Enhancing Student Learning in Information Security Courses: Integrating Generative AI, Critical Thinking, and Case-Based Pedagogy

Gary Yu Zhao
zhao@nwmissouri.edu

Cindy Zhiling Tu
cindytu@nwmissouri.edu

Joni Adkins
jadkins@nwmissouri.edu

School of Computer Science and Information Systems
Northwest Missouri State University
Maryville, Missouri, US

Abstract

Generative AI (GenAI) offers transformative potential in higher education, particularly in the information security field. This study explores the integration of GenAI tools into information security courses, proposing a structured framework that enhances critical thinking and problem-solving skills through case-based learning. By combining GenAI with the analytical framework, Motivation-Methods-Resources-Impact-Solutions (MMRIS), students gain a deeper understanding of complex cyber incidents and practical experience in GenAI-supported cybersecurity analysis. The approach fosters critical thinking across six dimensions and helps students allocate more time to higher-level tasks, such as evaluation and regulatory compliance. The findings suggest that GenAI tools can accelerate scenario comprehension and enrich educational outcomes.

Keywords: Generative AI (GenAI), MMRIS framework, information security, critical thinking, case study

Enhancing Student Learning in Information Security Courses: Integrating Generative AI, Critical Thinking, and Case-Based Pedagogy

Gary Yu Zhao, Cindy Zhiling Tu and Joni Adkins

1. INTRODUCTION

Utilizing case studies in an information security class offers numerous pedagogical and practical benefits, especially in boosting student comprehension, engagement, and critical thinking. As established through a comprehensive Delphi Study by the American Philosophical Association (Facione, 1990), critical thinking represents an intentional and self-monitored cognitive process that involves systematically interpreting information, analyzing components, and evaluating both evidence and contextual elements. These skills are essential for the problem-solving mindset. In the context of information security education, students regularly engage in discussions, challenging others' ideas, and approaches to problem-solving (Clarke & Konak, 2025). In a case study, critical thinking involves more than simply analyzing the incident; it requires students to challenge underlying assumptions, assess the validity of evidence, and develop logical, well-reasoned solutions. Throughout this process, students consistently apply analytical thinking and adapt their strategies, thereby demonstrating and strengthening their critical thinking abilities as they work through complex problems (Anderson et al., 2024).

Critical thinking skills and knowledge are generally considered in six dimensions: interpretation, analysis, evaluation, inference, explanation, and self-regulation (Facione, 1990). In the case study of information security, interpretation involves understanding the scenario, defining the problem, and recognizing the stakeholders, systems, and security controls involved. Analysis enables students to analyze the situation, break down the attack chain, examine vulnerabilities, and assess security defenses (Mukherjee et al., 2024). Evaluation involves evaluating evidence, verifying data, and assessing impact and biases (Grover & Pea, 2013). Inference allows students to brainstorm possible solutions, compare alternatives, and predict outcomes (Zimmerman, 2002). Explanation involves decision-making, choosing the best action, and considering ethics and compliance. Finally, self-regulation involves reflecting and improving. This allows students to review mistakes, document lessons learned, and ensure continuous improvement and adaptability (Zimmerman, 2002).

Generative AI (GenAI) technologies like ChatGPT have proven effective in diverse academic fields, performing tasks like encouraging students to question and refine their solutions, creating knowledge-based course content, supporting coding exercises in Java and Python, and offering feedback for learners (Elkhodr & Gide, 2025; Michel-Villarreal et al., 2023). Information security education is especially well-suited for GenAI integration, as it demands both theoretical understanding and hands-on implementation. Students must evaluate regulatory standards, craft security policies, and respond to evolving cyber threats, i.e., tasks that benefit from GenAI-assisted analysis but still necessitate human judgment to ensure precision and applicability (Al-Hawawreh et al., 2023; Balogh et al., 2024; Cao et al., 2025).

The extensive body of literature on GenAI technologies in information security education has documented various advancements; however, several notable gaps persist. Firstly, there is a limited amount of research that specifically investigates the direct impact of GenAI models, such as ChatGPT, on cybersecurity education and curriculum development. Most existing studies have focused broadly on AI, primarily emphasizing earlier technologies like machine learning and data mining (Khan et al., 2024). These studies have explored themes such as personalized learning, adaptive systems, and automated assessments, but they have largely overlooked the distinct capabilities and challenges introduced by GenAI tools. Secondly, there is a paucity of literature addressing how GenAI is integrated with case study pedagogy to promote students' critical thinking and problem-solving skills in the context of information security education. Educators in cybersecurity face the challenge of designing activities that encourage learning through trial and error, while striking the right balance between providing sufficient guidance and fostering independent problem-solving (Ibrahim & Ford, 2023).

This study seeks to bridge these gaps by offering a more in-depth exploration of the educational implications of GenAI, while also analyzing

students' responses and case study developments in the context of these emerging tools. Drawing upon the literature review and the gaps identified in existing research, this work seeks to explore the following research questions:

RQ1: In what ways can GenAI tools be integrated into information security education to strengthen students' critical thinking and their ability to apply knowledge in practical case analysis?

RQ2: How does the use of GenAI tools improve students' critical thinking skills?

