International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Factors Affecting the Effectiveness of Ethical Hacking Education among MIT Students

Reijus M. Cruz[1]; Patrick B. Solis[2]; Cherry Ann A. Angus[3]; Jomar A. Mondero[4]; Krislane Kate Santillan[5]; Marcelo Mermida III[6]; Joe D. Basanta[7]; Kristine T. Soberano[8]

[1,2,3,4,5,6,7,8] Graduate School, State University of Northern Negros, Philippines

[1] reijus.orange@gmail.com; [2] patricksolis007@gmail.com; [3] anguscherryann47@gmail.com; [4] jomzmondero@gmail.com; [5] krislane.santillan@gmail.com; [6] marsmermida1031@gmail.com; [7] jdbasanta@sunn.edu.ph; [8] ksoberano@sunn.edu.ph

DOI: https://doi.org/10.47760/ijcsmc.2026.v15i08.002

Abstract: This study examined the factors affecting the effectiveness of ethical hacking education among Master in Information Technology (MIT) graduate students at a state university in the Philippines. Using a quantitative, non-experimental, descriptive-correlational design, data were gathered from 20 respondents — the researcher's own MIT classmates — who had taken or were currently taking a formal ethical hacking or cybersecurity course. A researcher-made, 35-item structured questionnaire measured six constructs: curriculum design and content, instructor competence, laboratory and technological support, hands-on/practical learning opportunities, student motivation and engagement, and institutional support, alongside respondents' perceived effectiveness of ethical hacking education. All constructs were rated high to very high, with instructor competence (M = 4.53) and curriculum design (M = 4.48) receiving the strongest agreement and laboratory/technological support (M = 3.99) the weakest. Perceived effectiveness of ethical hacking education was rated very high overall (M = 4.27). Pearson correlation analysis showed that all six factors were significantly and positively related to perceived effectiveness ($r = .58$ to $.83$, $p < .05$), with institutional support and student motivation showing the strongest associations. Multiple regression confirmed that the six factors jointly explained 81.6% of the variance in perceived

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

effectiveness (R\u00b2 = .816, F(6,13) = 9.61, p < .001), with institutional support emerging as the only statistically significant unique predictor (\u03b2 = .471, p = .011). These findings suggest that while curriculum quality and instructional delivery shape student perceptions, sustained institutional support is the most direct lever for improving ethical hacking education outcomes. Recommendations for curriculum developers and institutional policy are discussed.

Keywords: ethical hacking education; cybersecurity education; self-efficacy; instructional factors learning style; curriculum design; hand-on/virtual labs; educational effectiveness; higher education institutions

---

I. INTRODUCTION

Ethical hacking has become a vital cybersecurity skill, as organizations seek penetration testers and security professionals to identify vulnerabilities before malicious actors can exploit them. Industry support for this approach is strong: in an interview study of 206 cybersecurity professionals, Pike [1] found unanimous support for integrating hacking instruction into academic curricula, along with several critical success factors for making such programs effective. MIT is one of the universities that have responded by adding ethical hacking courses to their programs to help prepare students for careers in cybersecurity. However, not all students who take these courses end up with the same level of proficiency or confidence in ethical hacking skills.

Many factors can affect how students learn and retain these skills. Curriculum design and access to hands-on labs play a particularly important role: virtual and hands-on lab environments have been shown to strengthen learning outcomes and engagement in cybersecurity coursework by allowing students to apply theoretical concepts in realistic, low-risk settings [2][3]. Instructional approaches that use experiential, hands-on learning models have also been linked to increased student self-efficacy and interest in the field, suggesting that how a skill is taught can be as influential as what is taught [4]. At the same time, student-related factors such as prior technical background, motivation, and learning approach shape outcomes independently of instructional design; research on computer science students has found that those with higher self-efficacy tend to adopt deeper, more effective learning approaches, while students with lower self-efficacy are more likely to rely on surface-level learning strategies that do not transfer well to applied skills [5]. If institutions do not know what matters most, they risk wasting resources on teaching methods that do not transfer to real-world competence.

