ISSN: 2473-4901
v9 n6046

# Educating the Next Generation of CSOs: An Exercise in Conversational Role Play with ChatGPT

Reshmi Mitra
rmitra@semo.edu
Department of Computer Science

Dana Schwieger
dschwieger@semo.edu
Department of Management

Indranil Roy
iroy@semo.edu
Department of Computer Science

Southeast Missouri State University
Cape Girardeau, MO 63701 USA

## Abstract

The role of Chief Security Officer (CSO) is of vital importance. Professionals are expected to have experience and a comprehensive set of capabilities addressing technical, business, legal, ethical, and soft skills. The multifaceted nature of this role and the need for meaningful experiential knowledge requires faculty to take a unique approach to preparing students to enter the field. In this paper, the authors describe a project developed for a graduate level cybersecurity course in which students assume cybersecurity roles in an industry of their choosing to gain insights into the day-to-day responsibilities of that position. Acting in their assigned roles, students interact with ChatGPT in a simulated complex cybersecurity scenario to explore potential attack vectors and devise strategic responses in a learning environment that bridges the gap between theory and practice. The authors describe the exercise as well as the background behind its development.

**Keywords:** Teaching tip, Cybersecurity, CSO, ChatGPT, Role Playing

### 1. INTRODUCTION

The rapidly evolving landscape of cybersecurity presents an array of unique challenges, both to industry professionals and the educational institutions responsible for preparing the next generation of experts. A position of vital importance within this landscape is the role of the Chief Security Officer (CSO), an individual charged with overseeing an organization's information and data security, monitoring threats, developing and implementing security strategies, and coordinating timely and effective responses to any cyber-attack. The CSO's responsibilities extend far beyond the realm of technology, encompassing areas such as regulatory compliance, risk management, and collaboration with various organizational stakeholders (Fruhlinger, 2021; Kappers & Harrell, 2020; Kim & Surendran, 2002; Staff, 2023).

Organizations seek applicants for this role with both academic and experiential knowledge. The challenge to educators is to develop and incorporate realistic experiential learning opportunities to provide students with hands-on

experience and bridge the gap between theory and practice. In the following sections, the authors address the challenges faced by graduate programs training the next generation of CSOs and offer an experiential learning exercise that faculty can adopt in their classrooms.

## 2. LITERATURE REVIEW

In an era marked by increasing digital interconnectivity and sophisticated cyber threats, the importance of the CSO's role cannot be overstated. The multifaceted nature of this position reflects the complex nature of cybersecurity itself, a field that requires a comprehensive understanding of technological systems and human behavior, as well as the legal and ethical frameworks that govern them (Fruhlinger, 2021). Preparing students for such intricate and demanding professional roles necessitates a departure from traditional pedagogical approaches (Gross & Ho, 2021; Kappers & Harrell, 2020; Lewis & Crumpler, 2019).

### Educational Frameworks

The Association of Computing Machinery (ACM) Education Board, in 2015, recognized the need to develop a joint task force to address the need for a comprehensive cybersecurity curricular framework. A panel of experts was assembled to develop the first set of global curricular recommendations for cybersecurity education, the CSEC2017 (CSEC2017, 2017). As part of their effort to link cybersecurity curriculum to professional practice, the task force recommended programs incorporate experiential learning opportunities into their educational program "roadmaps" (CSEC2017, 2017, p. 85)

Similarly, in revising the Computing Curricula CC2005 framework, the CC2020 task force recognized the importance of incorporating innovative strategies in helping students attain educational competencies (CC2020, 2020) The report noted that educational competency-based outcomes often required a broader set of pedagogical experiences such as "interactive simulations, intensive projects, field experiences, internships, and cooperative programs with industry" (CC2020, 2020, p. 55).