By systematically assessing the results of the proposed approach, the study establishes a transferable model for integrating GenAI in the information security curriculum. It serves as a practical reference for educators aiming to leverage AI as a pedagogical tool while maintaining academic rigor and fostering critical thinking.

2. RELATED WORK

Impact of GenAI on Information Security

The transformative capabilities of GenAI—particularly large language models (LLMs) like ChatGPT, image generators, and code synthesis tools, are reshaping the information security landscape, offering innovative solutions for detecting, analyzing, and mitigating security threats (Marquardson, 2024; Shepherd, 2025). Generative AI represents a paradigm shift in both the offensive and defensive dimensions of information security. On the positive side, GenAI enhances threat detection and analysis by enabling systems to recognize complex attack patterns and process large volumes of data more efficiently. It can generate summaries of incidents, analyze logs using natural language understanding, and assist in identifying anomalies that may indicate security breaches (Grover et al., 2023; Metta et al., 2024). Additionally, it supports the automation of defensive measures, such as generating scripts and configurations based on specific threat models, and is being increasingly integrated into Security Orchestration, Automation, and Response (SOAR) platforms to improve response times and accuracy (Metta et al., 2024). GenAI also contributes significantly to cybersecurity training and simulation (Mohawesh et al., 2025). It can create realistic phishing emails, simulated malware, and various attack scenarios, all of which are valuable for red teaming and awareness training without exposing organizations to actual threats. Furthermore, it aids in code and configuration auditing by helping developers identify vulnerabilities in source code or configuration files, often explaining risks in clear, natural language.

Despite these advantages, GenAI introduces a range of security risks. One of the most concerning issues is the automated generation of malware and exploits. Malicious actors can use AI tools to craft polymorphic malware or conceptualize zero-day attacks (Metta et al., 2024). These tools lower the technical barrier for inexperienced attackers, allowing them to generate sophisticated malicious code without advanced expertise. Social engineering and phishing attacks also become more dangerous with the help of GenAI, as it enables the creation of highly personalized, grammatically correct, and context-aware messages, as well as deepfake audio and video content that can convincingly impersonate individuals (Al-Hawawreh et al., 2023).

Data leakage is another significant risk. When organizations interact with AI models—particularly via public APIs—there is potential for inadvertent exposure of sensitive or proprietary information. Furthermore, model inversion attacks may extract confidential data from AI systems that have been trained on private datasets (Okdem & Okdem, 2024). In addition, GenAI can facilitate the evasion of traditional security controls. It can produce obfuscated or encoded malicious content that bypasses intrusion detection systems, firewalls, or other filtering mechanisms, and can adapt dynamically to different environments, undermining static or signature-based defenses (Okdem & Okdem, 2024).

GenAI in Information Security Education

GenAI enhances personalized learning by enabling tailored explanations, real-time tutoring, and adaptive assessments. Students can interact with AI models to clarify difficult concepts such as risk management frameworks, access control models, and compliance requirements (e.g., ISO 27001, NIST, GDPR), receiving instant feedback and examples relevant to their learning pace and context (Bukar et al., 2024; Crabb et al., 2024). Second, GenAI facilitates scenario-based learning and simulations (Elkhodr & Gide, 2025). Instructors can use GenAI to create dynamic case studies, threat models, and incident response simulations that reflect realistic, evolving attack scenarios. These AI-generated exercises can cover a wide range of topics, such as phishing campaigns, insider threats, or ransomware incidents, helping learners practice analytical thinking and decision-making in a safe

environment. Third, GenAI supports content creation and curriculum development (Elkhodr & Gide, 2025). Educators can generate instructional materials, quiz banks, lab exercises, and policy templates efficiently. This not only reduces preparation time but also allows for the rapid updating of content to reflect emerging threats and technologies (Elkhodr & Gide, 2025).

Additionally, GenAI is a useful tool for ethical and critical thinking discussions. It can be used to demonstrate how attackers might misuse AI for malicious purposes, such as generating social engineering scripts or deepfakes, thereby sparking dialogue about responsible AI use, data protection, and legal implications (Mathews et al., 2025).

However, integrating generative AI into information security education also requires caution. There is a risk of students relying too heavily on AI without fully understanding the underlying concepts. Furthermore, the use of GenAI tools must be framed within clear academic integrity policies to prevent misuse, such as plagiarism or unauthorized code generation during assessments (Laato et al., 2020; Michel-Villarreal et al., 2023).

Case Study for Information Security Education

The use of case studies in information security education has become increasingly valuable as a pedagogical tool for bridging theoretical knowledge with practical application (Anderson et al., 2024).

One of the primary benefits of employing case studies is their ability to contextualize abstract security concepts. Topics such as risk assessment, incident response, regulatory compliance, access control, and governance frameworks are often difficult for students to fully grasp through lectures or textbook examples alone (Blanken-Webb et al., 2018; Cai, 2018). Case-based learning situates these concepts in realistic organizational settings, allowing learners to explore how theoretical models apply in practice. Moreover, case studies foster active learning (Cai, 2018; Marquardson, 2024). Instead of passively receiving information, students engage in discussions, analyze evidence, and evaluate alternative strategies. This interaction encourages deeper comprehension and the retention of complex information. For instance, analyzing a case involving a data breach can lead students to consider the interplay between technical controls, user behavior, and management decisions,

thereby promoting a holistic understanding of cybersecurity. Case studies also serve to cultivate ethical awareness and policy literacy (Garcia & Inoue, 2024). By examining incidents involving insider threats, compliance failures, or controversial surveillance practices, learners can critically assess legal and ethical dimensions of security decision-making, which is particularly important in a domain where professionals must balance technical effectiveness with privacy rights, legal obligations, and organizational values (Mukherjee et al., 2024; Shivapurkar et al., 2020).