The purpose of this study is to identify and analyze the factors that affect the effectiveness of ethical hacking education for MIT students. In particular, it seeks to investigate the relationship between student-related factors, such as prior IT knowledge, motivation, and learning style; instructional factors, such as teaching methods, curriculum content, and lab facilities; and the perceived effectiveness of ethical hacking education.

The findings of this research will be helpful for teachers, curriculum developers, and students. Educators and curriculum developers can use the findings to improve course design and teaching strategies, while students can gain a better understanding of how to prepare themselves to succeed in ethical hacking courses. The study will also contribute to the limited literature on the effectiveness of cybersecurity education in academic institutions. The research will be conducted through a quantitative approach, distributing survey questionnaires to MIT students who have taken or are taking ethical hacking-related courses, with statistical analysis used to determine the significance of the relationships among the identified factors.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

II. OBJECTIVES OF THE STUDY

The primary purpose of this research is to identify and analyze the factors affecting the effectiveness of ethical hacking education among MIT students.

Specifically, this study aims to:

1. To determine the demographic profile of the respondents.
2. To assess the student-related factors affecting the effectiveness of ethical hacking education, such as prior knowledge, motivation, and learning style.
3. To assess the instructional factors affecting the effectiveness of ethical hacking education, such as teaching methods, curriculum content, lab facilities, and instructor expertise.
4. To determine the level of effectiveness of ethical hacking education as perceived by the respondents.
5. To determine the significant relationship between the identified factors and the effectiveness of ethical hacking education.
6. To propose recommendations for improving the design and delivery of ethical hacking education.

III. REVIEW OF RELATED LITERATURE

This chapter briefly reviews foreign and local literature relevant to the factors affecting the effectiveness of ethical hacking education among MIT students, organized around student-related factors, instructional factors, and effectiveness as an outcome, and closes with a synthesis of the gap this study addresses.

Ethical Hacking and Cybersecurity Education

Pike [1] surveyed 206 cybersecurity professionals and found unanimous support for integrating hacking instruction into academic programs, given sound ethics guidelines, qualified instructors, and realistic practice environments. Ahmed et al. [6] similarly found that learner-centered methods, such as case studies, simulations, and virtual labs, consistently strengthened engagement in university cybersecurity courses. Locally, De Ramos and Esponilla [9] found recurring cybersecurity-readiness gaps, such as weak user education and unclear security strategy, across Philippine state universities and colleges.

Student-Related Factors

Prior knowledge/self-efficacy: Laitinen et al. [5] found computer science students with higher self-efficacy used deeper learning approaches, while those with lower self-efficacy relied on surface-level strategies that transfer poorly to hands-on skills. Motivation: Towhidi and Pridmore [4] found experiential, hands-on learning increased both self-efficacy and interest in cybersecurity. Learning style: Magulod [11] found Filipino BSIT/BIT students favored visual, group, and kinesthetic styles, and recommended aligning instruction accordingly.

Instructional Factors

Curriculum/teaching methods: Miranda et al. [12] found Filipino students, teachers, and professionals agreed on the importance of communication, critical thinking, and ethical judgment for cybersecurity roles, though students rated these with less urgency, reflecting limited workplace exposure. Lab facilities: Aldwairi and Zeng et al. [2] [3] found virtual/hands-on labs strengthened learning by letting students apply concepts in realistic settings, and Kebande [10] found learners and educators alike rated virtual labs as engaging and effective. Instructor expertise: Aquino [8]

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

found faculty competence and ongoing training were consistently seen as foundational to teaching quality in Philippine HEIs, though evidence specific to cybersecurity instructors is limited.

Effectiveness of Cybersecurity Education

Alabab et al. [7] found strong cybersecurity awareness among 291 Filipino students, correlated only with age, while Palao et al. [13] found a strong positive correlation between cybersecurity education and awareness among 75 students, concluding that structured curricular initiatives build protective knowledge and skills.

Synthesis

Foreign literature links experiential, lab-based teaching and self-efficacy to stronger cybersecurity learning outcomes; local literature confirms distinct Filipino learning-style preferences, persistent curriculum-industry gaps, and a measurable link between cybersecurity education and awareness. No reviewed study, however, jointly examines student-related and instructional factors to predict the effectiveness of ethical hacking education specifically among students actively enrolled in such coursework — the gap this study addresses through a survey of MIT students who have taken or are taking ethical hacking-related courses.

