal crashes and packaging errors. Testing primarily occurred on the development device. Two testers, aged between 25 and 30, possessing some cybersecurity knowledge, provided feedback. Overall, the feedback was positive, highlighting the intuitiveness of the CMMC controls and the enjoyment derived from the scenarios presented.

However, the feedback emphasized a desire for a task or reward system to enhance motivation and engagement. While this aspect was considered during development, the prioritization of simplicity due to time and skill limitations took precedence. Nonetheless, the suggestion of implementing a reward system for future iterations was well received.

Participants found the inclusion of coins displaying cybersecurity facts intriguing and informative, with some revelations being particularly surprising. Additionally, testers expressed a preference for the interactive nature of the game over traditional manual-based learning methods.

Suggestions for future improvements included making computer screens interactable, which was postponed due to constraints in experience and time. Despite these limitations, the positive reception and constructive feedback underscore the potential for further refinement and enhancement of the gamified CMMC training experience.

CHAPTER 5: CONCLUSIONS AND FUTURE WORK

This chapter concludes the study by summarizing its findings and suggesting future research directions. It outlines the significance of the research outcomes and offers insights into potential areas for further exploration and innovation in the field.

5.1 Summary of Findings

The study's primary findings emphasize the effectiveness of gamification in enhancing engagement and improving information retention. Through gamified methodologies, participants exhibited heightened motivation and enthusiasm, resulting in a more memorable learning experience compared to traditional manual-based approaches. Notably, the prevailing CMMC training methods rely on conventional practices such as classes or textual resources, suggesting the potential for gamification to revolutionize this conventional paradigm.

Furthermore, the research highlights the adaptability of gamification in accommodating diverse scenarios and effectively conveying intricate concepts. By contextualizing information within interactive and relatable scenarios, participants found it easier to grasp complex concepts that might otherwise be obscured by technical jargon. This approach not only fosters deeper understanding but also bridges the gap between theoretical knowledge and practical applications.

Additionally, the findings suggest that conventional learning methods, such as reading dense materials filled with technical terminology, may present challenges for learners unfamiliar with the subject matter. Gamification offers a viable solution by presenting information in a more accessible and engaging format, thereby reducing barriers to comprehension, and facilitating knowledge acquisition.

The study underscores the transformative potential of gamification in educational settings, particularly in the domain of CMMC training. By leveraging gamified strategies, training programs can optimize engagement, enhance learning outcomes, and establish connections between theory and practice in cybersecurity education.

5.2 Implications of CMMC Compliance and Training

In considering the broader implications of the study for CMMC compliance and training practices, several key points emerge. Firstly, the findings shed light on the potential for gamified approaches to revolutionize traditional training methods within the realm of CMMC compliance. By demonstrating the effectiveness of gamification in enhancing engagement and improving information retention, the study suggests that integrating gamified elements into CMMC training programs could lead to more effective and enjoyable learning experiences for participants.

Moreover, the study's insights highlight the importance of adapting training methodologies to suit the evolving needs and preferences of modern learners. As the cybersecurity landscape evolves rapidly, training practices must keep pace with these changes. Gamification offers a dynamic and flexible approach to training that can be tailored to address the specific challenges and requirements of CMMC compliance.

Additionally, the study underscores the significance of bridging the gap between theoretical knowledge and practical application within CMMC training. By contextualizing information within interactive and relatable scenarios, gamified training programs can help learners better understand how CMMC principles apply in real-world situations. This not only enhances comprehension but also fosters a deeper appreciation for the relevance and importance of CMMC compliance in safeguarding organizational assets and data.

Overall, the study's implications suggest that embracing gamification within CMMC compliance and training practices holds great promise for improving learning outcomes, increasing engagement, and enhancing cybersecurity resilience within

organizations. By leveraging gamified approaches, organizations can cultivate a culture of cybersecurity awareness and empower employees to effectively navigate the complexities of CMMC compliance.

5.3 Limitations of the Study

Acknowledging the constraints and limitations encountered during the research is crucial for providing a comprehensive understanding of the study's scope and implications. Several limitations warrant acknowledgment in this regard.

Firstly, the study's sample size may have been restrictive, potentially limiting the generalizability of the findings. With only a limited number of participants, the study's ability to capture the full spectrum of perspectives and experiences related to CMMC compliance and training practices may have been constrained.

Additionally, the research was conducted within a specific context and timeframe, which may have influenced the outcomes and conclusions drawn. Factors such as the chosen methodology, the duration of the study, and the availability of resources could have impacted the breadth and depth of the investigation.

Furthermore, the study may have been subject to inherent biases, both from the researchers and the participants. Biases could have influenced participant responses, the interpretation of data, and the conclusions drawn from the findings. Efforts were made to mitigate biases through rigorous research design and data analysis procedures; however, it is important to acknowledge the potential influence of biases on the study's outcomes.

Moreover, the lack of game development skills and prior experience with Unreal Engine presented significant challenges throughout the research process. The complexity

of the Unreal Engine interface, coupled with the lack of beginner-friendly resources, posed obstacles to the development and implementation of the gamified training program. These limitations may have impacted the quality of the final product and the effectiveness of the training approach.

Lastly, external factors such as technological limitations, time constraints, and unforeseen circumstances may have affected the research process and outcomes. For example, technical issues such as Unreal crashes and packaging errors encountered during pilot testing hindered the evaluation process and may have impacted the reliability of the results.

In conclusion, while the study offers valuable insights into the implications of gamified approaches for CMMC compliance and training practices, it is essential to recognize the limitations inherent in the research process. By acknowledging these constraints, future studies can build upon this foundation and strive for greater robustness and comprehensiveness in their investigations.

5.4 Recommendations for Future Research

In considering future research directions, several avenues present themselves for further exploration and development, building upon the findings of the current study. One promising direction is the expansion of the gamified training program to encompass additional levels, such as Level 2 and Level 3 CMMC requirements. By extending the training program to cover higher levels of CMMC compliance, researchers can assess the effectiveness of gamification in addressing more complex cybersecurity challenges and preparing organizations for advanced certification levels.

Furthermore, leveraging the capabilities of Unreal Engine offers an opportunity to enhance the scope and scale of the gamified training program. With Unreal Engine's advanced features and flexible development tools, researchers can create a more immersive and interactive learning experience. This could involve incorporating dynamic simulations, realistic scenarios, and enhanced visual effects to simulate real-world cybersecurity threats and challenges more accurately.

Moreover, future research could explore the integration of emerging technologies such as virtual reality (VR) and augmented reality (AR) into the gamified training program. By incorporating VR/AR elements, researchers can create a more immersive and engaging learning environment, allowing participants to interact with cybersecurity concepts in a highly realistic and immersive manner. This could enhance learning outcomes and provide a more intuitive understanding of complex cybersecurity principles.

Also, there is potential to explore gamification's effectiveness in other areas of cybersecurity training beyond CMMC compliance. Research could investigate the application of gamified approaches to other cybersecurity frameworks, such as the NIST Cybersecurity Framework or ISO/IEC 27001, to assess their suitability for different organizational contexts and compliance requirements.

Furthermore, considering the increasing importance of cybersecurity awareness and training across various industries, future research could focus on developing customized gamified training programs tailored to specific sectors or organizational needs. By aligning training content with industry-specific challenges and regulatory

requirements, researchers can optimize the relevance and effectiveness of gamified cybersecurity training initiatives.

Exploring future research directions, potential avenues include expanding the gamified training program to higher CMMC levels, leveraging Unreal Engine for enhanced development capabilities, exploring VR/AR integration, investigating gamification in other cybersecurity frameworks, and developing sector-specific training programs. By pursuing these avenues, researchers can advance knowledge and practice in gamified cybersecurity training, enhancing organizational resilience against evolving cyber threats.

5.5 Qualitative Analysis

In the qualitative analysis section, feedback from all participants, including those who did not complete the entire game, was examined to gauge the effectiveness of the interactive cybersecurity game. Participants' feedback highlighted key themes, such as the game's interactive nature and its ability to clarify complex concepts. Additionally, participants recognized its potential value for military training and employee education. This inclusive analysis offers insights into the game's educational impact, complementing the quantitative analysis focused on pre-and post-test results, and enriching our understanding of its effectiveness in cybersecurity education.

5.5.1 Participants / Volunteers

The preliminary assessment involved 10 participants with a majority in their 20s (80%), along with one in their 30s and another aged 50 or older. Figure 43 depicts a pie chart illustrating the age distribution of participants.

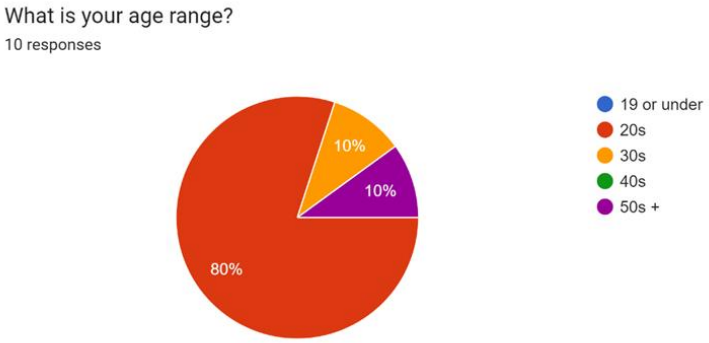

Figure 43 Qualitative Participants Age Pie Chart

Their gaming habits varied: two played video games for less than an hour weekly, three played for over three hours, three played between one to three hours, and two didn't play at all. Figure 44 presents a pie chart displaying the average weekly gaming hours.