Additionally, case studies support interdisciplinary learning. Information security spans multiple domains— technical, managerial, legal, and behavioral (Mathews et al., 2025; McDonald et al., 2019; Shepherd, 2025). A well-designed case can integrate perspectives from all these areas, encouraging students to synthesize diverse forms of knowledge (Tagarev, 2019). This is particularly useful for graduate-level education or professional development courses, where learners often come from varied backgrounds.

3. METHODOLOGY

This study aims to propose a structured framework for utilizing GenAI tools in information security courses, demonstrating how such technologies can be leveraged to sharpen learners' critical thinking and problem-solving skills. The implementation strategy unfolds in two structured phases. In the first phase, GenAI is incorporated into initial exercises, prompting students to evaluate AI-generated content, assess its validity, and enhance it through independent research and verified sources. This active engagement shifts learning from passive acceptance to critical analysis, reinforcing cybersecurity principles through hands-on scrutiny. The second phase integrates GenAI tools into formal case study assessment, challenging students to adapt AI-produced outputs to real-world cybersecurity situations while refining their work to meet industry and regulatory requirements. To solidify learning, reflective exercises are embedded, requiring students to compare different GenAI tools, evaluate GenAI's role in the case study process, its strengths, and its constraints.

This study was conducted in a graduate-level information security course at a Midwest public university, where one of the primary learning objectives was to prompt students to develop critical thinking and problem-solving skills. This study was built upon a case study in-class

assignment as shown in Appendix A. The assignment required group work, and the total class time was 6 hours over two weeks, with classes on Monday, Wednesday, and Friday (each lasting one hour). The main components of the assignment are summarized below.

No.	Case Title	Case Reference Link
1	ViaSat Attack in Ukraine	https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/ cases/viasat
2	Florida International University Ransomware Attack	https://www.scworld.com/brief/florida-international-university-attacked-by-blackcat-ransomware
3	Rockstar Games Data Breach	https://www.securityweek.com/rockstar-games-confirms-breach-leading-gta-6-leak/
4	A massive DDoS attack takes down Israeli government websites	https://www.timesofisrael.com/government-sites-crash-after-massive-cyberattack-officials-say/
5	Synnovis Healthcare breach in June 2024	https://www.webopedia.com/technology/biggest-cyber-attacks-2024/
6	What Caused the Uber Data Breach in 2022?	https://www.upguard.com/blog/what-caused-the-uber-data-breach
7	South Korea says DPRK hackers stole spy plane technical data	https://www.bleepingcomputer.com/news/security/south-korea-says-dprk-hackers-stole-spy-plane-technical-data/
8	Colonial Pipeline Ransomware Attack	https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
9	Attack on Saudi Aramco	https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
10	Data of More than 200 Million Twitter Users is Leaked	https://purplesec.us/breach-report/twitter-data-leak-200-million-users/
11	Iranian hackers breached a New York dam in 2013	https://www.ciodive.com/news/iranian-hackers-breached-new-york-dam-in-2013-wsj/411310/
12	Ransomware Breach Disrupted Indonesia Immigration	https://www.sangfor.com/blog/cybersecurity/ransomware-breach-disrupted-indonesia-immigration-and-other-government-services
13	Polycab targeted by ransomware attack	https://www.financialexpress.com/business/industry-polycab-targeted-by-ransomware-attack-company-says-core-systems-and-operations-not-impacted-3432321/
14	WazirX Cryptocurrency Exchange Loses $230 Million in Major Security Breach	https://thehackernews.com/2024/07/wazirx-cryptocurrency-exchange-loses.html

Table 1: The Case Pool for the In-class Assignment

For this in-class assignment, students were required to collaborate in groups to conduct a comprehensive analysis of a historical cyber incident using the Motivation-Methods-Resources-Impact-Solutions (MMRIS) framework adapted from the MMRI model (University of Washington, n.d.).

In phase one (2 class hours), students learned the MMRIS framework and used it to dissect the attack in terms of the attacker's motivation, the methods employed, the resources utilized, the impact of the incident, and the solutions suggested. Then, students practiced prompting two GenAI tools - ChatGPT and Gemini. The prompt must use the MMRIS framework in a cyberattack case. This practice was an iterative process that included a cycle of initializing a prompt, analyzing the output, and refining the prompt.

The second phase (4 class hours) involved randomly drawing and thoroughly reviewing a real-world cyber incident from the case pool (Table 1). Students then applied the MMRIS framework as they had learned in phase one. Again, students must engage with two generative AI tools, such as Gemini and ChatGPT, by prompting them to analyze the chosen case and compare the resulting outputs. Based on this comparison, each group would develop and present its own analysis using the MMRIS model.