IV. METHODOLOGY

This chapter presents the research design, research locale, population and sampling procedure, research instrument, data gathering procedure, statistical treatment of data, and ethical considerations that guided this study. Throughout this chapter, **MIT** refers to the **Master in Information Technology** program in which the respondents — the researcher's own classmates — were enrolled.

A. Research Design

This study employed a **quantitative, non-experimental, descriptive-correlational research design**. The descriptive component was used to determine the demographic profile of the respondents and their level of agreement on the student-related, instructional, and institutional factors, as well as their perceived effectiveness of ethical hacking education. The correlational component was used to determine whether, and to what extent, these identified factors were significantly related to and predictive of the respondents' perceived effectiveness of ethical hacking education. This design was deemed appropriate because the study's objectives required both the numerical description of respondents' perceptions and the statistical testing of relationships among variables, rather than the exploration of lived experience, which would call for a qualitative approach instead.

B. Research Locale

The study was conducted in a state university located in Sagay City, Negros Occidental, Philippines, among graduate students enrolled in the **Master in Information Technology (MIT)** program who had taken or were currently taking a formal subject or course related to ethical hacking or cybersecurity. The respondents were the researcher's own classmates within the same MIT class/cohort, providing direct access to graduate-level students with shared, verifiable exposure to the course content, laboratory activities, and instructional experiences under study.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

C. Population, Sample, and Sampling Technique

The population of this study consisted of graduate students enrolled in the **Master in Information Technology (MIT)** program who had taken or were currently taking a formal subject or course related to ethical hacking or cybersecurity. Given that this population was a single, intact graduate class/cohort, the study used **total enumeration (complete/purposive census) sampling**, wherein all classmates within the researcher's own MIT class who consented to participate during the data collection period were included as respondents. A total of **20 respondents** — all of them the researcher's classmates in the same MIT class — completed and submitted valid responses to the survey questionnaire.

The following inclusion criteria guided respondent eligibility: (1) the respondent must be a graduate student enrolled in the Master in Information Technology (MIT) program; (2) the respondent must have taken or be currently taking a formal subject, course, seminar, or training related to ethical hacking or cybersecurity; and (3) the respondent must be willing to voluntarily answer the survey questionnaire in full.

D. Research Instrument

The primary data-gathering instrument was a **researcher-made structured questionnaire** administered through Google Forms. The questionnaire was developed based on the specific objectives of the study and was composed of two parts.

Part I. Respondent Profile

This part gathered the respondents' demographic and background information, namely: age, sex, year level, whether they had taken a formal subject or course related to ethical hacking or cybersecurity, whether they had attended any related seminar, workshop, or training outside their regular class, and whether they had access to a personal computer or laptop capable of running security tools (e.g., Kali Linux, virtual machines).

Part II. Perception Items

This part consisted of 35 close-ended statements rated on a **five-point Likert scale** (1 = Strongly Disagree to 5 = Strongly Agree), organized into six constructs aligned with the study's specific objectives:

Table. Structure of the Research Instrument

Construct	No. of Items	Description
Curriculum Design and Content	5	Relevance, structure, balance of theory/practice, clarity of objectives, and currency of the ethical hacking curriculum
Instructor Competence	5	Instructor's technical expertise, clarity of instruction, use of real-world examples, feedback, and facilitation of critical thinking
Laboratory and Technological Support	5	Adequacy of computer laboratories, software/tools, internet connectivity, reference materials, and LMS support
Hands-on / Practical Learning Opportunities	5	Sufficiency of hands-on exercises, sandbox practice, CTF activities, practical assessment, and industry immersion opportunities
Student Motivation and	5	Personal interest, career motivation, self-directed learning,

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Construct	No. of Items	Description
Engagement		confidence, and engagement in class
Institutional Support	5	Institutional policies, certification support, industry engagement, budget allocation, and promotion of cybersecurity organizations
Perceived Effectiveness of Ethical Hacking Education	5	Applied competence, understanding of legal/ethical boundaries, tool proficiency, skills improvement, and overall preparedness for real-world practice

E. Validity and Reliability

Because a separate pilot administration was not feasible given the limited size of the eligible population, the reliability of each construct was instead established through Cronbach's alpha computed on the actual dataset gathered from the 20 respondents, yielding coefficients ranging from **α = .844 to α = .969** across constructs and an overall instrument reliability of **α = .974**, indicating excellent internal consistency (George & Mallery, 2003). This approach and its limitation are disclosed transparently and revisited in the discussion of the study's limitations.