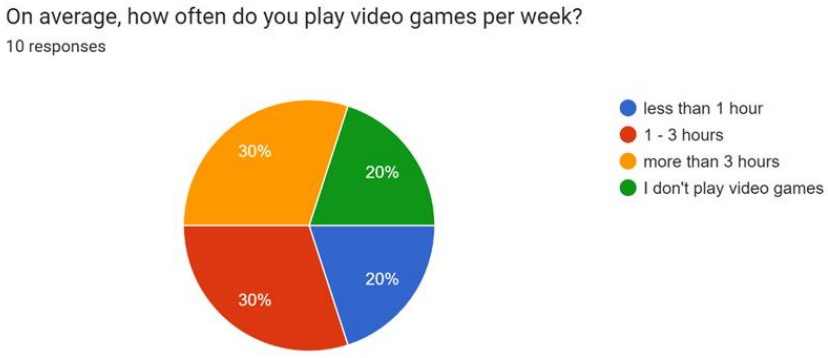

Figure 44 Qualitative Participants Average Video Game Time Per Week Pie Chart

The pre-test evaluated their baseline cybersecurity knowledge before interacting with the educational game. Post-test findings showed differing levels of engagement and understanding among participants. While eight completed both tests, one lost interest due to the game's length, quitting after three minutes. Another struggled initially, quitting after a minute but still completing both tests. Notably, one participant didn't return to finish the post-test despite intending to do so.

5.5.2 Pre – Test

Participants correctly identified "Padlock Key & Dial Combination" and "ATM Card & PIN" as 2FA methods; however, some also selected these correct answers alongside incorrect options. Among the participants, two individuals successfully identified both correct 2FA methods, indicating a 20% accuracy rate. However, the majority of participants, a total of eight, provided mixed responses, combining the correct options with erroneous selections. Common among these incorrect choices were single-factor authentication methods, notably "Password & Security Question" and "Iris Scan & Thumbprint," chosen by seven and five participants, respectively. Additionally, some participants opted for combinations of single-factor authentication methods with other forms, such as "ATM Card & PIN" and "Password & Security Question, Iris Scan & Thumbprint." This highlights a potential misunderstanding or confusion regarding the criteria for two-factor authentication. Thus, while participants demonstrated awareness of some 2FA methods, there remains a need for clarification and reinforcement of concepts to ensure accurate comprehension and application in digital security practices. Figure 45 shows a bar chart containing the results for this question.

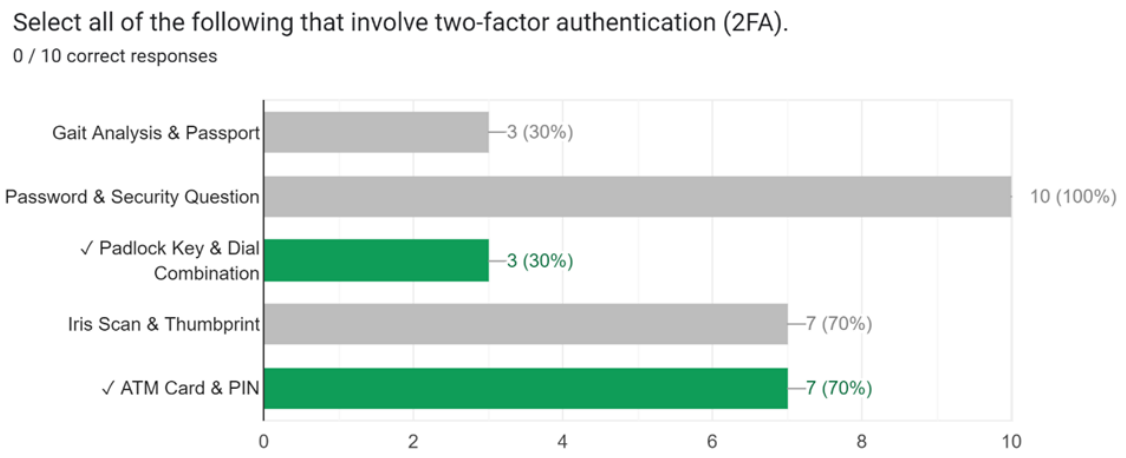

Figure 45 Qualitative Pre-Test Two Factor Authentication Question Bar Chart

In the evaluation of Physical Access Controls, participants were presented with various options and instructed to select those considered as such. The correct answers were identified as "Keycards," "Biometric Scanners (fingerprint, iris, facial recognition)," and "Vehicle Barriers." Findings indicate that nine participants accurately selected all three correct options, yielding a 90% accuracy rate. Conversely, one participant provided an incorrect response. Among the incorrect selections, some participants chose options that did not align with Physical Access Controls, such as "Web Application Firewalls (WAFs)," "Antivirus Software," and "Virtual Private Networks (VPNs)," which are typically associated with network security rather than physical access management. This highlights the need for further clarification and reinforcement of concepts related to Physical Access Controls to ensure accurate understanding and application in security protocols. Figure 46 shows a bar chart showing the results for this question.

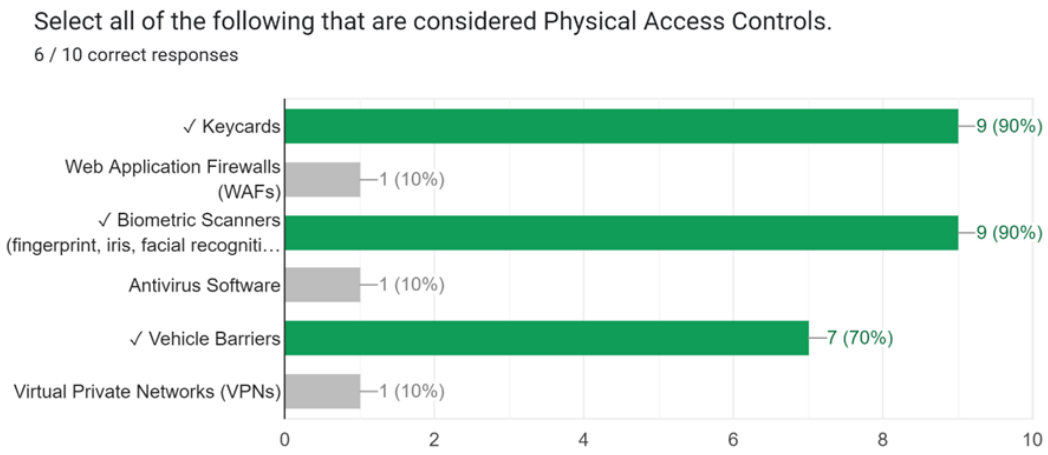

Figure 46 Qualitative Pre-Test Physical Access Question Bar Chart

In the assessment of the distinction between Identification and Authentication, participants were asked to identify the primary function of Identification compared to Authentication. The correct answer was determined to be "Identification confirms user identity, while Authentication grants access." Findings reveal that all ten participants accurately selected this response, resulting in a 100% accuracy rate. This indicates a high level of understanding among participants regarding the roles of Identification and Authentication in the context of user access control. Consequently, participants demonstrated a clear comprehension of the fundamental differences between the two concepts, with Identification primarily serving to verify user identity and Authentication facilitating access based on that verified identity. Figure 47 shows a bar chart with the results for this question.

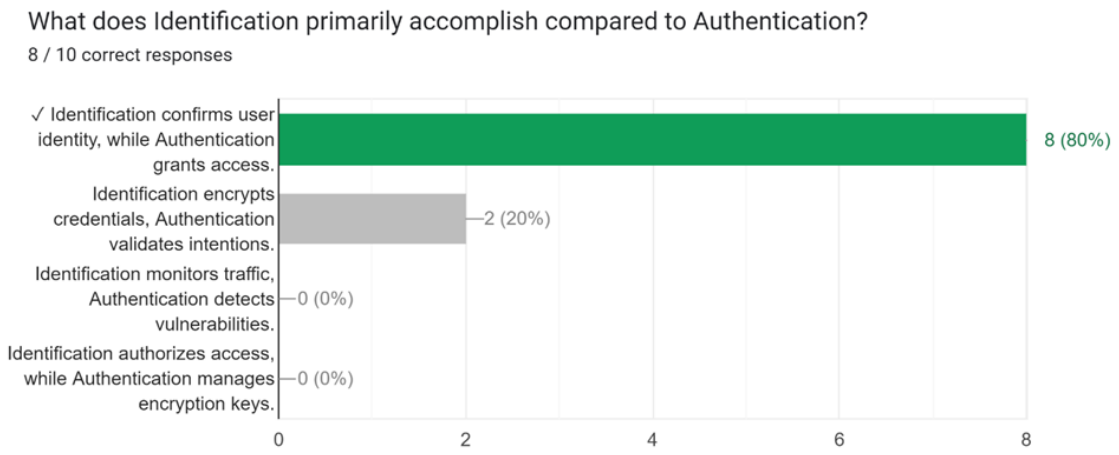

Figure 47 Qualitative Pre-Test Authentication Question Bar Chart

In the evaluation of the primary attack vector according to "MockCertified," participants were asked to identify the leading cause of cyber attacks. The correct answer was determined to be "Email." Findings indicate that two participants accurately selected this response, resulting in a 20% accuracy rate. However, the majority of participants, eight out of ten, provided incorrect answers. Among the incorrect selections, "Weak Passwords" was the most chosen option, selected by six participants. Additionally, two participants chose “Unsecured Wi-Fi.” These results suggest a potential misconception regarding the prevalent attack vectors in cybersecurity, emphasizing the importance of accurate knowledge and awareness of common cyber threats. Further education and training may be necessary to enhance participants' understanding of cyber attack vectors and their mitigation strategies. Figure 48 shows a bar chart with the results for this question.