After completing their case analysis, students gave a presentation to their classmates. They then submitted a final reflection, which included

the evidence of learning promised in their proposal, as well as insights into their learning experience.

Throughout the assignment, students were encouraged but not limited to use ChatGPT and Gemini in two phases. They could choose Grok, DeepSeek, Claude, or other models. They were instructed to cite ChatGPT and Gemini in both their initial learning plans and final reflections whenever they directly quoted its outputs. The instructor also demonstrated ChatGPT usage in class and provided examples highlighting instances of incorrect responses from the tool.

Once the final reflection was submitted, students were invited to participate in the study, which aimed to inform future classroom discussions. Participation was voluntary, with no course credit or other incentives offered. The study involved completing a single survey featuring both quantitative and qualitative questions. Survey prompts are detailed in the results section. Students also had the option to upload ChatGPT and Gemini chat logs.

No personal identifying information was collected unless a student chose to upload their logs. These logs compromised full anonymity due to filenames containing student names and the uniqueness of each student's topic, which could link the log to an individual.

4. RESULTS

In total, 191 students, divided into 32 groups (six students for 31 groups and five students for the last group), submitted the case study assignment, and all 191 students completed the reflection survey.

In phase one, students reported the count of how many times they refined the prompt based on applying the MMRIS framework (at least five prompts). As shown in Figure 1, the range of refining times is from 15 to 46 for all 32 groups. Group 24 refined the least — 15 times, and Group 19 refined the most — 46 times. The average number of refining times is 32, approximately 6 refinements per query.
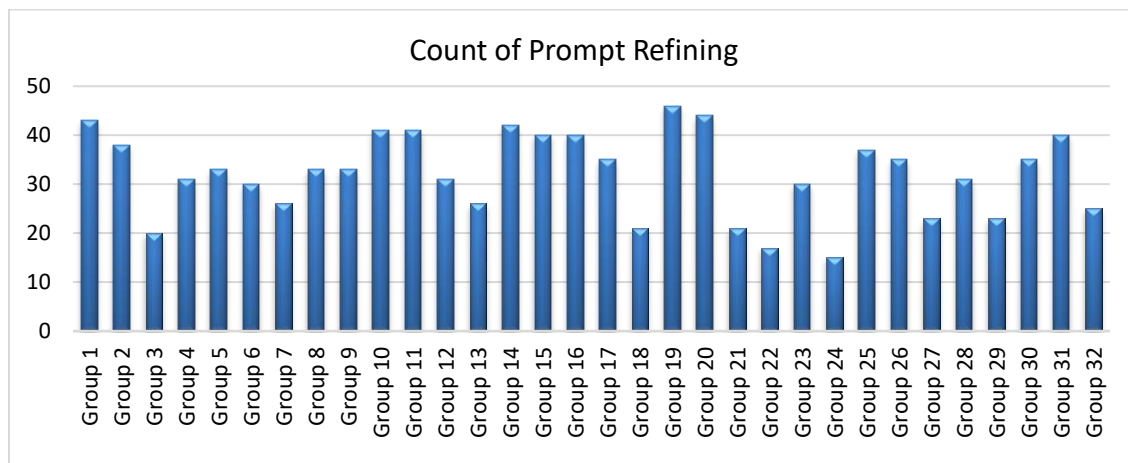

Figure 1. The Count of Prompt Refining

In phase two, students reported comparing their preferences for ChatGPT and Gemini when applying the MMRIS framework to the case study assignment. Figure 2 illustrates the overall group preferences: 72% of groups prefer ChatGPT, while 28% prefer using Gemini (chi-square $\chi^2 = 6.125, p < 0.05$, suggesting a clear preference between the two options presented). Moreover, as shown in Figure 3, student groups prefer using ChatGPT versus Gemini on the analysis of attack motivation by a ratio of 18:14, attack methods 16:16, attack resources 22:10, attack impact 17:15, and suggested solutions 21:11. The ANOVA results revealed significant differences among the groups ($F(df1, df2) = 11.701, p <$ 0.05), and the post-hoc tests identified which specific group comparisons were statistically different.
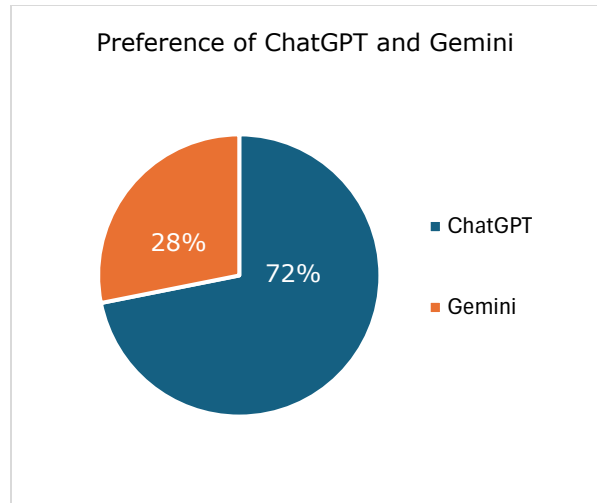
Figure 2. Student Group Preferences of ChatGPT and Gemini
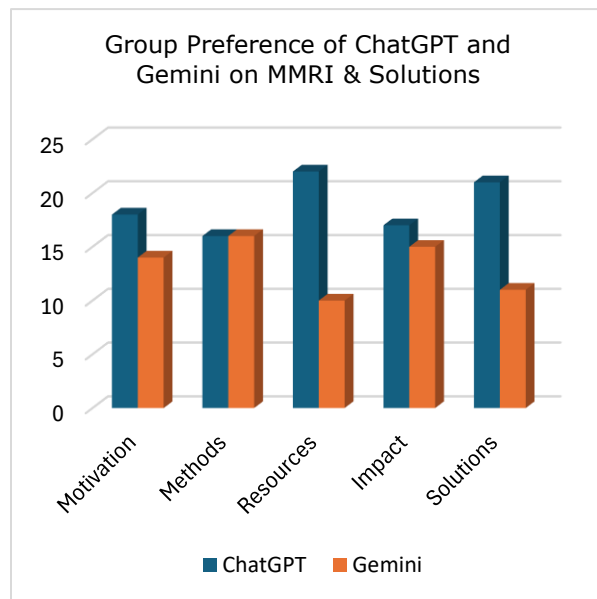
Figure 3. Student Group Preference of ChatGPT and Gemini on MMRI & Solutions