F. Data Gathering Procedure

1. A letter requesting permission to conduct the study was submitted to the appropriate institutional authority/program coordinator.
2. Upon approval, prospective respondents meeting the inclusion criteria were identified and invited to participate.
3. Eligible respondents were provided a Google Forms link containing an informed consent statement, followed by the two-part structured questionnaire.
4. Respondents answered the questionnaire independently and at their own convenience within the data collection period.
5. Responses were automatically compiled in a Google Sheets response file, which the researcher then reviewed for completeness and validity prior to encoding.
6. Data were exported, cleaned, and organized for statistical treatment.

G. Statistical Treatment of Data

To answer the specific objectives of the study, the responses gathered from the survey questionnaire were organized, tabulated, and analyzed using the following statistical tools.

H. Frequency and Percentage Distribution

Frequency counts and percentages were used to describe the demographic profile of the respondents in terms of age, sex, year level, prior exposure to a formal ethical hacking or cybersecurity course, participation in external training, and access to a personal computer or laptop capable of running security tools. This addresses **Objective 1** of the study.

I. Weighted Mean and Standard Deviation

The weighted mean and standard deviation were computed for each indicator and for each construct — student-related factors, instructional factors (curriculum design and content, instructor competence, laboratory and

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

technological support, and hands-on/practical learning opportunities), institutional support, and perceived effectiveness of ethical hacking education — to determine the respondents' level of agreement on the five-point Likert scale. This addresses **Objectives 2, 3, and 4** of the study. Mean scores were interpreted using the following scale:

- **4.20 – 5.00** — Very High / Strongly Agree
- **3.40 – 4.19** — High / Agree
- **2.60 – 3.39** — Moderate / Neutral
- **1.80 – 2.59** — Low / Disagree
- **1.00 – 1.79** — Very Low / Strongly Disagree

Cronbach's Alpha

Cronbach's alpha was computed for each construct and for the survey instrument as a whole to establish internal consistency reliability. Reliability was interpreted using the conventional threshold of $\alpha \geq .70$ as acceptable, with higher coefficients indicating stronger internal consistency (George & Mallery, 2003).

J. Pearson Product-Moment Correlation

Pearson's r was used to determine the strength and direction of the relationship between each identified factor and respondents' perceived effectiveness of ethical hacking education, directly addressing **Objective 5**. Composite (mean) scores per construct served as the unit of analysis, interpreted using Evans' (1996) guideline (.00–.29 negligible, .30–.49 low, .50–.69 moderate, .70–.89 high, .90–1.00 very high) at $\alpha = .05$ (two-tailed). Spearman's rank-order correlation (rho) was used as a robustness check given the non-normal distribution of several constructs at this sample size.

K. Multiple Linear Regression Analysis

Multiple linear regression was used, as a complement to the correlation analysis under **Objective 5**, to determine the combined predictive contribution of the identified factors to perceived effectiveness and to identify which factor(s) contributed a statistically significant unique effect. Model fit was evaluated using R^2 and the overall F-test; variance inflation factors (VIF) were examined to check for multicollinearity. Given the sample size (n = 20) relative to the number of predictors (six factors), regression results are treated as **exploratory and supplementary** to the correlation analysis, which more directly addresses Objective 5.

L. Statistical Software

All statistical computations were performed using standard statistical computing tools (Python, with SciPy and statsmodels libraries, and/or IBM SPSS), with results cross-checked for accuracy prior to interpretation.

M. Ethical Considerations

Informed Consent

Respondents indicated their informed consent by selecting a consent option before proceeding to the questionnaire. The consent statement explained the purpose of the study, the voluntary nature of participation, the respondents' right to withdraw at any time without consequence, and the measures taken to protect confidentiality.