### Post-Secondary Cybersecurity Programs

The process of teaching cybersecurity to graduate students presents unique challenges that require tailored approaches, especially considering the likely diversity in student backgrounds (CC2020, 2020). Some students may be well-versed in the fundamental concepts of cybersecurity, while others may lack exposure to advanced security concepts and techniques. The varying degrees of knowledge and experience within the classroom necessitate the implementation of a learning framework that can cater to all skill levels.

Providing such individualized instruction and assessment is a daunting task. This is especially true when concerned with producing high quality project deliverables for client-based projects. Although not the perfect client, artificial intelligence can provide an alternative platform for offering a client-based project experience.

### OpenAI's ChatGPT

OpenAI's ChatGPT provides a flexible tool for simulating real-world scenarios for a variety of skill levels. According to OpenAI's ChatGPT, the app can do a variety of tasks including: answering questions on a wide range of topics, generating text, learning complex concepts and explaining them in simpler terms, making recommendations, and serving as a conversational partner (ChatGPT, 2023). ChatGPT's conversational responses build upon prior dialog to simulate working with a client. This ability allows students with a variety of skill levels to arrive at similar results even though the conversations paths may widely differ.

The adoption of chatbots (like ChatGPT) as a pedagogical tool is gaining traction in higher education (Adiguzel, 2023; Grassini, 2023), allowing educators to automate grading and focus on lesson planning and individualized student support. These personalized learning platforms not only save time, but also enhance student engagement and motivation by catering to their unique needs and interests. On the downside, ChatGPT's inability to engage in higher-order cognitive tasks and deep understanding can limit its educational applications (Farrokhnia, 2023). Moreover, ethical challenges, like the potential for bias and the risk to academic integrity, need to be carefully managed. These limitations necessitate caution and ongoing research into how best to integrate such AI tools into educational settings.

## 3. ChatGPT Client-Base Exercise

Given the urgency of this educational challenge (CC2020), particularly at the graduate level, this teaching tip paper outlines an innovative and immersive approach to cybersecurity education, tailored to meet the diverse needs and varying skill levels of Computer Science students. Recognizing that theoretical knowledge alone is insufficient, this method focuses on engaging students through real-world scenarios, case studies, and hands-on exercises (CC2020, 2020;

CSEC2017, 2017; Gross & Ho, 2021; Lewis & Crumpler, 2019). By grounding abstract principles in practical applications, it aims to foster critical thinking and analytical skills, encouraging students to ask probing questions and apply their learning in contexts that closely mirror the professional world of cybersecurity.

One of the core elements of this approach is the inclusion of role-playing techniques, through which students are designated specific roles within simulated organizational frameworks. Assigning students, the role of CSO, for example, allows them to gain insights into the day-to-day responsibilities and challenges of this pivotal position. It also promotes a sense of ownership and accountability, instilling an appreciation of the multifaceted challenges and decision-making processes that security professionals face.

This real-world simulation is further enriched through the utilization of cutting-edge tools like ChatGPT. This dynamic platform provides an interactive learning environment, enabling students to simulate complex cybersecurity scenarios, explore potential attack vectors, and devise strategic responses. It bridges the gap between theory and practice, equipping students with the tools and confidence to apply their knowledge in a meaningful and impactful manner. In today's globalized and interconnected world, the stakes of cybersecurity have never been higher. As recent high-profile breaches have shown, failures in cybersecurity can have devastating consequences, affecting not only individual organizations but entire economies and national security. In this context, the role of the CSO is not merely a technical one, but also a strategic and leadership position that requires a broad understanding of technology, governance, human factors, and more.

The need to prepare students for such multifaceted roles is a driving force behind the pedagogical approach outlined in this paper. By moving beyond traditional lecture-based learning and embracing interactive and experiential methods, it seeks to provide students with a more holistic and nuanced understanding of the field. The integration of role-playing, real-world scenarios, and cutting-edge tools like ChatGPT represents a departure from conventional teaching methods, reflecting a commitment to innovation, adaptability, and relevance.