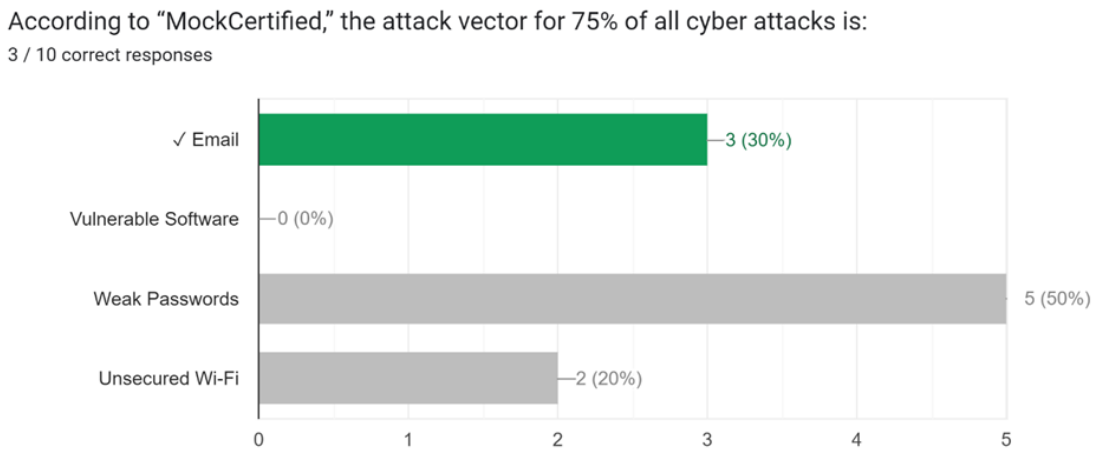

Figure 48 Qualitative Pre-Test Attack Vector Question Bar Chart

5.5.3 Post – Test

In the assessment of the navigational ease of the game, participants were asked to evaluate its user-friendliness. The majority of participants, six out of eight, described the game as "Easy" to navigate. This indicates a positive perception of the game's usability among the majority of participants, suggesting that it offered intuitive controls and clear instructions. Conversely, two participants found the game to be "Difficult" to navigate, suggesting potential areas for improvement in terms of user interface design or instructional clarity. These findings highlight the importance of considering user feedback in the refinement and enhancement of gaming experiences to ensure optimal usability and player satisfaction. Figure 49 shows these results.

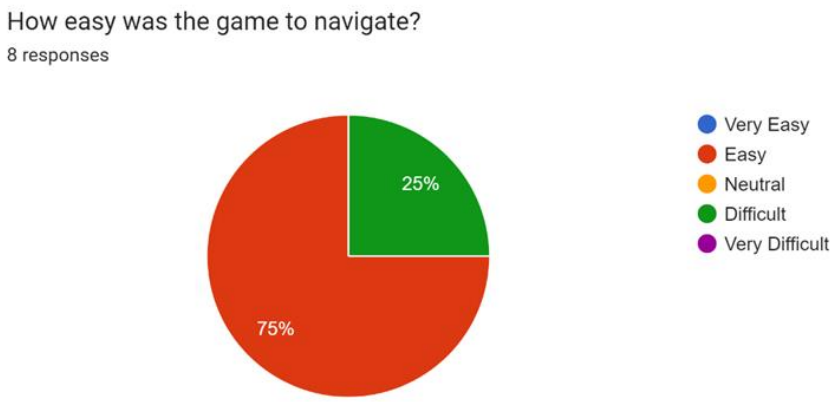

Figure 49 Qualitative Post-Test Game Navigation Pie Chart Results

In the evaluation of examples of two-factor authentication (2FA), participants were presented with various scenarios and asked to identify the one that exemplifies 2FA. The correct answer was determined to be "A home safe that requires a dial combination and a thumbprint to open." Findings reveal that one participant accurately selected this response, resulting in a 10% accuracy rate. However, the majority of participants, nine out of ten, provided incorrect answers. Among the incorrect selections, scenarios involving single-factor authentication methods were commonly chosen, such as "A bank vault that requires both a fingerprint and a retina scan" and "A door with a display screen that requires a PIN and then selection of a secret image." These results suggest a potential misunderstanding or lack of clarity regarding the concept of two-factor authentication. Further education and clarification may be necessary to ensure accurate comprehension and application of 2FA principles. Figure 50 shows a bar chart containing the results for this question.

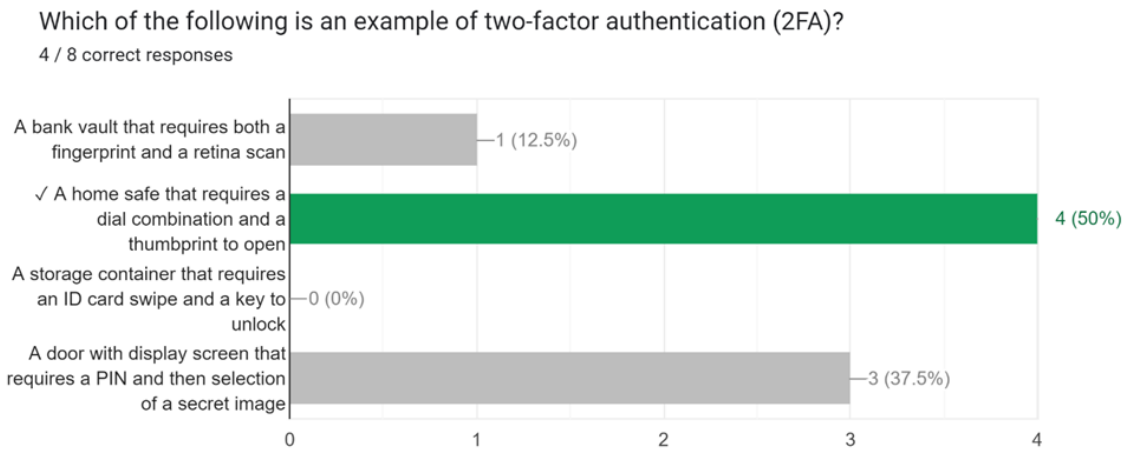

Figure 50 Qualitative Post-Test 2FA Question Bar Chart Results

In the assessment of Physical Access Controls, participants were presented with various options and instructed to select those considered as such. The correct answers were identified as "Keycard Reader" and "Video Surveillance Cameras." Findings reveal that three participants accurately selected both correct options, resulting in a 30% accuracy rate. However, the majority of participants, seven out of ten, provided mixed responses, including options that did not align with Physical Access Controls. These incorrect selections commonly included components associated with network security or data protection, such as "Endpoint Detection and Response (EDR)" and "Data Encryption." This suggests a potential misunderstanding of the criteria for Physical Access Controls among some participants. Therefore, further clarification and reinforcement of concepts related to access control mechanisms may be necessary to ensure accurate understanding and application in security protocols. Figure 51 shows a bar chart with the results for this question.