Confidentiality and Anonymity

No personally identifying information (e.g., full name, contact details) was collected. Responses were stored in a password-protected account accessible only to the researcher, and data were reported only in aggregate or statistical form, ensuring that no individual respondent could be identified from the results.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Voluntary Participation
Participation was entirely voluntary. Respondents were free to skip items they were uncomfortable answering or to discontinue the survey at any point without penalty.

V. RESULTS AND DISCUSSION

This section presents the findings of the study on the factors affecting the effectiveness of ethical hacking education among Information Technology students, based on data gathered from **20 respondents** who had taken or were currently enrolled in an ethical hacking-related course. Results are organized according to the specific objectives of the study: (1) the demographic profile of the respondents; (2) student-related factors; (3) instructional factors, comprising curriculum design, instructor competence, laboratory and technological support, and hands-on practical opportunities; (4) institutional support; (5) the level of perceived effectiveness of ethical hacking education; and (6) the relationship between the identified factors and perceived effectiveness. A five-point Likert scale was used for all perception items, interpreted as follows: 4.20–5.00 (Very High/Strongly Agree), 3.40–4.19 (High/Agree), 2.60–3.39 (Moderate/Neutral), 1.80–2.59 (Low/Disagree), and 1.00–1.79 (Very Low/Strongly Disagree). Instrument reliability was assessed using Cronbach's alpha, which yielded an overall coefficient of $\alpha = 0.974$ across all 35 perception items, indicating excellent internal consistency (George & Mallery, 2003).

A. Demographic Profile of the Respondents

Table 1 presents the demographic characteristics of the respondents in terms of age, sex, year in the MIT program, prior formal exposure to ethical hacking or cybersecurity coursework, participation in external training, and access to a personal computing device capable of running security tools.

Table 1. Demographic Profile of the Respondents

Variable	Category	f	%
Age	24 years old and above	17	85.0%
	22-23 years old	3	15.0%
Sex	Male	10	50.0%
	Female	10	50.0%
Year in the MIT Program	1st Year	11	55.0%
	4th Year	5	25.0%
	2nd Year	2	10.0%
	3rd Year	2	10.0%
Formal Course Taken	Yes	19	95.0%
	No	1	5.0%
External Training Attended	No	11	55.0%

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Variable	Category	f	%
	Yes	9	45.0%
Access to Capable Device	Yes	17	85.0%
	No	3	15.0%

Note. N = 20.

The results show that the sample was predominantly composed of respondents **24 years old and above (85.0%)**, with an equal distribution between **male and female respondents (50.0% each)**. In terms of academic standing, the majority were in their **first year of the MIT program (55.0%)**, followed by those in their fourth year (25.0%). Nearly all respondents (**95.0%**) reported having taken a formal subject or course related to ethical hacking or cybersecurity, while slightly less than half (**45.0%**) had attended an external seminar, workshop, or training beyond regular coursework. A large majority (**85.0%**) reported having personal access to a computer or laptop capable of running security tools such as Kali Linux or virtual machines. This profile suggests that the respondent pool was largely composed of students with direct, current classroom exposure to ethical hacking content and reasonably strong access to the hardware needed for hands-on practice, which strengthens the credibility of their perception-based responses on curriculum, instruction, and effectiveness.

B. Student-Related Factors

Table 2 presents the respondents' perception of student-related factors, including personal interest, career motivation, self-directed learning, confidence, and engagement, which the study's second objective sought to assess.

Table 2. Student-Related Factors: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
I am personally interested in learning ethical hacking and cybersecurity.	4.40	1.10	Very High
I am motivated to pursue a career related to cybersecurity or ethical hacking.	4.20	1.06	Very High
I actively seek additional knowledge on ethical hacking outside class requirements.	4.00	1.08	High
I feel confident in applying ethical hacking concepts and techniques.	4.00	1.17	High
I am engaged and attentive during ethical hacking lectures and activities.	4.20	1.01	Very High
Composite Mean	**4.16**	**1.02**	**High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.969.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

As shown in Table 2, respondents rated student-related factors **overall high** (M = 4.16, SD = 1.02). Personal interest in learning ethical hacking and cybersecurity and motivation to pursue a related career obtained the highest ratings, while self-reported confidence in applying concepts and independent knowledge-seeking beyond class requirements were comparatively lower, though still within the high range. These findings suggest that while students enter and engage with ethical hacking coursework with strong intrinsic interest, a gap remains between interest and self-assessed applied competence — an area instructional design may need to target more directly.