The modern Computer Science graduate student must be more than a technically proficient individual. They must be aware of the work of security professionals and the broader context in which cybersecurity operates. They must be able to think critically, communicate effectively, and operate ethically. Above all, they must be prepared for the constantly changing and often unpredictable nature of cybersecurity itself.

In conclusion, the innovative pedagogical approach described herein offers a promising pathway towards these educational goals. By aligning academic learning with professional practice, fostering collaboration, and emphasizing the complex and multifaceted nature of cybersecurity, it seeks to prepare students for the challenges and opportunities of a rapidly changing field.

The following sections of this paper will delve further into the methods, strategies, and assessments employed, offering educators insights and practical tools to enhance their teaching and better equip their students for the vital roles they will play in safeguarding our digital future, including the critical position of CSO.

## 4. ASSIGNMENT BACKGROUND AND FRAMEWORK

The following subsections outline the logic and methods used to incorporate a cyber security simulated interview into a 500-level computer science course at the authors' institution.

**Preparation and Contextualization:**
Recognizing that the class comprised students with varying levels of familiarity with cybersecurity, the first 4 weeks were devoted to foundational lectures on (1) CIA (Confidentiality, Integrity, Availability) concepts in hardware, software, data and network, (2) Introductory preventive measures like access control and authentication, and (3) Malicious software attacks. The course was carefully scaffolded to ensure that all students had a grounding in essential concepts before progressing to more advanced material.

The first midterm assignment was devised to build upon this foundation, challenging students to apply their newfound knowledge to realistic scenarios. To achieve this, the assignment was structured to simulate the responsibilities and decision-making processes inherent to a security leadership role, providing opportunities for hands-on exploration and analysis.

**Objective and Real-World Incorporation:**
To better align theoretical constructs with practical reality, students are required to construct comprehensive security case studies that focus on hypothetical, yet plausible, attack scenarios and

solutions. Special emphasis is placed on key aspects of cybersecurity, notably authentication and access control mechanisms. These case studies serve as a bridge between abstract concepts and real-world application providing a tangible context in which students can apply their learning.

The assignment addresses the following learning objectives:

1. Understand basic information assurance terminology.
2. Understand computer security policies and how they are implemented in organizations.
3. Understand privacy concerns in computing
4. Identify and reduce complexity of Cyber enabled systems
5. Understand how secure computer systems are designed.

The primary objective of this assignment is multifaceted to achieve several educational outcomes simultaneously. First, it aspires to foster a deep-rooted understanding of the real-world implications of cybersecurity challenges thereby elevating the learning experience beyond the realm of mere theoretical knowledge. Second, the assignment seeks to engage students in practical applications that mirror the complexities and challenges faced by cybersecurity professionals in the field. Last, but just as critical, it aims to cultivate critical thinking and collaborative skills, enabling students to evaluate problems from various angles and work cohesively as a team to develop solutions.

To further aid the learning process, students are provided with high-quality, industry-trusted documentation two weeks before the assignment is due. This preparatory material includes the Open Worldwide Application Security Project (OWASP2023) attack surface analysis cheat sheet and the National Institute of Standards and Technology (NIST2006) guide on Integrating Forensic Techniques into Incident Response. These resources serve as foundational texts that guide the students in both the theory and practical aspects of the assignment, thereby enhancing the quality and depth of their engagement with the material.

**Group Formation and Role Assignment:**
The assignment began with dividing students into groups, each given an industry-specific scenario such as medical device wearables, unpatched vulnerabilities exploited by ransomware actors, security on a shoestring budget, phishing attack on financial institution, handling employee lay-offs in remote work, among others. Role-playing was employed, with each student assuming the position of a CSO (Chief Security Officer), responsible for planning against cyber-attacks within their industry. (See Appendix 1.)

This approach facilitated a more profound engagement, simulating professional practice and promoting empathy for the complexities and challenges faced by security professionals. The role-play not only made the task more engaging but also allowed students to synthesize and apply their learning in a context that mirrored professional realities.