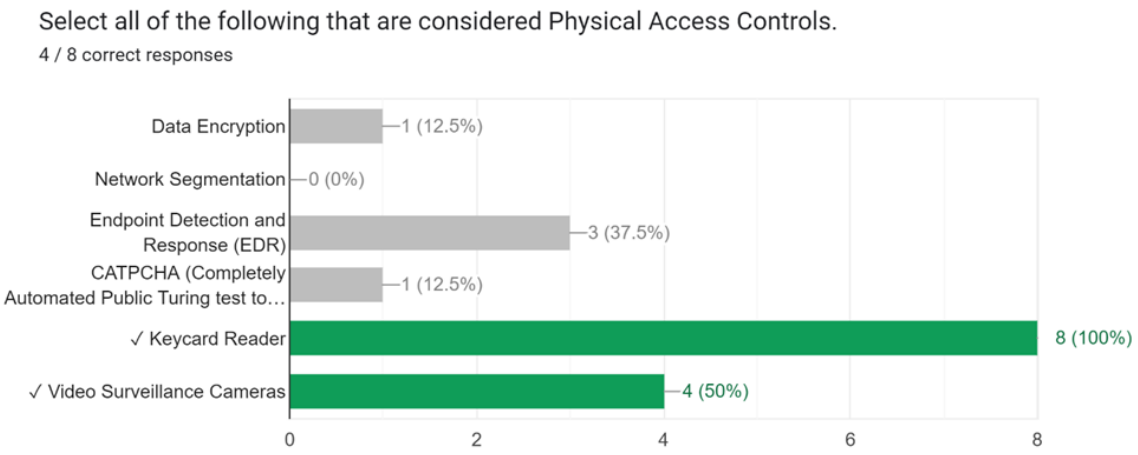

Figure 51 Qualitative Post-Test Physical Access Question Bar Chart Results

In the evaluation of the distinction between Authentication and Identification, participants were asked to identify how these concepts differ. The correct answer was determined to be "Authentication confirms, identification assigns." Findings indicate that one participant accurately selected this response, resulting in a 10% accuracy rate. However, the majority of participants, nine out of ten, provided incorrect answers. Among the incorrect selections, options commonly included statements that did not accurately differentiate between Authentication and Identification. For instance, "Authentication assigns roles, whereas identification verifies" was chosen by three participants, and "Authentication labels, while identification proves" was chosen by one participant. These results suggest a potential misunderstanding or lack of clarity regarding the distinction between Authentication and Identification among some participants. Therefore, further education and clarification may be necessary to ensure accurate comprehension and application of these fundamental concepts in security protocols. Figure 52 shows a bar chart containing the results of this question.

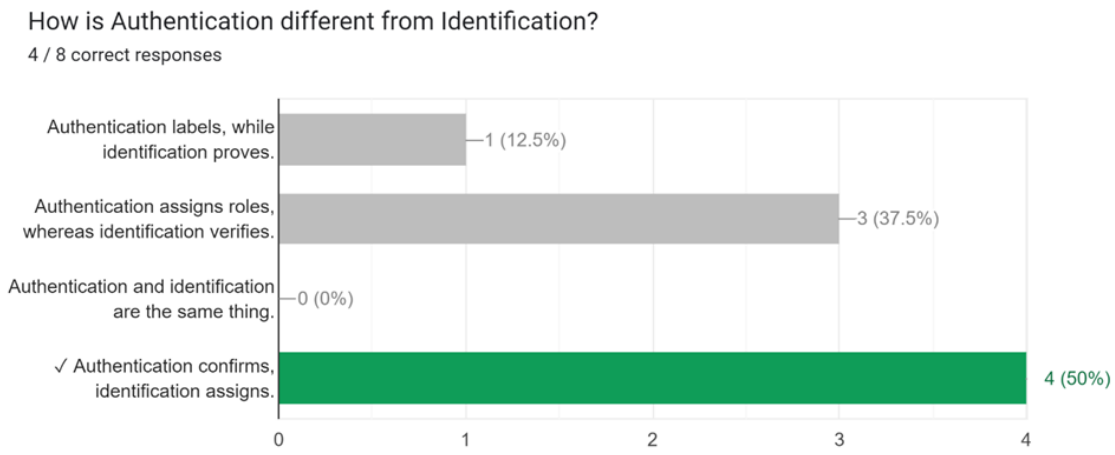

Figure 52 Qualitative Post-Test Authentication Question Bar Chart Results

In the assessment of the primary attack vector according to “MockCertified,” participants were tasked with identifying the leading cause of cyber attacks. The correct answer was determined to be "Email." Findings reveal that six participants accurately selected this response, resulting in a 60% accuracy rate. However, a considerable number of participants, four out of eight, provided incorrect responses. Among the incorrect selections, "Weak Passwords" was the most common choice, selected by two participants. Additionally, one participant each chose "Unsecured Wi-Fi" and "Email." These results suggest a potential misconception or lack of awareness regarding prevalent cyber attack vectors among some participants. Therefore, further education and reinforcement of cybersecurity concepts may be necessary to enhance participants' understanding of common cyber threats and mitigation strategies. Figure 53 shows a bar chart containing the results for this question.

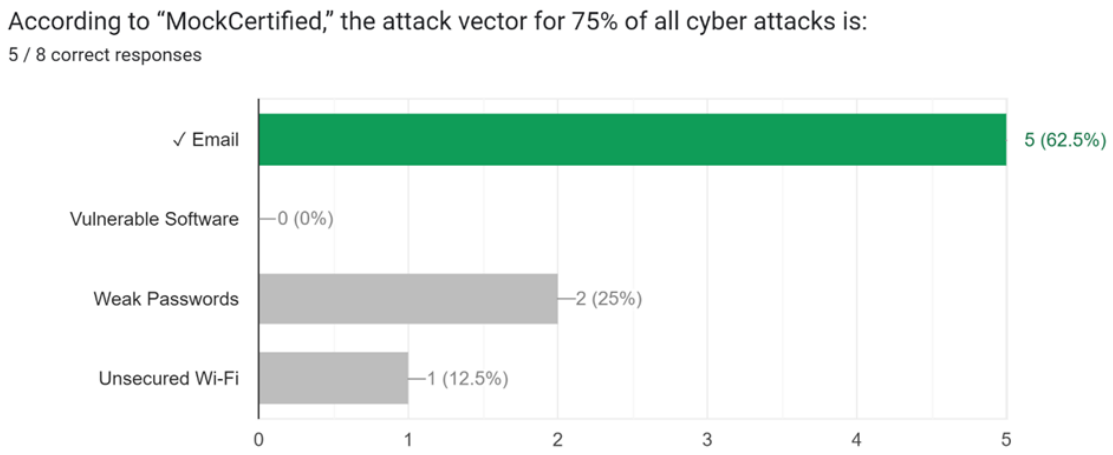

Figure 53 Qualitative Post-Test Vector Attack Question Bar Chart Results

In the feedback provided regarding the interactive cybersecurity game, participants shared insightful observations and positive remarks about their experience. One participant noted a brief challenge with navigating the doors initially but eventually found a solution, suggesting potential usability enhancements. Despite this, they found the game to be informative and enjoyable, appreciating its interactive approach to learning about cybersecurity. Another participant echoed these sentiments, praising the game's engaging and informative nature. Additionally, there were comments from individuals who did not participate directly in the game but recognized its potential value for military training and employee education. These remarks highlight the perceived effectiveness and versatility of the game as a tool for teaching cybersecurity concepts in various contexts. Overall, the feedback indicates a positive reception of the game, emphasizing its educational value and engaging design. Figure 54 shows a few of these comments.

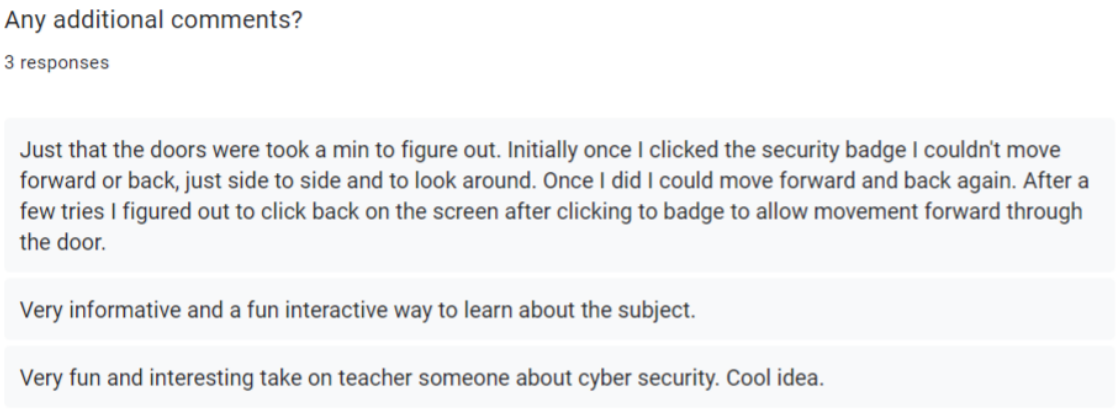

Figure 54 Qualitative Post-Test Additional Comments

5.5.4 Qualitative Findings

Comparing the pre-test and post-test results provides valuable insights into the effectiveness of the interactive cybersecurity game in enhancing participants' knowledge and comprehension. In the pre-test, participants displayed varying levels of proficiency across different questions. For instance, while all participants correctly identified the primary function of Identification compared to Authentication, only a minority accurately recognized examples of two-factor authentication and physical access controls. Specifically, in the pre-test question regarding two-factor authentication, only two participants out of ten identified both correct examples, resulting in a 20% accuracy rate. Similarly, in the question about physical access controls, only one participant out of ten accurately selected all three correct options, yielding a 10% accuracy rate.