At the end of phase two, a questionnaire survey was completed to gather feedback on the impact of GenAI tools on critical thinking and problem-solving skills. The survey includes 17 questions with a 5-point Likert scale (1=Strongly Disagree, 5=Strongly Agree) covering seven aspects. The survey questions focus on the reflection of six dimensions (Clarke & Konak, 2025) of critical thinking and the intention of using GenAI. A total of 191 feedback responses from students were collected and analyzed. Table 2 shows the survey report.

#	Question	Mean	SD
1	GenAI can learn the MMRIS framework fairly	3.3	0.9
2	GenAI helps me understand the cyber incident scenario and learn the problems	2.9	0.5
3	GenAI helps me recognize the stakeholders, systems, and security controls involved.	3.7	0.6
4	GenAI can help me analyze the attack chain and the situation when an incident occurs.	3.1	0.4
5	GenAI can examine the vulnerabilities in the incident case	4.2	0.5
6	GenAI can help me evaluate the evidence and verify the data provided in the incident case	2.8	0.6
7	GenAI can help me assess the impact on individuals, organizations, and society	3.9	0.4
8	GenAI can suggest possible solutions and predict outcomes	4.6	0.5
9	GenAI helps me consider different perspectives when finding solutions	4.5	1.5
10	GenAI can provide comments on choosing the best action	3.5	1.4
11	GenAI can help me consider ethics and compliance	3.9	1.6
12	GenAI helps me document lessons learned from the incident cases	2.8	1
13	GenAI encourages me to ask deeper or more refined questions	3.1	0.9
14	GenAI helps me identify gaps or overlooked factors in our case study processes	2.4	1.5
15	Overall, GenAI was a valuable tool for enhancing my critical thinking skills	4.1	0.6
16	I would recommend the use of GenAI in future information security case studies or similar assignments	4.7	0.6
17	I have the intention of using GenAI ethically in my future professional practice	4.9	0.7

Table 2. Helpfulness of GenAI on Critical Thinking and Intention of Adoption

As shown in Figure 4, in the six dimensions of critical thinking, students perceived that GenAI tools have a good performance on five dimensions, especially on inference (providing possible solutions, scoring 4.55). The worst

performance is on self-regulation, with a score of 2.77. Additionally, the intention to adopt GenAI is high, with a score of 4.57.
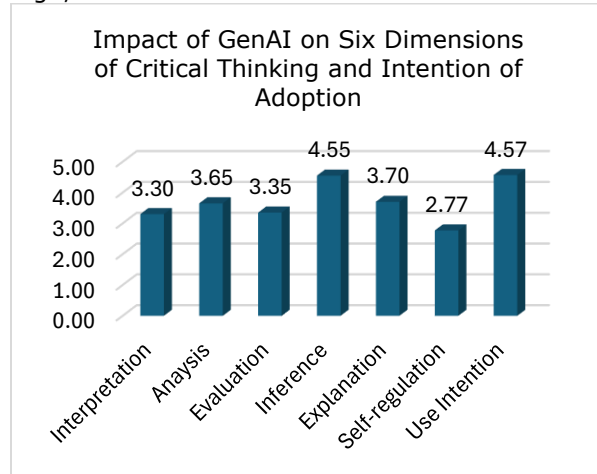
Figure 4. Impact of GenAI on Six Dimensions of Critical Thinking and Intention of Adoption

5. DISCUSSION

Overall, the results suggest that GenAI tools can enhance students' critical thinking skills and support structured analysis using the MMRIS framework in information security case studies; however, despite the high intention to use GenAI tools, students must be aware of potential inaccuracies and ethical issues.

In phase one, students counted the prompt refining times and compared the outputs based on the word changes. All students agreed that refining prompts when using GenAI tools was crucial because the quality of the input (prompt) directly determined the quality of the output (response). However, there is no evidence in our study to show a positive relationship between the refining times and students' satisfaction with the output. It could be a direction for future research.