**Utilizing ChatGPT for scenario development:**
ChatGPT usage in the cybersecurity course provided a transformative experience for students, particularly for the current generation accustomed to rapid, dynamic learning environments. In an era where digital literacy extends beyond basic computing skills to include proficiency in navigating complex AI-driven platforms, understanding ChatGPT is no longer optional; it's essential. This generation of students will likely encounter AI interfaces and tools in their future roles in cybersecurity, making their familiarity with platforms like ChatGPT not just advantageous but crucial for professional adaptability.

ChatGPT served as a versatile tool for crafting, exploring, and critically analyzing various attack and defense scenarios. Unlike static models or templates, ChatGPT offers a dynamic environment where students can simulate real-time dialogues around evolving cybersecurity issues. This feature is incredibly relevant for the modern student who thrives on interactive and immediate feedback mechanisms, thus providing a richer, more engaging learning experience. By functioning as a 'virtual collaborator,' the tool allowed students to probe complex questions, iterate ideas, and arrive at nuanced solutions, all while adapting to the specific contexts of different industries.

Furthermore, ChatGPT ensures that the educational content stays aligned with contemporary industry trends. The platform's advanced AI algorithms and real-world applicability prepare students for the fluid, fast-paced challenges they will face in today's cybersecurity landscape. Therefore, ChatGPT does more than facilitate topic exploration; it cultivates a set of skills and a mindset aligned with the complexities and demands of modern cybersecurity work.

**Deliverables and Evaluation Criteria:**
The final deliverable required the submission of a comprehensive report, detailing the scenario, original design diagrams of the cyberinfrastructure, attack surface, attack vectors, potential attack scenarios, a checklist on access control and authentication remedial measures, references, and a list of

contributions from each group member. The assessment criteria were designed to encourage a holistic approach, rewarding not only technical accuracy but also creativity, critical thinking, and collaboration. Throughout the process, continuous instructor feedback was provided, guiding students towards successful completion of the project.

The assessment criteria were explicitly aligned with the learning objectives, encouraging a holistic approach that rewarded technical accuracy, creativity, critical thinking, and collaboration. Students were provided a comprehensive rubric detailing the expectations for each component of the report. (See Appendix 1, 2 and 3.)

## 5. COMPREHENSIVE REPORT

The assignment required the submission of a comprehensive report that encompassed an in-depth security analysis, alignment with institutional goals and profiles, clarity in idea development, critical analysis of readings and references, quality of writing and proofreading, and a clear listing of contributions by group members. These deliverables were crafted to assess various dimensions of student learning, from technical knowledge to critical thinking, collaboration, and communication skills.

**Grading Rubric:**
Evaluation of the deliverables was carried out using a clearly defined grading rubric that categorized performance into three levels: Very Good (100-80%), Fair (80-60%), and Poor (60-40%). The rubric was shared with students at the outset to ensure transparency and clarity in expectations. (See Appendix 3.)

**Security Analysis:**
This aspect evaluated the report's discussion of potential security breaches, focusing on vulnerabilities and implications for confidentiality, integrity, and availability. A comprehensive report that addressed at least three ways in which security might be breached received a higher rating, while missing or incomplete information rated poorly.

**Security Goals and Institution Profile**:
This criterion assessed the connection between the institution's profile, recovery budget, and the implications of the attack. A well-connected analysis scored highly, whereas a failure to make these connections was rated poorly.

**Development of Idea and Clarity:**
This part of the rubric examined the development and articulation of ideas within the report. Well-developed and clearly expressed ideas were rated highly, while poorly developed ideas that lacked clarity received a lower score.

**Critical Analysis:**
This section evaluated the report's understanding of required readings, underlying concepts, and links to real-life case studies. Strong understanding and connection with outside references were rated highly, while personal opinions without supporting evidence were rated poorly.

