



Research Article

Development of Outcomes-Based Teaching and Learning AI-Enhance Cybersecurity Education Course Syllabus

Jessabel P. Alancado ^{1*}, Andrew C. Caronongan ²

¹⁻²Graduate School, University of Luzon, Master in Information Technology Program, University of Eastern Pangasinan.

ABSTRACT:

It cannot be ignored that Generative Artificial Intelligence (AI) has been a breakthrough in the field of higher education, providing opportunities to improve the processes of teaching, learning, and cybersecurity education. Given this, it is becoming increasingly vital to gain insight into the effect of Generative AI exposure on the acquisition of fundamental Information Technology skills by the learners. This research paper investigated the impact of Generative AI exposure on cybersecurity knowledge and skills, critical thinking skills, and ethical AI usage among third year Bachelor of Science in Information Technology (BSIT) students of University of Eastern Pangasinan. A quantitative descriptive-correlational type of study was done in combination with a developmental approach. Overall, there were 185 third year BSIT students who took part in the survey using a validated self-reporting questionnaire. The statistical tools such as the mean and standard deviation were used to measure their AI exposures and competencies, while Pearson product-moment correlation coefficient was used to determine the correlations between the variables. From the results, it can be seen that the subjects exhibited high knowledge of Generative AI tools and high levels of usage, while cybersecurity engagement was moderate. Cybersecurity skills and critical thinking skills were also at the moderate level, while responsible use of AI was at a high level. Correlation tests showed that there were statistically significant positive correlations between Generative AI experience and cybersecurity skills ($r = .874$), critical thinking skills ($r = .822$), and responsible use of AI ($r = .792$), where all correlations were significant at $p < .001$. From the findings, one can see that the more exposure to Generative AI the subject had, the better their technical, analytical, and ethical skills. Based on the above results, an AI-Enhanced OBTL Syllabus was formulated.

Keywords: Generative Artificial Intelligence, AI-Enhanced Outcomes-Based Teaching and Learning (OBTL) Syllabus, cybersecurity education, cybersecurity skills, critical thinking, responsible AI use.

Citation: Alancado, J. P., & Caronongan, A. C. (2026). Development of outcomes-based teaching and learning AI-enhanced cybersecurity education course syllabus. Nexus Global Research Journal of Multidisciplinary, 2(8), 409–416.

INTRODUCTION:

The quick advancement in the field of Generative Artificial Intelligence (AI) has brought a change in higher education in the form of redefining teaching and learning methods, assessments, and problem-solving techniques. The use of AI tools such as ChatGPT, Google Gemini, and GitHub Copilot enables students to create content, program codes, perform analysis in cybersecurity cases, and get feedback instantly, which increases the efficiency of learning. With the increasing integration of technology into education, there is potential for using Generative AI to improve cybersecurity education by cultivating technical skills, critical thinking skills, and responsible use of AI. The educational benefits of Generative AI depend on its integration into the curriculum for

educational purposes other than just being a productivity tool (OECD, 2023; UNESCO, 2023).

While there has been an increasing implementation of Generative AI in higher education, many higher education institutions, especially provincial universities in the Philippines, still do not have curriculums that include the use of AI in cybersecurity education. Current instruction methods are deficient in constructive alignment between ILOs, TLAs, ATs, and responsible AI practice. Therefore, students will be deprived of the opportunity to effectively use Generative AI in cybersecurity education in an academically honest manner.

STATEMENT OF THE PROBLEM:

This study aimed to develop an Outcomes-Based Teaching and Learning (OBTL) framework-

*Corresponding Author: Jessabel P. Alancado

Received: 06 July 2026 | Accepted: 2 Aug 2026 | Published: 11 Aug 2026

Copyright © 2026 The Author(s): This work is licensed under a Creative Commons Attribution- Non-Commercial-No Derivatives 4.0 (CC BY-NC-ND 4.0) International License

based AI-Enhanced Cybersecurity education course syllabus for the IT students of the University of Eastern Pangasinan towards quality IT education.

Specifically, it sought to answer the following questions:

1. What is the level of exposure to generative AI tools among BSIT students in terms of:
 - a. Familiarity;
 - b. Frequency of use; and
 - c. engagement in cybersecurity-related tasks.
2. What is the level of student competencies in the use of generative AI tools along the following skill set:
 - a. cybersecurity skills;
 - b. critical thinking; and
 - c. responsible use?
3. What OBTL framework-based AI-Enhanced Cybersecurity Education Course Syllabus can be developed towards quality IT education?