C. Instructional Factors

Table 3 presents the results for instructional factors, disaggregated into four dimensions identified in the study's third objective: curriculum design and content, instructor competence, laboratory and technological support, and hands-on/practical learning opportunities.

Table 3. Curriculum Design and Content: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
The ethical hacking curriculum covers topics relevant to current cybersecurity trends.	4.55	0.69	Very High
The course content is well-structured and logically sequenced.	4.45	0.60	Very High
The curriculum balances theoretical knowledge with practical application.	4.45	0.69	Very High
The learning objectives of the ethical hacking course are clearly defined.	4.55	0.60	Very High
The curriculum includes updated tools and techniques used in the industry.	4.40	0.99	Very High
Composite Mean	**4.48**	**0.63**	**Very High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.915.

Curriculum design and content was rated very high overall (M = 4.48, SD = 0.63), with respondents most strongly affirming that the curriculum covers current cybersecurity trends and that learning objectives are clearly defined. This indicates that the ethical hacking curriculum is perceived as relevant and well-articulated, consistent with prior findings that curriculum currency and clarity are foundational to effective cybersecurity instruction [2].

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

D. Instructor Competence

Table 4. Instructor Competence: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
The instructor has sufficient technical expertise in ethical hacking and cybersecurity.	4.45	1.10	Very High
The instructor effectively explains complex hacking concepts and techniques.	4.55	1.00	Very High
The instructor uses real-world examples and case studies during instruction.	4.60	0.94	Very High
The instructor provides timely and constructive feedback on students' performance.	4.50	0.95	Very High
The instructor encourages critical thinking and problem-solving among students.	4.55	0.94	Very High
Composite Mean	**4.53**	**0.93**	**Very High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.965.

Instructor competence received the highest composite rating among all instructional dimensions (M = 4.53, SD = 0.93), interpreted as very high. Respondents particularly affirmed the use of real-world examples and case studies during instruction. This finding aligns with the view that instructor expertise and pedagogical delivery are critical success factors for hacking-related instruction [1].

E. Laboratory and Technological Support

Table 5. Laboratory and Technological Support: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
The school provides adequate computer laboratories for hands-on practice.	3.65	1.04	High
Necessary software and tools (e.g., virtual machines, penetration-testing tools) are available and accessible.	4.10	0.91	High
Internet connectivity in the laboratory is stable and sufficient for practical exercises.	3.95	0.89	High
Reference materials (books, e-books, online resources) on ethical hacking are accessible.	4.20	0.89	Very High

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Indicator	Mean	SD	Verbal Interpretation
The learning management system (LMS) or online platform effectively supports course delivery.	4.05	0.83	High
Composite Mean	**3.99**	**0.72**	**High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.851.

Laboratory and technological support obtained the lowest composite mean among the instructional dimensions (M = 3.99, SD = 0.72), still interpreted as high. Adequacy of computer laboratories for hands-on practice was rated relatively lower than access to reference materials and required software tools. This pattern echoes concerns raised in the literature that infrastructure and lab access — rather than instructional intent — often constitute the binding constraint on cybersecurity skill development (Zeng et al., 2018).

F. Hands-on / Practical Learning Opportunities

Table 6. Hands-on / Practical Learning Opportunities: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
The course provides sufficient hands-on laboratory exercises.	4.05	0.94	High
Students are given opportunities to practice hacking techniques in a safe, controlled (sandbox) environment.	4.25	0.85	Very High
Capture-the-Flag (CTF) competitions or similar activities are incorporated into learning.	4.25	0.91	Very High
Practical assessments accurately measure students' technical skills.	4.40	0.82	Very High
Opportunities for internships, on-the-job training, or industry immersion in cybersecurity are available.	3.70	1.22	High
Composite Mean	**4.13**	**0.84**	**High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.923.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Hands-on and practical learning opportunities were rated high overall (M = 4.13, SD = 0.84). Practical assessments were perceived as most accurately measuring technical skills, while access to internships, on-the-job training, or industry immersion received the lowest rating within this dimension, suggesting an area for curricular strengthening consistent with recommendations for experiential, applied learning in cybersecurity education (Towhidi & Pridmore, 2022).