**Quality of Writing and Proofreading:**
This criterion looked at the grammatical accuracy, spelling, punctuation, and overall writing style. Error-free and well-facilitated communication scored highly, while numerous errors that hindered effective communication were rated poorly.

**List of Contributions:**
This portion of the evaluation assessed the coherence of the report and the distribution of work among group members. Uniform work distribution and a single coherent report were rated highly, while missing or incomplete group member information was rated poorly.

**Alignment with Objectives:**
The evaluation criteria were meticulously aligned with the objectives of the assignment to ensure a fair and comprehensive assessment of student performance. By explicitly detailing the grading expectations and aligning them with the deliverables, a clear roadmap was provided to guide students' efforts, ensuring that the assessment process was transparent, consistent, and aligned with the educational goals of the assignment.

**Iterative Process and Collaborative Learning:**
The assignment was designed as an iterative, collaborative learning journey. Students were encouraged to work together, progressively deepening their analysis, and expanding their focus. Initial stages involved broad exploration, with subsequent iterations concentrating on specific attack vectors, preventive measures, and context-specific considerations.

Regular checkpoints were built in to facilitate ongoing dialogue within groups, fostering a genuinely collaborative environment. Opportunities for peer review and feedback were also embedded, promoting a culture of shared learning and collective responsibility for the group's success.

**Reflection and Analysis:**
Post-assignment reflection was a key component of the learning process. Facilitated sessions allowed students to share insights, reflect on their learning journey, and critically assess the effectiveness of the

methods used. This reflective practice was vital for reinforcing learning, providing opportunities for meta-cognition, and fostering a deeper appreciation of the applicability of the skills and knowledge acquired.

To guide these reflective discussions, the following questions were posed to the class:

1. What are the challenges your team faced in balancing the core principles of the CIA triad (Confidentiality, Integrity, Availability) within your case study. Were compromises or trade-offs necessary? How did you prioritize?

2. Assess the authentication and access control measures your group proposed for the case study. How confident are you in the effectiveness of these measures, and what were the primary challenges in formulating solutions that were both secure and practical?

3. Evaluate the attack surface as presented in your case study. How would you go about minimizing it, and what would you do differently in a real-world setting?

4. As a group, discuss how the role of a Chief Security Officer (CSO) in your simulated organization diverged from your initial perceptions. Were there responsibilities or facets of the role that surprised you? How has this deepened understanding of the CSO role prepared you for future careers in cybersecurity?

5. Delve into the ethical considerations that your team grappled with while crafting potential attack scenarios. What measures did you take to ensure the ethical integrity of your work, and how do you think these ethical considerations will apply in real-world settings?

These reflection questions were designed to stimulate critical thought, encourage meaningful dialogues among team members, and to add layers of complexity to their understanding of cybersecurity.

## 6. IMPLEMENTATION RESULTS

This assignment was introduced in fall 2020 in its current take-home format where each student group had seven days to complete the assignment with a requirement to submit an early draft by the 3rd or 4th day. This was the first semester in which ChatGPT was introduced into the curriculum, capitalizing on its growing popularity as an AI-based pedagogical tool. The assignment was largely well-received, with many students indicating a preference for this hands-on approach over traditional textbook questions. The use of ChatGPT and the structure of the assignment encouraged students to develop a nuanced understanding of secure computing system design guided by NIST frameworks. Furthermore, in the future we aim to incorporate student feedback into the assignment's structure and evaluation methods to be collected and analyzed under IRB-approved protocols.

## 7. CONCLUSION

In conclusion, this teaching tip paper highlights the intricacies of crafting a dynamic and comprehensive learning experience for graduate students enrolled in an introductory cybersecurity course. The central objective of the assignment was to bridge the gap between theoretical frameworks and real-world applications, particularly emphasizing the role of the Chief Security Officer (CSO) within an organization. The modern landscape of cybersecurity is incredibly complex and understanding the multidimensional concerns that a CSO faces-ranging from multifaceted threats to compliance to managing human factors—is indispensable for any student aspiring to a career in this field.