In phase two, students applied ChatGPT and Gemini with the MMRIS model to case studies and compared the outputs. The results show that students preferred ChatGPT over Gemini with a ratio of 72% to 28%. Additionally, ChatGPT outperformed Gemini in analyzing attack motivation, resources, and impact, as well as in providing possible solutions; however, it tied with Gemini in analyzing attack methods.

"ChatGPT provided a broader perspective, focusing on motivations and methods. Its analysis included high-level recommendations for financial and reputational recovery."

"ChatGPT can be a great tool for generating general information and overviews, especially when needing fast answers on common topics."

"ChatGPT is useful for providing business-focused insights, such as explaining how companies handle crises, respond to threats, and manage operational continuity."

"Our team found ChatGPT to be more user-friendly for broad brainstorming, while Gemini excelled in detailed and actionable insights."

"Gemini suits formal, in-depth needs; ChatGPT offers flexible, quick insights adaptable to follow-up questions."

"Gemini excels in delivering detailed, technical information, especially about the methods and tools used by attackers."

"Gemini offered detailed operational insights and practical steps for mitigating risks. It emphasized post-attack recovery strategies and operational continuity measures."

The above students' feedback affirms the results. ChatGPT is more user-friendly for providing broad and summarized analysis, more efficient for interacting with users' natural language prompts, more effective for engaging the cyber incident contexts, and more concise for organizing related concepts in the responses. Gemini provides more granular, technical breakdowns and organizes responses into detailed subcategories. Moreover, the survey analysis reveals that GenAI significantly enhances the processes of interpretation, analysis, evaluation, inference, and explanation, but performs poorly in self-regulation. Affirmatively, all students agree that both ChatGPT and Gemini help users develop critical thinking and problem-solving skills.

Based on the analysis and discussion of the survey and students' feedback, we propose a conceptual framework that integrates GenAI tools, critical thinking, and the MMRIS framework to support the analysis of cybersecurity case studies.
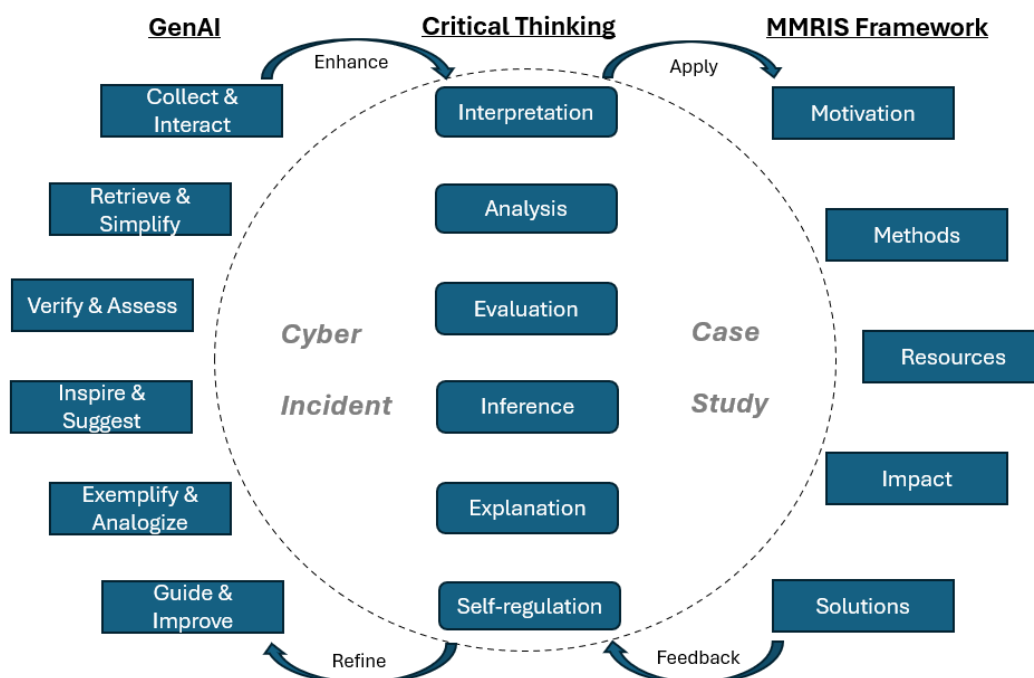
Figure 5. A Conceptual Framework

As shown in Figure 5, at the center of the diagram is the case of a cyber incident, which serves as the focal point for applying both technological and cognitive tools in an educational context. On the left side of the diagram, GenAI tools, such as ChatGPT, Gemini, or similar models, play a supporting role by offering a variety of cognitive and assistive functions. These tools enable users to collect and interact with information, retrieve and simplify complex data, verify the credibility of sources, generate suggestions, provide examples and analogies, and guide users toward continuous improvement. These functionalities contribute to enhancing and refining students' critical thinking processes throughout the case analysis. Critical thinking itself is situated at the core of the framework, depicted as a sequence of interconnected cognitive activities. These include interpretation, analysis, evaluation, inference, explanation, and self-regulation. These thinking processes are not isolated; they are supported and enriched by GenAI's capabilities, which offer feedback and opportunities for iterative improvement. On the right side of the diagram lies the MMRIS framework, comprising motivation, methods, resources, impact, and solutions, which provides a structured approach to dissecting and understanding the selected cybersecurity incident. Through the application of critical thinking skills, students are encouraged to examine why the incident occurred, how it was executed, what tools were involved, what effects

it had, and how the situation was or could be resolved.