G. Institutional Support

Table 7 presents respondents' perceptions of institutional support mechanisms for ethical hacking education, including policy clarity, certification support, industry engagement, budget allocation, and awareness of related organizations.

Table 7. Institutional Support: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
The institution provides clear policies on the ethical and legal use of hacking skills.	4.30	0.86	Very High
The institution supports certifications (e.g., CEH, CompTIA Security+) related to ethical hacking.	3.90	0.91	High
The school invites industry practitioners or holds guest lectures on cybersecurity topics.	3.75	0.85	High
The institution allocates sufficient budget for cybersecurity laboratory equipment and tools.	3.80	0.95	High
The institution promotes awareness of cybersecurity clubs, organizations, or competitions.	4.30	0.92	Very High
Composite Mean	**4.01**	**0.74**	**High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.880.

Institutional support was rated high overall (M = 4.01, SD = 0.74). Clear policies on the ethical and legal use of hacking skills and promotion of cybersecurity clubs and competitions received the strongest agreement, while budget allocation for laboratory equipment and invitations of industry practitioners for guest lectures were comparatively lower, pointing to specific, actionable areas for institutional investment.

H. Level of Perceived Effectiveness of Ethical Hacking Education

Table 8 addresses the study's fourth objective by presenting the respondents' overall perceived effectiveness of the ethical hacking education they received.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Table 8. Level of Perceived Effectiveness of Ethical Hacking Education: Item Means, Standard Deviations, and Verbal Interpretation

Indicator	Mean	SD	Verbal Interpretation
I can apply ethical hacking concepts to identify security vulnerabilities.	4.05	1.00	High
I understand the legal and ethical boundaries of hacking practices.	4.55	0.69	Very High
I am capable of using the penetration-testing tools and techniques learned in class.	4.10	0.91	High
My knowledge and skills in ethical hacking have improved significantly since taking the course.	4.35	0.75	Very High
Overall, the ethical hacking education I received adequately prepared me for real-world cybersecurity challenges.	4.30	0.73	Very High
Composite Mean	**4.27**	**0.65**	**Very High**

Note. n = 20; Scale: 4.20–5.00 Very High, 3.40–4.19 High, 2.60–3.39 Moderate, 1.80–2.59 Low, 1.00–1.79 Very Low. Cronbach's α = 0.844.

The overall perceived effectiveness of ethical hacking education was rated very high (M = 4.27, SD = 0.65). Respondents most strongly agreed that they understood the legal and ethical boundaries of hacking practices, while their capability to apply concepts to identify security vulnerabilities was rated comparatively — though still favorably — lower. Taken together, these results indicate that students perceive the program as having substantially prepared them for real-world cybersecurity practice, with ethical grounding perceived as a stronger outcome than applied technical mastery.

I. Relationship Between the Identified Factors and Perceived Effectiveness

Table 9 addresses the study's fifth objective by presenting the Pearson product-moment correlation between each factor and respondents' perceived effectiveness of ethical hacking education. Composite (mean) scores per construct were used as the unit of analysis.

Table 9. Correlation Between Identified Factors and Perceived Effectiveness of Ethical Hacking Education

Factor	r	p-value	Strength of Relationship	Decision (α = .05)
Institutional Support	0.833	<0.001	High	**Significant**
Student Motivation and Engagement	0.776	<0.001	High	**Significant**

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Factor	r	p-value	Strength of Relationship	Decision (α = .05)
Laboratory and Technological Support	0.739	<0.001	High	**Significant**
Curriculum Design and Content	0.688	<0.001	Moderate	**Significant**
Instructor Competence	0.621	0.0035	Moderate	**Significant**
Hands-on / Practical Learning Opportunities	0.584	0.0069	Moderate	**Significant**

Note. Strength of relationship interpreted per Evans (1996): .00–.29 Negligible, .30–.49 Low, .50–.69 Moderate, .70–.89 High, .90–1.00 Very High. Significant at α = .05 (two-tailed).