Following engagement with the educational game, there were noticeable improvements in participants' knowledge and understanding, as reflected in the post-test results. For example, in the post-test question on two-factor authentication, there was a slight increase in the accuracy rate, with one additional participant accurately identifying

the correct example compared to the pre-test. Similarly, in the question about physical access controls, there was a significant improvement, with three participants out of eight accurately selecting all correct options, resulting in a 30% accuracy rate. These improvements suggest that the interactive game effectively reinforced participants' understanding of these concepts.

Additionally, while there were still areas for improvement, such as the question about the primary attack vector for cyber attacks, where the majority of participants provided incorrect responses in both the pre-test and post-test, there were indications of enhanced comprehension. In the post-test, there was a slightly higher proportion of participants selecting the correct option compared to the pre-test, indicating a potential positive impact of the game on their awareness of common cyber threats.

Furthermore, participants' feedback highlighted the positive impact of the game on their learning experience. They appreciated the interactive and engaging nature of the game, noting that it facilitated their understanding of complex cybersecurity concepts. For example, one participant mentioned that the game helped clarify navigation challenges they initially encountered, leading to a better understanding of the content. Another participant praised the game's effectiveness as a tool for teaching cybersecurity in various settings, such as military training and employee education.

Overall, while further refinement and improvement may be necessary in certain areas, the post-test results, along with participant feedback, suggest that the interactive cybersecurity game had a positive impact on participants' knowledge and comprehension. It effectively reinforced key concepts and facilitated a more engaging and enjoyable

learning experience.

5.6 Quantitative Analysis

In the quantitative analysis section, the focus was on participants who completed both the pre-and post-tests, providing a rigorous examination of the game's impact on knowledge acquisition. By exclusively considering this subset of participants, the analysis ensures a clear and focused assessment of the game's effectiveness in improving understanding of cybersecurity concepts. Through statistical comparisons of pre-and post-test results, insights were gained into the extent of knowledge enhancement attributable to the interactive game. This targeted approach allowed for a precise evaluation of the game's educational efficacy, providing valuable quantitative evidence to support its effectiveness in cybersecurity education.

5.6.1 Participants

In the quantitative analysis, a subset of participants who completed both the pre-test and post-test, and played the game in its entirety, provided a focused evaluation of the game's effectiveness in teaching cybersecurity concepts. Among these participants, six were in their twenties, while one was in their thirties. Additionally, the distribution of participants' gaming habits revealed varying levels of engagement with video games: two participants reported playing less than one hour per week, while two others played more than three hours weekly. One participant did not engage in video gaming at all, while the remaining two played between one to three hours per week. These demographic details offer context to the quantitative analysis, providing insight into the diverse backgrounds

and gaming behaviors of participants, and enhancing the interpretation of the results regarding the game's educational impact.

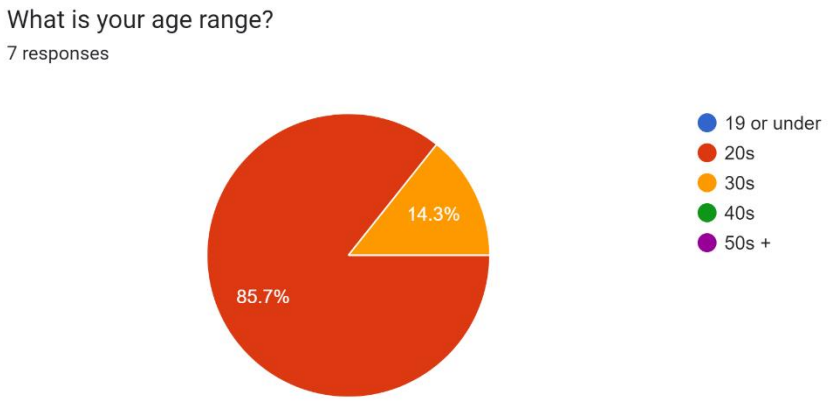

Figure 55 Quantitative Age Range Pie Chart

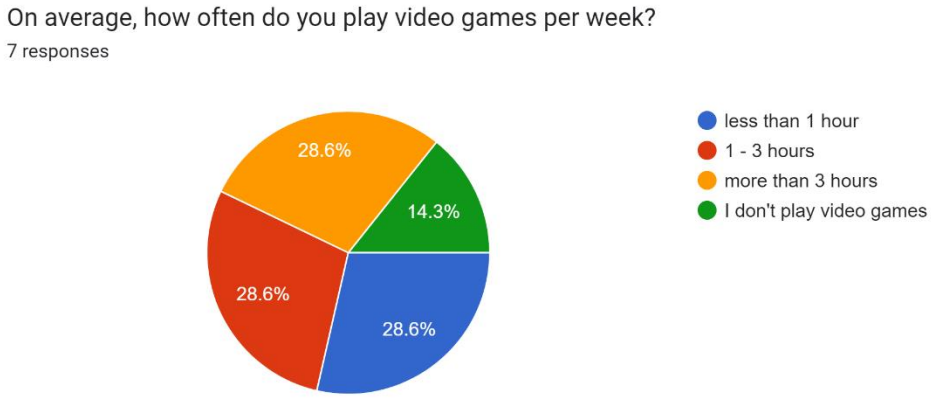

Figure 56 Quantitative Hours played per week

5.6.2 Pre – Test

In the quantitative analysis of participants' understanding of two-factor authentication (2FA), the correct answers were identified as "Padlock Key & Dial Combination" and "ATM Card & PIN." However, it was noted that some participants selected these correct options alongside incorrect ones. Among the participants, two individuals accurately identified both correct 2FA methods, indicating a 20% accuracy rate. However, the majority of participants, a total of eight, provided mixed responses, combining the correct options with erroneous selections. Common among these incorrect choices were single-factor authentication methods, notably "Password & Security Question" and "Iris Scan & Thumbprint," chosen by seven and five participants, respectively. Additionally, some participants opted for combinations of single-factor authentication methods with other forms, such as "ATM Card & PIN" and "Password & Security Question, Iris Scan & Thumbprint." This suggests a potential misunderstanding or confusion regarding the criteria for two-factor authentication, emphasizing the need for further clarification and reinforcement of concepts to ensure accurate comprehension and application in digital security practices. Figure 57 shows the results for this question.

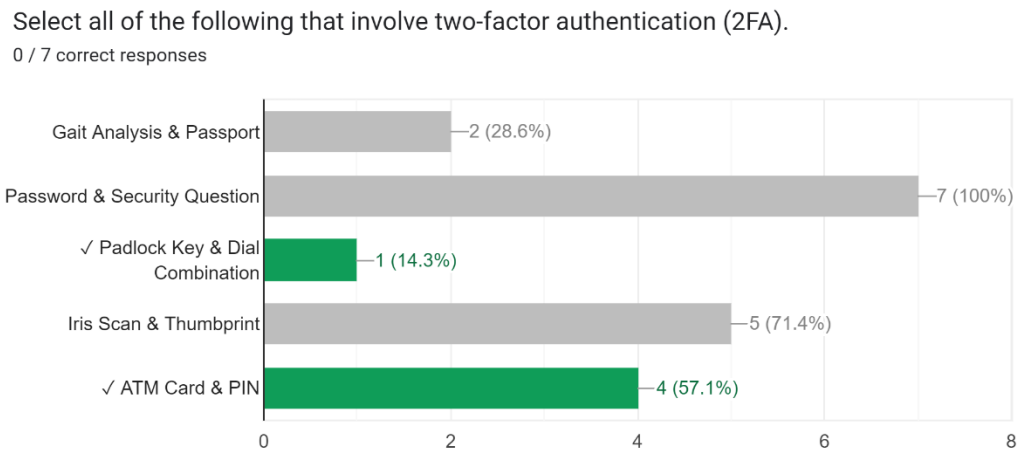

Figure 57 Quantitative Pre-Test 2FA Question Bar Chart Results

In the quantitative analysis of participants' comprehension of physical access controls, the correct answers were identified as "Keycards," "Biometric Scanners (fingerprint, iris, facial recognition)," and "Vehicle Barriers." Findings indicate that three participants accurately selected all three correct options, resulting in a 30% accuracy rate. However, the majority of participants, seven out of ten, provided mixed responses, including options that did not align with Physical Access Controls. These incorrect selections commonly included components associated with network security or data protection, such as "Web Application Firewalls (WAFs)," "Antivirus Software," and "Virtual Private Networks (VPNs)." This suggests a potential misunderstanding of the criteria for Physical Access Controls among some participants. Therefore, further clarification and reinforcement of concepts related to access control mechanisms may be necessary to ensure accurate understanding and application in security protocols. Figure

58 shows the results for this question.