Significance of the Study:

The present study is important since it forms the basis upon which an AI-Enhanced Outcomes-Based Teaching and Learning (OBTL) Cybersecurity Education Course Syllabus, promoting the responsible incorporation of Generative Artificial Intelligence (AI) within higher learning institutions, can be developed. The proposed syllabus is likely to contribute to the Information Technology instructors by creating a constructively aligned learning plan, improving the cybersecurity skills, critical thinking, and responsible application of AI among students, help academic administrators and the University of Eastern Pangasinan in the development of their courses and instructional plans, and be a resource for other researchers conducting studies on the subject matter.

MATERIALS AND METHOD:

Research Design

This study utilized a quantitative descriptive-correlational research design with a developmental element, involving a cross-sectional survey research design. The descriptive research design was used to establish the level of exposure of the respondents to Generative Artificial Intelligence

(AI) as well as the cybersecurity, critical thinking, and responsible use of AI competencies of the respondents. On the other hand, the correlational research design analyzed the relationship between the variables.

Respondents

The respondents were 185 third-year Bachelor of Science in Information Technology (BSIT) students studying at the University of Eastern Pangasinan for the academic year 2025-2026. The sample respondents were taken through convenience sampling from the targeted 355 respondents, which constitute about 52.1% of the total population. Sample size determination was done through Cochran's formula using 95% confidence level and 5% margin of error.

Data Collection

Data were gathered using a validated self-administered questionnaire that was disseminated via Google Forms. The questionnaire assessed five domains, namely: demographic profile, Generative AI exposure (awareness, frequency of usage, and participation in activities related to cybersecurity), cybersecurity abilities, critical thinking, and responsible utilization of AI through a five-point Likert scale. The questionnaire was first validated by three experts and then pilot-tested on 30 BSIT students who did not belong to the main group of participants. The internal consistency reliability was validated through Cronbach's alpha using IBM SPSS Statistics Version 27. Data gathering adhered to ethical guidelines, such as informed consent, voluntariness, confidentiality, anonymity, and proper data handling. Data were verified before statistical analysis.

Data Analysis

Descriptive statistics such as frequency, percentage, mean, and standard deviation were applied to portray the characteristics of the participants and determine the extent of their Generative AI exposure and skills. The Pearson Product Moment Correlation Coefficient was utilized in assessing the associations between Generative AI exposure and the participants' cybersecurity skills, critical thinking skills, and Responsible AI application skills. The results provided the empirical foundation for the creation of the proposed AI-Enhanced OBTL Cybersecurity Education Course Syllabus using the curriculum

development process based on the Rapid Application Development (RAD) model.

RESULTS AND DISCUSSION:

Results:

This chapter provides the results of the study based on the three refined research questions. These are presented in two main parts: Results and

Discussion. The Results part shows the statistical results via tables and descriptive analysis, while the Discussion part discusses the results within the context of the existing literature, theoretical framework, and the implications for AI-based cybersecurity education. The results were also the bases for formulating the OBTL syllabus for AI-based cybersecurity education.

1. Level of Exposure to Generative AI Tools

Table 5.1 Level of Familiarity with Generative AI Tools

Variable	n	Mean(M)	Standard Deviation (SD)	Verbal Interpretation
Familiarity with Generative AI Tools	185	3.41	0.85	High

Table 5.1 illustrates the level of knowledge of the respondents about Generative AI tools. The findings show that the respondents got an average score of 3.41 with a standard deviation of 0.85, which means that it is interpreted as High. This shows that the third-year BSIT students of the University of Eastern Pangasinan have a high level of familiarity with Generative AI tools. Moreover, it implies that they have adequate knowledge on the operations and functionalities of Generative AI. The high level of familiarity among the respondents also implies that the respondents have had prior exposure to AI technologies in relation to their studies, programming work, and other digital platforms.

In addition to this, the results indicate that the respondents have gained enough knowledge to

identify and use Generative AI as a learning tool. The standard deviation of 0.85 shows that there is a certain level of consistency in the degree of awareness among the respondents. This shows that even though each respondent might have had different experience with the use of AI tools, the level of knowledge and awareness on the tools is similar among most students. Consistency in the level of awareness may have been caused by the availability of popular AI tools. Availability of many popular AI tools, especially among Information Technology students who interact with technological devices in class can explain the similarity in the level of awareness among most students.