The assignment leveraged the capabilities of ChatGPT as an innovative pedagogical tool to simulate realistic cyber-attack scenarios. This AI-driven approach allowed students to grapple with nuanced security challenges in a risk-free environment, further enriching their understanding of both attack and defense strategies. Importantly, the assignment was structured to encourage peer-to-peer learning, where student groups could analyze and learn from each other's case studies, thereby gaining a broader perspective on the diverse challenges that security professionals confront. This collaborative approach provides a two-fold benefit: it enhances individual comprehension and collectively elevates the class's mastery over complex cybersecurity issues. Overall, the assignment served as a multi-faceted learning approach that can be adapted and scaled for various educational settings, fostering not only technical skills but also the holistic competencies required for excelling in the rapidly evolving cybersecurity landscape.

## 8. REFERENCES

Adiguzel, T., Kaya, M. H., & Cansu, F. K. (2023). Revolutionizing education with AI: Exploring the transformative potential of ChatGPT. *Contemporary Educational Technology*,

15(3), ep429.

ACM and IEEE-CS, (2017). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY. https://doi.org/10.1145/3184594

CC2020 Task Force (2020). Computing Curricula 2020 (2020). Retrieved on May 29, 2023, from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf

Farrokhnia, M., Banihashem, S. K., Noroozi, O., & Wals, A. (2023). A SWOT analysis of ChatGPT: Implications for educational practice and research. *Innovations in Education and Teaching International*, 1-15.

Fruhlinger, J. (2021). The CSO role today: Responsibilities and requirements for the top security job. *CSO*. Retrieved August 26, 2023, from https://www.csoonline.com/article/521506/the-cso-role-today-responsibilities-and-requirements-for-the-top-security-job.html

Grassini, S. (2023). Shaping the future of education: exploring the potential and consequences of AI and ChatGPT in educational settings. *Education Sciences*, 13(7), 692.

Gross, M. & Ho., S. M. (2021). Collective learning for developing cyber defense consciousness: An activity system analysis. *Journal of Information Systems Education*. 32(1), 65-76.

Kappers, W. M., & Harrell, M. N. (2020). From degree to Chief Information Security Officer (CISO): A framework for consideration. *American Society for Engineering Education Virtual Conference Proceedings*. Retrieved August 26, 2023, from https://commons.erau.edu/publication/1575/

Kim, K. Y. & Surendran, K. (2002). Information security management curriculum design: A joint industry and academic effort. *Journal of Information Systems Education*. *13*(3), 227–235

Lewis, A. W. & Crumpler, W. (2019). The cybersecurity workforce gap. Center for Strategic & International Studies. Retrieved August 26, 2023, from https://www.csis.org/analysis/cybersecurity-workforce-gap

NIST (2006) National Institute of Standards and Technology Guide to Integrating Forensic Techniques into Incident Response https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

OWASP (2023). Open Worldwide Application Security Project (OWASP) Attack Surface Analysis Cheat Sheet. Retrieved on Oct 9, 2023, from https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

Staff, S.M. (2023). Fast Facts: 5 essential competencies for CSOs *Security Management Journal of Information Systems Education Retrieved August 26, 2023, from https://www.asisonline.org/security-management-magazine/articles/2023/05/how-to-become-a-cso/fast-facts/*.

ISSN: 2473-4901
v9 n6046

# Appendix 1 - Exercise Description

**Midterm 1**
**30 points**

**Overview:**
In this assignment, you will assume the role of the **Chief Security Officer (CSO)** within a simulated organization, focusing on preparing for potential cyber-attacks. Your specific topic and case study will be posted on your group's Canvas announcements page. The aim is to provide you with a hands-on experience in planning and strategy development for countering cyber threats.