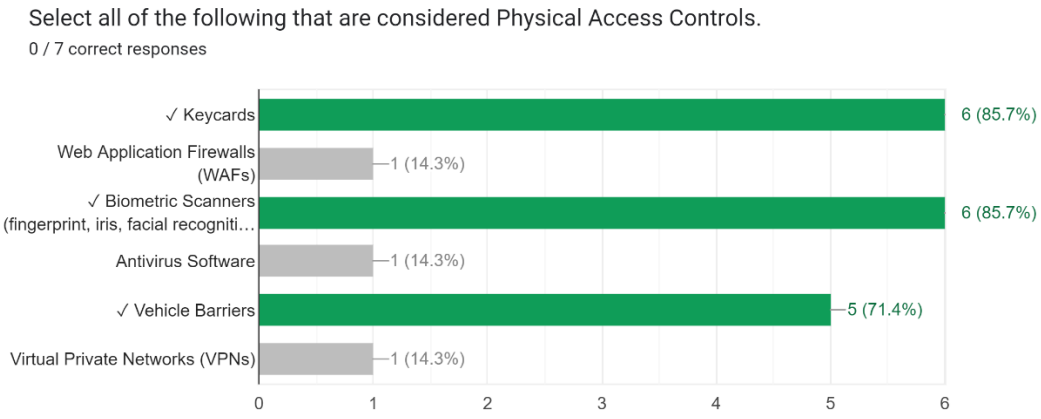

Figure 58 Quantitative Pre-Test Physical Access Controls Question

In the quantitative analysis of participants' understanding of the distinction between Identification and Authentication, the correct answer was determined to be "Identification confirms user identity, while Authentication grants access." Findings reveal that all ten participants accurately selected this response, resulting in a 100% accuracy rate. This indicates a high level of understanding among participants regarding the roles of Identification and Authentication in the context of user access control. Consequently, participants demonstrated a clear comprehension of the fundamental differences between the two concepts, with Identification primarily serving to verify user identity and Authentication facilitating access based on that verified identity. These results suggest a strong grasp of the concepts among the participants, highlighting their proficiency in understanding user access control mechanisms in cybersecurity. Figure 59 shows these results.

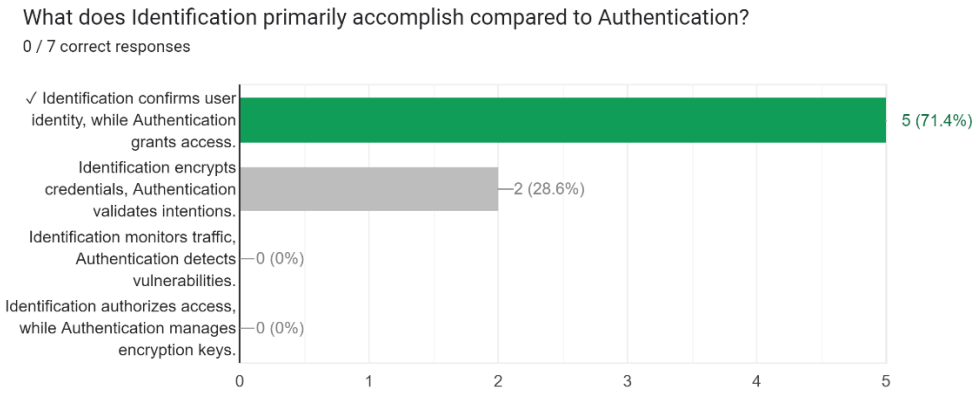

Figure 59 Quantitative Pre-Test Identification Question

In the quantitative analysis of participants' knowledge of prevalent cyber attack vectors, the correct answer was determined to be "Email," as reported by "MockCertified." Findings reveal that six participants accurately selected this response, resulting in a 60% accuracy rate. However, a considerable number of participants, four out of eight, provided incorrect responses. Among the incorrect selections, "Weak Passwords" was the most common choice, selected by two participants. Additionally, one participant each chose "Unsecured Wi-Fi" and "Email." These results suggest a potential misconception or lack of awareness regarding prevalent cyber attack vectors among some participants. Therefore, further education and reinforcement of cybersecurity concepts may be necessary to enhance participants' understanding of common cyber threats and mitigation strategies. Figure 60 shows these results.

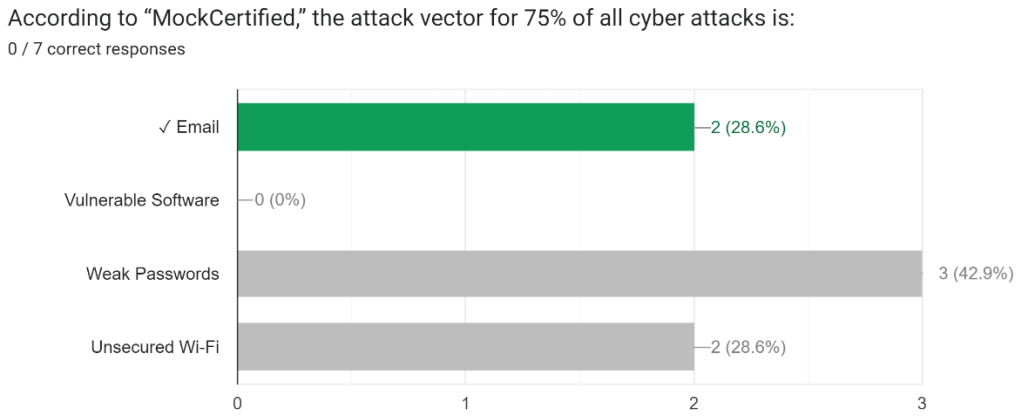

Figure 60 Quantitative Pre-Test Attack Vector Question

5.6.3 Post – Test

In the quantitative analysis of participants' feedback on the navigational ease of the game, the majority, comprising six out of seven participants, reported finding the game "Easy" to navigate. This positive feedback suggests that the game's interface and controls were intuitive and user-friendly for most participants. However, one participant found the game to be "Difficult" to navigate, indicating potential areas for improvement in terms of user interface design or instructional clarity. Despite this, the overall feedback indicates a positive reception of the game's navigational aspects by the majority of participants. Figure 61 shows these results.

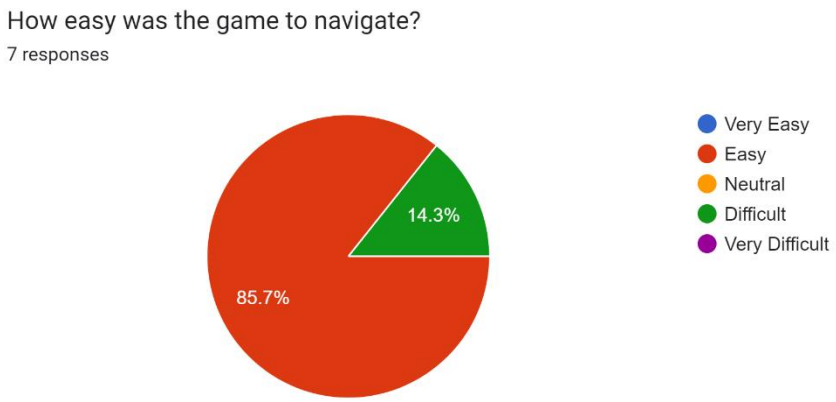

Figure 61 Quantitative Post-Test Navigation Results

In the quantitative analysis of participants' understanding of two-factor authentication (2FA), the correct example was identified as "A home safe that requires a dial combination and a thumbprint to open." Findings reveal that one participant accurately selected this response, resulting in a 10% accuracy rate. However, the majority of participants, nine out of ten, provided incorrect answers. Among the incorrect selections, scenarios involving single-factor authentication methods were commonly chosen, such as "A bank vault that requires both a fingerprint and a retina scan" and "A door with a display screen that requires a PIN and then selection of a secret image." These results suggest a potential misunderstanding or lack of clarity regarding the concept of two-factor authentication. Further education and clarification may be necessary to ensure accurate comprehension and application of 2FA principles. Figure 62 shows these results.

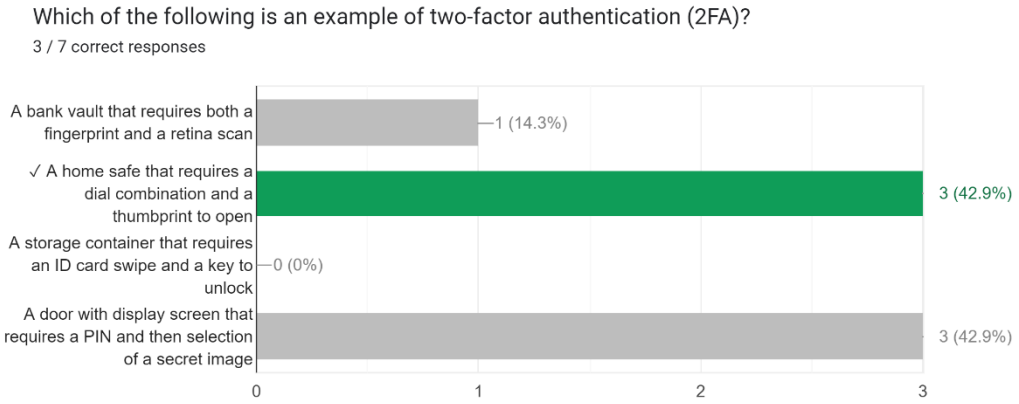

Figure 62 Quantitative Post-Test 2FA Question

In the quantitative analysis of participants' comprehension of physical access controls, the correct options were identified as "Keycard Reader" and "Video Surveillance Cameras." Findings reveal that three participants accurately selected both correct options, resulting in a 30% accuracy rate. However, the majority of participants, seven out of ten, provided mixed responses, including options that did not align with Physical Access Controls. These incorrect selections commonly included components associated with network security or data protection, such as "Endpoint Detection and Response (EDR)" and "Data Encryption." This suggests a potential misunderstanding of the criteria for Physical Access Controls among some participants. Further clarification and reinforcement of concepts related to access control mechanisms may be necessary to ensure accurate understanding and application of security protocols. Figure 63 shows

these results.