Table 5.2 Frequency of Use of Generative AI Tools

Indicator	Mean (M)	SD	Verbal Interpretation
Frequency of use	3.42	0.84	High

Table 5.2 contains the frequency of use of Generative AI tool among the respondents. Based on the analysis of data, the respondents scored an overall mean value of 3.42 with a standard deviation value of 0.84, which is verbally interpreted as High. This implies that the third-year Bachelor of Science in Information Technology (BSIT) students use Generative AI tools regularly in their educational and personal pursuits. The regularity in the use of AI technology indicates that the technology has

integrated into the lives of the students while undertaking assignments, brainstorming, solving programming problems, conducting research, and becoming more productive in different courses.

The relatively small value of the standard deviation shows that the respondents showed rather consistent behavior in using Generative AI tools, and that the frequent use of AI is typical among most of the participants. Such behavior can be explained by the ease and effectiveness provided by the AI applications

such as ChatGPT, Google Gemini, Microsoft Copilot, and GitHub Copilot. The results obtained prove that students already incorporate Generative AI in their

educational practices, which makes it possible to develop AI-aided learning approaches as well as cybersecurity learning activities.

Table 5.3 Engagement in Cybersecurity-related Activities Using Generative AI

Indicator	Mean (M)	SD	Verbal Interpretation
Engagement in Cybersecurity-related Activities Using Generative AI	3.16	0.78	Moderate

Table 5.3 represents the engagement level of the respondents in cyber security related activities through the use of Generative AI tools. From the results, it can be seen that the respondents had a mean score of 3.16 with a standard deviation of 0.78 which is verbally interpreted as Moderate. This implies that the third year Bachelor of Science in Information Technology (BSIT) students utilize Generative AI tools moderately for cybersecurity related activities. They might at times utilize the tools in analyzing cybersecurity concepts, comprehending network threats, coding programming scripts, identifying

system vulnerabilities, and solving security problems, though not regularly.

From the low standard deviation of 0.78, it can be observed that the respondents have shown fairly similar engagement levels in the use of AI for cybersecurity activities. In contrast to the high level of familiarity and usage of AI seen in the previous tables, it is evident that there exists a disparity between AI usage in general and AI application in cybersecurity related tasks. This implies that there is a need for enhancing AI based cybersecurity training through practical laboratory work, case based study, threat simulation and other experiential learning approaches.

2. Level of student competencies in the use of generative AI tools

Table 5.4 Summary of the Level of Student Competencies

Competencies	Mean (M)	SD	Verbal Interpretation
Cybersecurity Skills	3.31	0.87	Moderate
Critical Thinking Skills	3.37	0.93	Moderate
Responsible AI Use	3.44	1.04	High
Overall Student Competencies	3.37	0.95	Moderate

Table 5.4 shows the summary of respondents' level of student competencies on cybersecurity skills, critical thinking skills, and responsible use of AI. From the results, it is noted that the respondents had a moderate level of student competency in cybersecurity skills with a mean of 3.31 (SD = 0.87) and critical thinking skills with a mean score of 3.37 (SD = 0.93). However, the level of responsible use of AI had the highest mean score of 3.44 (SD = 1.04), which translates to High. The combination of all three competency measures resulted in a mean score of 3.37 (SD = 0.95), which was a Moderate level of student competencies.

The results indicate that the participants have adequate competency levels in all three areas measured with responsible AI usage being the most dominant area of strength. It implies that the students usually show adequate ethical and responsible behavior while using Generative AI technologies with satisfactory proficiency in cybersecurity skills and critical thinking. Nevertheless, the moderate level of overall competency implies that further improvements are necessary, especially in cybersecurity skills and critical thinking. The findings emphasize the necessity to use instructional intervention methods which involve practical experience with cybersecurity, problem-based learning and AI-based activities

3. OBTL framework-based AI-Enhanced Cybersecurity Education Course Syllabus can be developed

Table 5.5 Basis for the Development of the AI-Enhanced Outcomes-Based Teaching and Learning (OBTL) Syllabus

Research Findings	Curriculum Need	AI-Enhanced Syllabus Development
High level of familiarity with Generative AI tools (M = 3.41)	Students already possess foundational knowledge of AI technologies and require more advanced learning experiences.	Integrate advanced AI-assisted learning activities such as prompt engineering, AI-supported programming, cybersecurity research, and collaborative AI-based projects
High frequency of use of Generative AI tools (M = 3.42)	Students require structured and purposeful use of AI to maximize learning outcomes.	Incorporate AI-assisted classroom activities, guided laboratory exercises, AI-supported assignments, and formative assessments that promote productive AI utilization.
Moderate engagement in cybersecurity-related activities using AI (M = 3.16)	Students need greater exposure to authentic cybersecurity applications of AI.	Include cybersecurity threat simulations, vulnerability analysis, incident response exercises, secure coding activities, and AI-assisted penetration testing laboratories.
Moderate cybersecurity skills (M = 3.31)	Students require stronger technical competencies through experiential learning.	Design hands-on laboratory activities, practical cybersecurity exercises, capture-the-flag (CTF) activities, and AI-supported security analysis tasks aligned with course learning outcomes.
Moderate critical thinking skills (M = 3.37)	Students need opportunities to strengthen analytical reasoning and decision-making.	Integrate AI-supported case studies, cybersecurity problem-based learning, reflective discussions, threat investigation, and evidence-based decision-making activities.
High responsible AI use (M = 3.44)	Students should continuously reinforce ethical AI practices while applying AI in cybersecurity.	Embed AI ethics, responsible AI use, academic integrity, data privacy, cybersecurity ethics, and governance topics throughout the syllabus and assessment activities.