The framework also highlights the dynamic interaction between these components. GenAI tools enhance critical thinking, which in turn supports the application of the MMRIS framework to the case study. The process includes a feedback loop where self-regulation, supported by AI guidance, leads to refined analysis and deeper learning. Overall, the framework emphasizes how the integration of GenAI, structured analytical models, and critical thinking skills can significantly enrich students' ability to interpret, evaluate, and respond to real-world cybersecurity challenges.

6. CONCLUSIONS

This study sheds light on how GenAI tools can be utilized to enhance learning in the field of information security. We propose a structured framework for incorporating GenAI into cybersecurity education, highlighting its ability to improve critical thinking and hands-on problem-solving skills. The framework illustrates a pedagogical model for teaching cybersecurity through case-based learning. It emphasizes how GenAI tools, when integrated with critical thinking skills and a structured analytical framework (MMRIS), can enhance students' abilities to understand and respond to complex cyber

incidents. This approach provided students with immersive, practical experience in AI-driven cybersecurity strategies.

Using a case-study-centered pedagogical approach, the study illustrates how GenAI can enhance students' critical thinking in six dimensions. The findings reveal that GenAI significantly accelerates understanding of the scenarios, allowing students to dedicate more time to evaluating, refining, and ensuring compliance with industry standards and regulations. The proposed case analysis method supported by GenAI can be adapted to disciplines beyond security education, reinforcing the generalizability of the pedagogical model.

This study has several limitations that warrant consideration. First, the findings are based on a single academic term and a relatively small student group. Thus, the effectiveness of the proposed framework may vary across different information security curricula and different institutions. Second, the study did not set a control group to compare with and without GenAI integration across different sections or semesters. Third, the research did not objectively assess students' ability to identify inaccuracies in AI-generated content. Future studies should address this gap by examining how detection capabilities vary between novice and advanced learners, thereby exploring potential correlations between skill level and discernment of AI-generated misinformation. Further, future research should investigate the long-term effects on student skill development, adaptive GenAI-learning frameworks, and scalable methods for integrating GenAI into cybersecurity education programs.

7. REFERENCES

Al-Hawawreh, M., Aljuhani, A., & Jararweh, Y. (2023). Chatgpt for cybersecurity: Practical applications, challenges, and future directions. *Cluster Computing*, *26*(6), 3421–3436. https://doi.org/10.1007/s10586-023-04124-5

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. *Information & Management*, *61*(7), 104015. https://doi.org/10.1016/j.im.2024.104015

Balogh, Š., Mlynček, M., Vraňák, O., & Zajac, P. (2024). Using Generative AI Models to Support Cybersecurity Analysts. *Electronics*, *13*(23), 4718. https://doi.org/10.3390/electronics1323471 8

Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N. C., Campbell, R. H., & Bashir, M. (2018). *A Case Study-based Cybersecurity Ethics Curriculum*. 2018 USENIX Workshop on Advances in Security Education (ASE 18). https://www.usenix.org/conference/ase18/p resentation/blanken-webb

Bukar, U. A., Sayeed, Md. S., Fatimah Abdul Razak, S., Yogarayan, S., & Sneesl, R. (2024). Decision-Making Framework for the Utilization of Generative Artificial Intelligence in Education: A Case Study of ChatGPT. *IEEE Access*, *12*, 95368–95389. https://doi.org/10.1109/ACCESS.2024.3425 172

Cai, Y. (2018). Using Case Studies To Teach Cybersecurity Courses. *Journal of Cybersecurity Education, Research and Practice*, *2018*(2). https://doi.org/10.62915/2472-2707.1041

Xiao, H., Shah, B., Spring, J., Kuzminykh, I., & Janku, S. (2025). Scaffolding Student Learning through GenAI in Cybersecurity Education. In *The 3rd International Workshop on Cyber Security Education for Industry and Academia (CSE4IA 2025), Munich, Germany*.

Clarke, C. J. S. F., & Konak, A. (2025). The Impact of AI Use in Programming Courses on Critical Thinking Skills. *Journal of Cybersecurity Education, Research and Practice*, *2025*(1). https://doi.org/10.62915/2472-2707.1220

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A Critical Review of Cybersecurity Education in the United States. *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, 241–247. https://doi.org/10.1145/3626252.3630757

Elkhodr, M., & Gide, E. (2025). *Integrating Generative AI in Cybersecurity Education: Case Study Insights on Pedagogical Strategies, Critical Thinking, and Responsible AI Use* (arXiv:2502.15357). arXiv. https://doi.org/10.48550/arXiv.2502.15357

Facione, P. A. (1990). *Critical Thinking: A Statement of Expert Consensus for Purposes of Educational Assessment and Instruction. Research Findings and Recommendations*. https://eric.ed.gov/?id=ED315423

Garcia, C., & Inoue, S. (2024). Relabeling for Indoor Localization Using Stationary Beacons

in Nursing Care Facilities. *SENSORS*, *24*(2). https://doi.org/10.3390/s24020319

Grover, S., Broll, B., & Babb, D. (2023). Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, 980–986. https://doi.org/10.1145/3545945.3569750

Grover, S., & Pea, R. (2013). Computational thinking in K–12: A review of the state of the field. *Educational Researcher*, *42*(1), 38–43. https://doi.org/10.3102/0013189X12463051

Khan, M. I., Arif, A., & Khan, A. R. A. (2024) The Most Recent Advances and Uses of AI in Cybersecurity. Jurnal Multidisiplin Ilmu, vol. 3, no. 4, 2024, pp. 566-578.

Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020). AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs. *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, 6–10. https://doi.org/10.1109/ICALT49669.2020.00009

Marquardson, J. (2024). Embracing Artificial Intelligence to Improve Self-Directed Learning: A Cybersecurity Classroom Study. *Information Systems Education Journal*, *22*(1), 4–13.

Mathews, N., Schwartz, C., & Wright, M. (2025). Teaching Generative AI for Cybersecurity: A Project-Based Learning Approach. *Journal of The Colloquium for Information Systems Security Education*, *12*(1), Article 1. https://doi.org/10.53735/cisse.v12i1.211

Mcdonald, J., Hansen, D., Balzotti, J., Tanner, J., Winters, D., Giboney, J., & Bonsignore, E. (2019). *Designing Authentic Cybersecurity Learning Experiences: Lessons from the Cybermatics Playable Case Study*. http://hdl.handle.net/10125/59689

Metta, S., Chang, I., Parker, J., Roman, M. P., & Ehuan, A. F. (2024). *Generative AI in Cybersecurity* (arXiv:2405.01674). arXiv. https://doi.org/10.48550/arXiv.2405.01674

Michel-Villarreal, R., Vilalta-Perdomo, E., Salinas-Navarro, D. E., Thierry-Aguilera, R., & Gerardou, F. S. (2023). Challenges and Opportunities of Generative AI for Higher Education as Explained by ChatGPT. *Education Sciences*, *13*(9), Article 9. https://doi.org/10.3390/educsci13090856

Mohawesh, R., Ottom, M. A., & Salameh, H. B. (2025). A data-driven risk assessment of cybersecurity challenges posed by generative AI. *Decision Analytics Journal*, *15*, 100580. https://doi.org/10.1016/j.dajour.2025.100580

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, *15*(2), Article 2. https://doi.org/10.3390/info15020117

Okdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences*, *14*(22), Article 22. https://doi.org/10.3390/app142210487

Shepherd, C. (2025). *Generative AI Misuse Potential in Cyber Security Education: A Case Study of a UK Degree Program* (arXiv:2501.12883). arXiv. https://doi.org/10.48550/arXiv.2501.12883

Shivapurkar, M., Bhatia, S., & Ahmed, I. (2020). Problem-based Learning for Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education*, *7*(1), Article 1.

Tagarev, N. (2019). *Role of Case Study Analyses in Education of Cybersecurity Management*. Proceedings of the 13th International Multi-Conference on Society, Cybernetics and Informatics (IMSCI 2019), pp.61-64.

University of Washington. (n.d.). *The Security Cards: A Security Threat Brainstorming Kit*. Retrieved June 7, 2025, from https://securitycards.cs.washington.edu/

Zimmerman, B. J. (2002). Becoming a Self-Regulated Learner: An Overview. *Theory Into Practice*, *41*(2), 64–70. https://doi.org/10.1207/s15430421tip41022

APPENDIX A

The Group Assignment of Case Study with GenAI

In this class work, you need to work with your group members to complete the following tasks:

1. Go through a case of a cyber incident that occurred in the past.

2. Learn and apply the Motivation-Methods-Resources-Impact-Solutions (MMRIS) framework to the cyber incident case.

   MMRIS materials are linked under Module 12 on the course site.

3. Prompt two generative AI tools (Gemini, ChatGPT, Grok, Claude, etc.) using MMRIS and present the outputs.

4. Compare the output difference between two AI tools.

5. Propose your own analysis based on MMRIS.

6. Address what you have learned about using Gen-AI tools for this case study.

At the end of Monday's class, you must submit at least 15 PowerPoint slides covering the above topics.

You will do a class presentation on Wednesday and Friday's classes.

Here is the rubric:

44652 - Group Case Study Presentation Scoring Guide Section No:

Group Names (First name Last name)	M1:		M4:	
	M2:		M5:	
	M3:		M6:	

	Case Title:	Total Points	Points Awarded
Group Asssesment	1) Title slide contains team name and team members, total >12 slides	1	
	2) Case Introduction	2	
	3) ChatGPT prompt and answers(motivation, methods, resources, impact)	4	
	4) Gemini prompt and answers (motivation, methods, resources, impact)	4	
	5) Comparison on two generative AI answers, differences?	4	
	6) What are your own analysis based on these AI tools (motivation, methods, resources, impact)?	5	
	7) What have you learned on how to use these AI tools?	5	
	Total	25	

		Total Points	M1	M2	M3	M4	M5	M6
Individual Assessment	Member time limits >1 minute	4						
	Team total time 8-10 minutes	2						
	Effective use of notes (note cards or paper notes)	4						
	Professionalism (appropriate gestures, posture, professional attire)	4						
	Eye contact	2						
	Voice control (pitch, rate, volume)	2						
	Appropriate pace of speech, interaction	2						
	Total	20	0	0	0	0	0	0