To further enrich your learning, we have integrated **ChatGPT** to help refine your understanding and simulate realistic cyber-attack scenarios. Working in your team teams, you will be responsible for crafting a comprehensive security case study. This will involve identifying potential vulnerabilities, attack scenarios, and creating robust **access control and authentication** measures that align with industry standards. Through this group work, you will emulate the challenges and decision-making processes faced by a modern cybersecurity team led by a CSO.

**Instructions:**
Please upload a single PDF with the following components:

1. **Abstract (2.5 points)**: Include a 150-word abstract that succinctly explains the cyber-attack scenario your group has explored.
2. **Original Case Study Design Diagram (5 points):** Construct an original, case study-specific diagram that vividly illustrates the unique aspects of your chosen cyberinfrastructure system. The diagram should also clearly outline the attack surface as well as potential attack vectors relevant to your scenario.
3. **Attack Surface Definition (5 points):** Define and articulate the attack surface for your specific case study, with a particular emphasis on the CIA (Confidentiality, Integrity, Availability) components. Clarify how these elements create vulnerabilities that could be exploited in a cyber-attack. This foundational understanding will be crucial for discussing potential attack scenarios in the following section.
4. **Attack Scenarios (5 points):** Identify 2-3 potential scenarios in which the vulnerabilities outlined within your attack surface could be exploited, with a preference for software-based attacks. These scenarios should make clear how weaknesses in CIA could be targeted.
5. **Access Control and Authentication Checklist (5 points):**
    a. Identify stakeholders related to the infrastructure component and describe how to prioritize the work of security engineers in the event of an attack.
    b. Create a multi-level checklist detailing remedial measures to address the attack scenario.
6. **Sample Prompts (2.5 points)**: Include a section where you list 3-5 sample prompts that your group created and utilized to explore the case study more deeply using ChatGPT. Explain how using these prompts helped refine your understanding and contributed to your overall strategy.
7. **References (2.5 points):** Include 3-5 relevant articles, cited in IEEE style.
8. **Contributions (2.5 points):** Clearly list which group member was responsible for each part of the assignment preparation.

Your document should be 2-5 pages maximum, formatted in 12-point Times New Roman font with 1-inch margins. This is a group assignment, so please submit a single PDF for the entire group.

**Deliverables:**
Your comprehensive report should include the following:

- In-depth security analysis based on the scenario.
- Practical authentication and access control solutions.
- Alignment of proposed solutions with institutional goals and guidelines.
- Critical analysis of supplemental readings and references.

- Quality of writing, proofreading, and clear listing of contributions by each group member.

These deliverables are crafted to assess various dimensions of your learning, from technical skills to critical thinking, collaboration, and effective communication.

**Additional reading:** For this assignment, we strongly encourage you to consult the additional reading materials from NIST and OWASP. These documents offer essential frameworks and guidelines that are widely respected in the cybersecurity industry. Familiarizing yourself with NIST's recommendations and OWASP's vulnerability assessments can provide you with invaluable context for your case study. *Pls feel free to adapt the material to better suit the tone and needs of your case study.* Incorporating these resources in your report not only deepen your understanding of planning and countering cyber-attacks but also align your academic experience with industry standards.

# Appendix 2 – Final Report Format

**Midterm 2**
**30 points**

**Overview:**
In this part of the assignment, you will continue your role as the Chief Security Officer (CSO) of a simulated organization, with a focus on data collection and threat intelligence gathering specific to an assigned cyberinfrastructure topic. Your primary guide is Section 3.1 from a provided NIST PDF, but you are encouraged to consult additional resources to enrich your analysis. Your group will create a robust checklist for threat intelligence and be responsible for an executive summary and forensic analysis plan, among other deliverables.