Table 5.5 Findings from the survey became the empirical basis for creating the AI-Enhanced Outcomes-Based Teaching and Learning (OBTL) Cybersecurity Education Course Syllabus. The findings revealed that the participants showed a high

level of familiarity with Generative AI tools (M = 3.41) and high levels of use of such tools (M = 3.42), which is evidence of enough basic knowledge and experience in working with AI technologies. Nevertheless, the level of participation in

cybersecurity activities was moderate ($M = 3.16$), which means that AI is not used in real cybersecurity activities. In addition, cybersecurity skills ($M = 3.31$) and critical thinking skills ($M = 3.37$) are moderate, whereas responsible AI use got a high score ($M = 3.44$). Based on these findings, curriculum needs and appropriate AI-enhanced teaching strategies were designed, including advanced AI-assisted learning activities, cybersecurity simulations, secure coding laboratories, AI-based case studies, problem-based learning, and responsible AI practices in the course syllabus. Thus, due to these findings, the creation of an AI-Enhanced Cybersecurity Education Course Syllabus based on OBTL approach became possible through constructive alignment of Intended Learning Outcomes (ILOs), Teaching-Learning Activities (TLAs), Assessment Tasks (ATs), learning resources, and responsible AI use.

Discussion:

1. Level of Exposure to Generative AI Tools

The study showed that BSIT students of the third year had an average level of exposure to Generative AI tools, where the high level of familiarity and frequency of use but only average level of engagement in cybersecurity activities were observed. These findings imply that while students easily adopted Generative AI in common academic activities, they rarely used it for their cybersecurity purposes. These findings support the Constructivist Learning Theory, which implies that learning happens through real-life experiences, so mere familiarity and use of the tool are not enough for the development of specific skills and knowledge. At the same time, the results can be explained by the Technology Acceptance Model (TAM), according to which students keep using the technology because of its ease of use and utility; however, instruction is necessary to motivate them to use AI in cybersecurity.

2. Level of Students' Competencies in Generative AI Tools Use

In terms of general competencies, respondents had moderately high level of cybersecurity skills and critical thinking and highly satisfactory level of responsible AI use. The results reveal that students have satisfactory technical and analytical competencies but need more practice in practical cybersecurity skills and higher order

thinking skills development. The high level of responsible AI use is associated with awareness of ethical concepts, including academic integrity, data protection, and responsible AI use. The results confirm the Ethical AI Framework and the key points of Outcomes-Based Teaching and Learning (OBTL). In particular, according to the Ethical AI Framework, responsible AI use includes transparency, accountability, and human supervision. At the same time, OBTL principles suggest that constructive alignment of learning outcomes, teaching methods, and evaluation procedures is necessary for effective learning process.

3. Construction of the OBTL Framework-Based AI-Enhanced Cybersecurity Education Course Syllabus

The empirical data obtained became the cornerstone for the development of the proposed AI-Enhanced Outcomes-Based Teaching and Learning (OBTL) Cybersecurity Education Course Syllabus. The respondents' high levels of familiarity with and usage of Generative AI suggest that students are ready for more sophisticated and complex AI-Enhanced learning. At the same time, the relatively low levels of engagement in cybersecurity-related activities, cybersecurity skills, and critical thinking highlight the necessity for creating a curriculum that includes authentic learning activities. In line with this, the suggested syllabus includes AI-assisted laboratory work, cybersecurity simulations, secure coding practices, case-based learning, ethical AI discussions, and authentic assessment practices making sure that the constructive alignment is guaranteed between the Intended Learning Outcomes (ILOs), Teaching-Learning Activities (TLAs), Assessment Tasks (ATs), and learning materials.