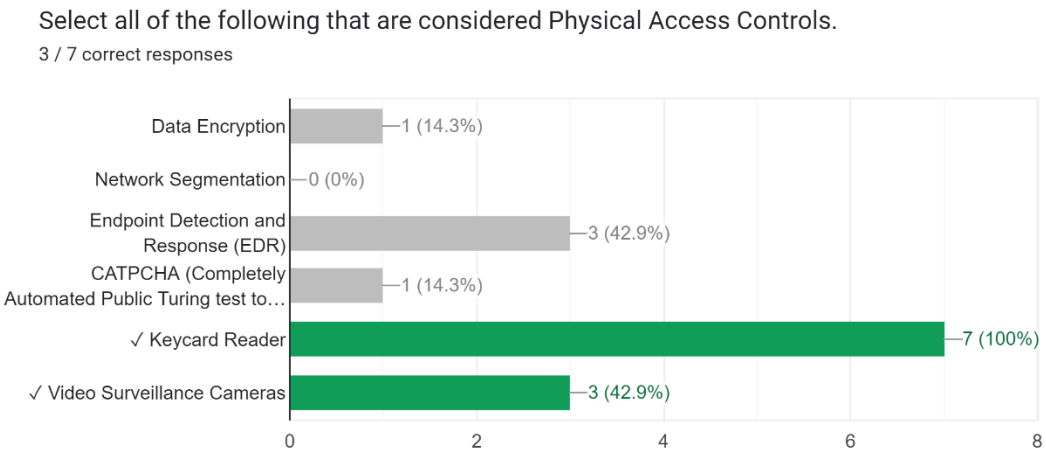

Figure 63 Quantitative Post-Test Physical Access Controls Question

In the quantitative analysis of participants' understanding of the distinction between Authentication and Identification, the correct answer was determined to be "Authentication confirms, identification assigns." Findings indicate that one participant accurately selected this response, resulting in a 10% accuracy rate. However, the majority of participants, nine out of ten, provided incorrect answers. Among the incorrect selections, options commonly included statements that did not accurately differentiate between Authentication and Identification. For instance, "Authentication assigns roles, whereas identification verifies" was chosen by three participants, and "Authentication labels, while identification proves" was chosen by one participant. These results suggest a potential misunderstanding or lack of clarity regarding the distinction between Authentication and Identification among some participants. Therefore, further education

and clarification may be necessary to ensure accurate comprehension and application of these fundamental concepts in security protocols. Figure 64 shows these results.

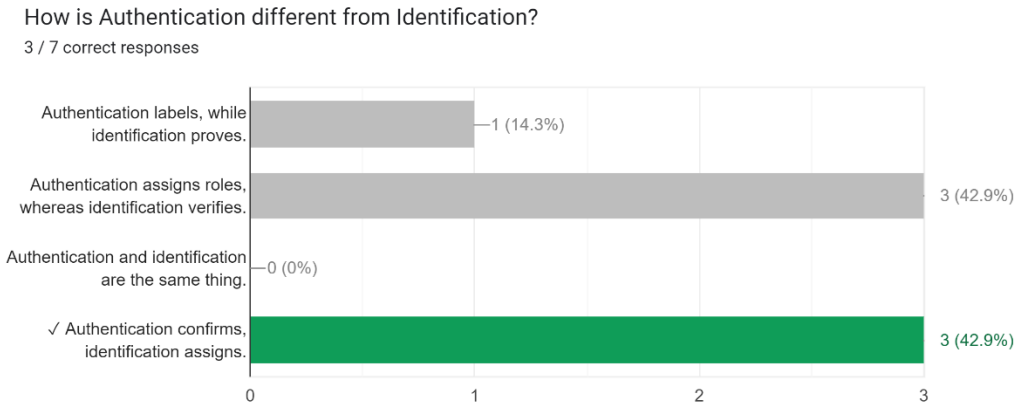

Figure 64 Quantitative Post-Test Authentication Question

In the quantitative analysis of participants' knowledge regarding prevalent cyber attack vectors, the correct answer, as reported by "MockCertified," was identified as "Email." Findings reveal that six participants accurately selected this response, resulting in a 60% accuracy rate. However, a significant number of participants, four out of seven, provided incorrect responses. Among the incorrect selections, "Weak Passwords" was chosen twice. These results suggest a potential misconception or lack of awareness regarding prevalent cyber attack vectors among some participants. Therefore, further education and reinforcement of cybersecurity concepts may be necessary to enhance participants' understanding of common cyber threats and mitigation strategies. Figure 65 shows these results.

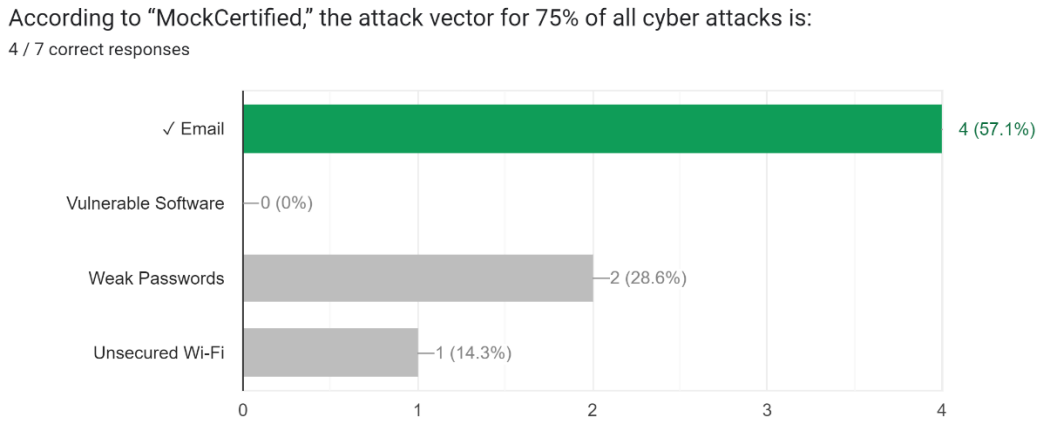

Figure 65 Quantitative Post-Test Attack Vector Question

In the qualitative analysis of participants' feedback on the interactive cybersecurity game, several insightful comments were provided by those who completed the entire gameplay. One participant noted a brief challenge with navigating the doors initially, describing a momentary confusion after clicking the security badge. They mentioned difficulty moving forward or backward, only being able to move sideways and look around. However, after several attempts, they discovered that clicking back on the screen after clicking the badge allowed movement forward through the door. Despite this initial hurdle, they found the game to be highly informative and engaging, appreciating its interactive approach to learning about cybersecurity. Another participant echoed similar sentiments, describing the game as a fun and interesting way to teach cybersecurity concepts. They found the game to be a cool idea and enjoyed the interactive experience it offered. These comments highlight the positive reception of the game among participants, emphasizing its effectiveness as an educational tool and its

engaging design. Figure 66 shows this.

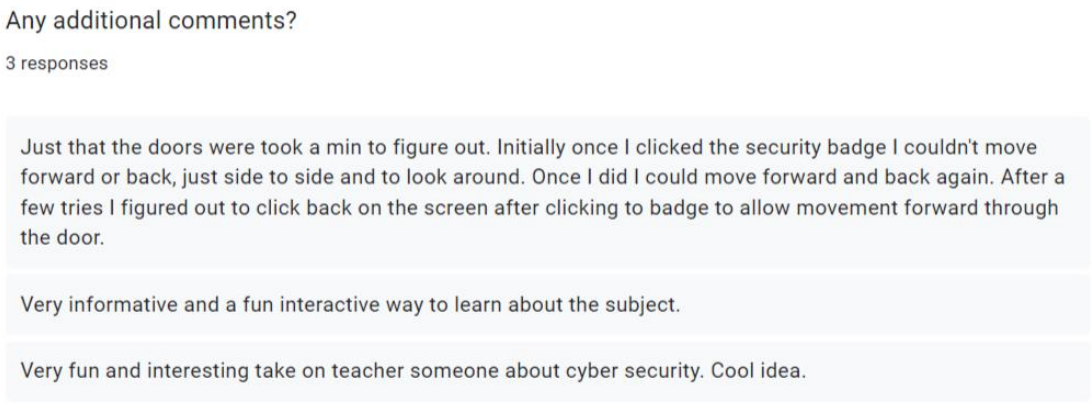

Figure 66 Quantitative Post-Test Additional Comments

5.6.4 Quantitative Findings

The quantitative analysis provides detailed insights into the effectiveness of the interactive cybersecurity game in enhancing participants' understanding of key concepts. Before engaging with the game, only 20% of participants accurately identified examples of two-factor authentication (2FA). This indicates a significant gap in comprehension. However, post-gameplay, this figure remained unchanged, with only 10% accurately selecting the correct 2FA example. Similarly, while all participants correctly understood the distinction between Identification and Authentication in the pre-test, their performance varied in other areas. For instance, in the assessment of prevalent cyber attack vectors, only 20% accurately identified "Email" as the leading cause, with the majority providing incorrect responses.