An integral aspect of this assignment is peer review, a critical practice for quality assurance in cybersecurity. Your group will evaluate another group's security plan, offering a thorough critique of its strengths and weaknesses. This process not only improves your work through feedback but also provides exposure to alternative strategies and perspectives. Peer review serves as a real-world exercise in critical evaluation, honing your skills for a career in cybersecurity.

**Deliverables:**

Please upload a single PDF that includes:

1. **Group and Topic Identification (2.5 points):** State the name of your group and the assigned topic.

2. **Member Contributions (2.5 points):** Detail what each group member contributed to the assignment's preparation.

3. **Executive Summary (5 points):** In 2-3 sentences, summarize the problem statement and your approach to analysis.

4. **Peer-Group Critique (5 points):** Provide a half-page critique of the peer-group report assigned to your team. Evaluate the report as 'poor,' 'good,' or 'acceptable,' justifying your rating with reasoned arguments.

5. **Forensic Analysis Plan (5 points):** Submit a plan of less than one page for forensic analysis in the event of a cyber-attack. Your plan should include:
    a. Checklist with 15-30 bullet points: Emphasize potential sources of forensic data that have been covered in class.
    b. Categorize your attack surface in terms of vulnerability and recovery cost.
    c. Specify the memory media, logging systems, and network architecture used in your case study.
    d. Mention any forensic tools suitable for analysis.

6. **Original Design Diagram (5 points):** Create an original diagram that illustrates the system's complexity, potential attack vectors, and your forensic analysis plan. Make it presentable and meaningful, employing high-quality icons, a professional color scheme, and legible fonts.

7. **Sample Prompts (2.5 points)** - Include sample prompts that your group used to guide your investigation and final report. Explain how these prompts helped shape your final submission.

8. **References (2.5 points):** Include 3-5 relevant articles, cited in IEEE style.

ISSN: 2473-4901
v9 n6046

# Appendix 3 - Grading Rubric

**Grading Rubric**

| | Very good (100-80%) | Fair (80-60%) | Poor (60-40%) |
|---|---|---|---|
| **Security Analysis** (25% content) | Report discusses at least three ways in which the security of the system might be breached, focusing on security vulnerabilities. It addresses implications for various sort of security breach of confidentiality, integrity, and availability. | Report discusses at least two ways in which the security of the system might be breached, focusing on security vulnerabilities. It addresses implications for each sort of security breach of confidentiality, integrity, and availability. | Missing or incomplete information about vulnerabilities, attacks and harm to system and stakeholder. |
| **Security goals and institution profile** (25% content) | Institution profile and recovery budget is well-connected to the attack implications. | Institution profile and recovery budget is haphazardly connected to the attack implications. | Report fails to connect the budget constraints and does not consider institution-specific considerations. |
| **Development of idea and clarity** | • Well-developed ideas<br>• Introduces new ideas<br>• Well-articulated and understandable | • Developing ideas, work in progress<br>• Report is understandable, but some thought is required | • Poorly developed ideas which do not add to the objective of the assignment.<br>• Report is difficult to clarify |
| **Critical Analysis (Understanding of Reading and Outside References)** | Report displays an understanding of the required reading and underlying concepts including correct use of terminology and links with a specific real-life case study. | Report repeats and summarizes basic, correct information, but does not link readings to outside references, relevant research or specific real-life case study. | Report shows little or no evidence that readings were completed or understood. Report is largely personal opinions without supporting statements with concepts from the reading, outside resources, relevant research, or specific real-life case study. |
| **Quality of Writing and Proofreading** | Report is free of grammatical, spelling or punctuation errors. The style of writing facilitates communication. | Report contains some grammatical, spelling or punctuation errors that distract the reader. | Report contains numerous grammatical, spelling or punctuation errors. The style of writing does not facilitate effective communication. |
| **List of contributions** | Group submits a single coherent report | Work distribution is not uniform, and it is clear from the report writing that only one student did most of the work. | This list is missing, or name of the group members is incomplete |

*Figure 1- Report Grading Rubric*