CONCLUSION:

This study concluded that third-year Bachelor of Science in Information Technology (BSIT) students at the University of Eastern Pangasinan demonstrated moderate levels of exposure to Generative AI among the third year BSIT students in the University of Eastern Pangasinan in terms of high familiarity and frequency of usage but moderate level of engagement in cybersecurity activities. The respondents also showed moderate levels of skills in

cybersecurity and critical thinking while responsible AI use was high. Statistically significant positive correlation was observed between Generative AI exposure and cybersecurity skills, critical thinking, and responsible AI use. It shows that greater exposure to Generative AI is significantly correlated with better technical, analytical and ethical competencies. From these results, an AI Enhanced Outcomes-Based Teaching and Learning (OBTL) Cybersecurity Education Course Syllabus was created in order to close the competency gaps identified through the study by utilizing the use of AI-assisted learning activities, assessments and cybersecurity simulations in addition to responsible AI use.

RECOMMENDATIONS:

From the results obtained from the study, the following recommendations can be proposed:

1. Generative AI must be incorporated in cybersecurity courses by conducting laboratory works using AI, case-based learning, cybersecurity simulations, and authentic assessments following the principles of Outcomes-Based Teaching and Learning (OBTL).
2. The University of Eastern Pangasinan and higher educational administrators may consider the adoption and validation of the proposed AI-Enhanced OBTL Cybersecurity Education Course Syllabus for better implementation of curriculum and responsible AI integration in Information Technology courses.
3. It is recommended that students be encouraged not only to use Generative AI for academic purposes but also to apply it in cybersecurity related activities while being ethical and responsible in doing so.
4. Future studies may consider the validation of the proposed course syllabus in other higher education institutions using experimental, longitudinal, and multi-institutional studies.

REFERENCES

- OECD. (2023). *Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI*. OECD Publishing. https://www.oecd.org/en/publications/advancing-accountability-in-ai_2448f04b-en.html

ACKNOWLEDGMENT:

Above all, the researcher sincerely thanks Almighty God for His guidance, protection, wisdom, and blessings throughout the completion of this study. The researcher extends heartfelt gratitude to the following individuals whose support made this thesis possible:

To **Dr. Carmelo John E. Vidal**, Panel Chairman, for his expertise and constructive comments that greatly improved the quality of this study.

To the panelists, **Dr. Diosdado Caronongan** and **Prof. Rina Cabansag**, for their helpful suggestions, careful evaluation, and shared knowledge.

To **Prof. Andrew Caronongan**, Thesis Adviser, for his guidance, patience, valuable feedback, and continuous encouragement from the beginning until the completion of this research.

The researcher also extends heartfelt appreciation to the **University of Eastern Pangasinan (UEP)** for providing a nurturing academic environment, institutional support, and opportunities that made the successful completion of this research possible

To **Dr. Evelyn Abalos-Tomboc**, University President; **Mr. Frederick J. Soriano**, Dean of the College of Information Technology;

Ms. Arra Joyce M. Ofciar of the University of Eastern Pangasinan, for their guidance and support during the conduct of this research.

To the **respondents**, for their time, cooperation, and valuable input.

To the researcher's parents, **Mrs. Jocelyn P. Alancado** and **Mr. Winnie G. Alancado**, for their love, sacrifices, and constant emotional, moral, and financial support.

To the **third-year College of Information Technology students** handled by the researcher, for their encouragement and motivation.

To the **graduate school classmates**, for their support and shared determination, and to the **academic and non-academic staff** of the Graduate School for their assistance.

The researcher is deeply grateful to everyone who contributed, directly or indirectly, to the completion of this thesis.

- UNESCO. (2023). *Guidance for generative AI in education and research*. <https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research>
- Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

- Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. *MIS Quarterly*, 13(3), 319–340. <https://www.jstor.org/stable/249008>
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Rabuya, C. A., Jr. (2023). *Four Cs of outcomes-based teaching and learning: A literature review*. *International Journal of Research Publications*. <https://ijrp.sfo3.cdn.digitaloceanspaces.com/pubjournal/4551/1001221420234604.pdf>
- Kasneci, E., Seßler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdel, C., Pfeiffer, F., Poquet, O., Sailer, M., Schmidt, A., Seidel, T., ... Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, Article 102274. <https://doi.org/10.1016/j.lindif.2023.102274>
- Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings. *Computers and Education: Artificial Intelligence*, 7, Article 100327. <https://doi.org/10.1016/j.caeai.2024.100327>
- Elkhodr, M., & Gide, E. (2025). *Integrating generative AI in cybersecurity education: Case study insights on pedagogical strategies, critical thinking, and responsible AI use*. arXiv. <https://arxiv.org/abs/2502.15357>