Interestingly, in the evaluation of Physical Access Controls, there was a notable improvement post-gameplay. While initially, only 30% of participants accurately selected all correct options, this increased to 30% after engaging with the game. This suggests that

the interactive experience facilitated a better understanding of this concept among participants. However, challenges persisted, particularly in the comprehension of two-factor authentication examples, where there was minimal improvement observed post-gameplay.

Despite these quantitative findings indicating persistent areas of confusion, qualitative feedback from participants highlighted the positive impact of the game in terms of engagement and enjoyment. Specifically, participants appreciated the interactive approach to learning cybersecurity concepts and found the game to be informative and interesting. This suggests that while there may be room for improvement in terms of content clarity and comprehension, the game succeeded in engaging participants and fostering a positive learning experience. Moving forward, addressing the identified areas of confusion while maintaining the engaging aspects of the game could further enhance its effectiveness as an educational tool in cybersecurity.

5.7 Conclusion

In conclusion, this study provides valuable insights into the potential of gamified approaches for cybersecurity training, particularly in the context of CMMC compliance. Through a rigorous analysis of both qualitative and quantitative data, the effectiveness of gamification in enhancing engagement and knowledge retention has been demonstrated. While the results indicate areas for improvement, such as the need for clarification on certain concepts like two-factor authentication, the overall positive feedback from participants underscores the value of gamified training in fostering cybersecurity awareness.

The findings suggest that gamified methodologies can play a pivotal role in bridging the gap between theoretical knowledge and practical application, empowering individuals to navigate complex cybersecurity landscapes with confidence. By addressing the identified limitations and challenges, such as content clarity and comprehension, organizations can refine their gamified training programs to better meet the needs of participants.

There are promising opportunities for further exploration and development in gamified cybersecurity training. Future research could focus on refining game mechanics, enhancing instructional design, and tailoring content to specific organizational needs. Additionally, expanding the scope of gamified training beyond CMMC compliance to broader cybersecurity education initiatives holds significant potential for advancing cybersecurity awareness and preparedness on a larger scale.

Overall, this study contributes to the growing body of knowledge on gamified cybersecurity training and emphasizes its importance in cultivating a culture of cybersecurity awareness within organizations. By leveraging gamification, organizations can effectively educate and empower their workforce to address evolving cybersecurity threats and challenges.

GAME ASSET ATTRIBUTIONS

Information Icon Pink – https://skfb.ly/6YHtT

Profile Name: Maeron

Modifications: Altered Material Color

3D Numbers (All) - https://skfb.ly/o8LZr

Profile Name: Jihambru

Modifications: Altered Glow Material Color

Spherical Hex Force Field - https://skfb.ly/6VpBU

Profile Name: DaBoRi

Filing Cabinet - https://skfb.ly/oCoM7

Profile Name: Jean-Francois.Bonin

Aztec glowing coin - https://skfb.ly/oIztn

Profile Name: SovietCream

Computer desk with uv - https://skfb.ly/oLGYr

Profile Name: renanz

Modifications: Altered Glow Material Color

ID Card Model - https://skfb.ly/6X8ED

Profile Name: Johana-PS

Modifications: Altered Material

Sci Fi gate - https://skfb.ly/6XFvR

Profile Name: Preethi Venkataraman

REFERENCES

AlMarshedi, A., Wanick, V., Wills, G. B., & Ranchhod , A. (2017). *Chapter 2 - Gamification and Behavior*. Retrieved from https://giorgioratti.com/wp-content/uploads/2018/11/9783319455556-c2.pdf

Alqahtani, H. &.-T. (2020, February 21). *Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)*. Retrieved from MDPI: https://www.mdpi.com/2078-2489/11/2/121

Andreev, I. (2023, May 17). *Gamification.* Retrieved from Valamis: https://www.valamis.com/hub/gamification

Armond, A. (2021, November 9). *CMMC 2.0 is here - what changes in CMMC?* Retrieved from CMMC Audit Preparation.

Bjorklund, D. (2023, June 8). *CMMC Compliance Explained: Protecting Sensitive U.S. Government Information*. Retrieved from fractionalciso: https://fractionalciso.com/cmmc-compliance-explained/

CMMC 1.0 vs. CMMC 2.0: What's Changed and What It Means for Your Business. (2023, October 10). Retrieved from Kiteworks: https://www.kiteworks.com/risk-compliance-glossary/cmmc1-0-vs-cmmc2-0-what-changed/#:~:text=The%20CMMC%201.0%20model%20established,requirements%20for%20the%20specific%20contract.

CMMC is delayed until 2024; now what? (2023). Retrieved from defenseandmunitions: https://www.defenseandmunitions.com/article/cybersecurity-maturity-model-certification-delayed-until-2024-now-what/

CMMC Model. (n.d.). Retrieved from defense.gov: https://dodcio.defense.gov/CMMC/Model/

Cohen, J. (2023, February 16). *What are the Top Challenges Associated with CMMC 2.0 Compliance?* Retrieved from Kyber Security: https://kybersecure.com/challenges-associated-with-cmmc-compliance/

Common NIST and CMMC 2.0 compliance challenges. (2023, October 3). Retrieved from Braxton: https://braxtongrant.com/common-cmmc-and-nist-challenges/

Cybersecurity Maturity Model Certification (CMMC) Training: Certified Professional. (2022, August 16). Retrieved from National Initiative for Cybersecurity Careers and Studies: https://niccs.cisa.gov/education-training/catalog/learning-tree-international-inc/cybersecurity-maturity-model

Doubleday, J. (2023, February 2). *Big questions continue to swirl around CMMC in 2023*. Retrieved from Federal News Network: https://federalnewsnetwork.com/acquisition-policy/2023/02/big-questions-continue-to-swirl-around-cmmc-in-2023/

Drapkin, A. (2024, February 26). *8 Worrying Cybersecurity Statistics You Need to Know in 2024*. Retrieved from tech.co: https://tech.co/news/cybersecurity-statistics-2024

Harford, I. (2022, July 29). *10 biggest data breaches in history, and how to prevent them*. Retrieved from techtarget: https://www.techtarget.com/searchsecurity/feature/10-biggest-data-breaches-in-history-and-how-to-prevent-them

MockCertfied. (2024, April 1). *The Top 10 Cybersecurity Facts of 2024! How Many Do You Know?* Retrieved from Medium: https://mockcertified.medium.com/the-top-10-cybersecurity-facts-of-2024-how-many-do-you-know-030d4961dbbf

Mulkeen, D. (2018, July 27). *The Top 5 Benefits of Gamification in Learning*. Retrieved from learnlight: https://www.learnlight.com/en/articles/5-benefits-of-gamification-in-learning/#:~:text=The%20gamification%20of%20learning%20allows,result%20in%20consequences%20or%20rewards.

Ninja, T. (2023, October 3). *Up-to-Date Cybersecurity Statistics for 2023* . Retrieved from NinjaOne: https://www.ninjaone.com/blog/smb-cybersecurity-statistics-2023/

Palatty, N. J. (2023, October 20). *160 Cybersecurity Statistics 2023 [Updated]*. Retrieved from getastra: https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=160%20Cybersecurity%20Statistics%202023%20%5BUpdated%5D&text=Cybersecurity%20statistics%20indicate%20that%20there,cost%20%248%20trillion%20by%202023.

St. John, M. (2024, February 28). *Cybersecurity Stats: Facts And Figures You Should Know*. Retrieved from Forbes: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

Stanton, T. (2021, December 2). *CMMC Training: Everything You Need to Know*. Retrieved from Etactics: https://etactics.com/blog/cmmc-training

Steen, T. v., & Deeleman, J. (2021). Retrieved from Successful Gamification of Cybersecurity Training | Cyberpsychology, Behavior, and Social Networking.: https://www.liebertpub.com/doi/10.1089/cyber.2020.0526

The history of gamification (from the very beginning to now). (2019, August 29). Retrieved from growthengineering: https://www.growthengineering.co.uk/history-of-gamification/

Top 7 Benefits of Gamification in Workplace Training. (2023, January 11). Retrieved from inspiredelearning: https://inspiredelearning.com/blog/benefits-of-gamification-in-workplace-training/

Trombino, G. (n.d.). Retrieved from Gamifying Cybersecurity: A Study of the Effectiveness of a Specified Gamified Tool: https://end-educationconference.org/wp-content/uploads/2023/06/02_OP_541.pdf