All six hypothesized factors were found to have a statistically significant positive relationship with perceived effectiveness at the .05 level. **Institutional support (r = .833, p < .001)** and **student motivation and engagement (r = .776, p < .001)** showed the strongest associations, followed by laboratory and technological support, curriculum design and content, instructor competence, and hands-on/practical learning opportunities, all in the moderate-to-high range. These results indicate that improvements in any of the six factors are associated with more favorable perceptions of program effectiveness, with institutional-level support and student engagement emerging as the strongest single correlates.

To determine the combined and relative predictive contribution of the six factors, a multiple linear regression analysis was conducted with perceived effectiveness as the dependent variable. Table 10 presents the model summary and regression coefficients.

Table 10. Multiple Regression Analysis Predicting Perceived Effectiveness of Ethical Hacking Education

Predictor	β (Unstd.)	SE	t	p-value	Decision (α = .05)
(Constant)	0.735	0.623	1.180	0.2592	Not Significant
Curriculum Design and Content	0.128	0.252	0.506	0.6216	Not Significant
Instructor Competence	-0.067	0.189	-0.355	0.7286	Not Significant
Laboratory and Technological Support	-0.014	0.201	-0.072	0.9436	Not Significant
Hands-on / Practical Learning Opportunities	0.155	0.145	1.070	0.3040	Not Significant
Student Motivation and Engagement	0.192	0.152	1.265	0.2281	Not Significant
Institutional Support	0.471	0.159	2.970	0.0109	**Significant**

Note. $R^2 = 0.816$, *Adjusted* $R^2 = 0.731$, $F(6, 13) = 9.613$, $p < .001$.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The overall regression model was statistically significant, $F(6, 13) = 9.61$, $p < .001$, and accounted for approximately **81.6%** of the variance in perceived effectiveness ($R^2 = 0.816$, Adjusted $R^2 = 0.731$), confirming that the identified student-related, instructional, and institutional factors jointly and dependably predict how effective ethical hacking education is perceived to be. Among the individual predictors, **institutional support** emerged as the only statistically significant unique predictor ($\beta = 0.471$, $p = 0.011$) when all six factors were considered simultaneously. The attenuation of the other predictors' unique effects in the presence of significant zero-order correlations reported in Table 9 is consistent with shared variance (multicollinearity) among the instructional and student-related constructs, which were themselves moderately-to-highly intercorrelated ($r = .53$ to $.84$) — a common and expected pattern when related institutional and pedagogical factors are measured concurrently in a single cohort. This suggests that while each factor is meaningfully related to perceived effectiveness on its own, institutional-level support conditions may exert the most direct, non-redundant influence once curricular, instructor, laboratory, and motivational factors are held constant.

J. Summary of Findings

Overall, the results indicate that the respondents — predominantly students aged 24 and above with prior formal exposure to ethical hacking coursework — perceived all examined factors favorably, with instructor competence and curriculum design rated highest, and laboratory/technological support rated relatively lowest among the instructional dimensions. Perceived effectiveness of ethical hacking education was rated **very high** ($M = 4.27$). All six factors examined — student motivation and engagement, curriculum design and content, instructor competence, laboratory and technological support, hands-on/practical learning opportunities, and institutional support — were significantly and positively correlated with perceived effectiveness, and jointly explained a substantial proportion of variance in perceived effectiveness, with institutional support showing the strongest unique contribution. These findings provide an empirical basis for the recommendations addressing the study's sixth objective.

VI. CONCLUSION

This study set out to identify and analyze the factors affecting the effectiveness of ethical hacking education among MIT students, examining student-related, instructional, and institutional dimensions against respondents' perceived effectiveness of the education they received. Based on data gathered from 20 graduate students who had taken or were currently taking an ethical hacking-related course, the findings indicate that respondents perceived their ethical hacking education very favorably overall, with particularly strong ratings for instructor competence and curriculum design, and comparatively lower — though still high — ratings for laboratory and technological support and for industry immersion opportunities.

All six examined factors were significantly and positively correlated with perceived effectiveness, confirming that student motivation, curriculum quality, instructor expertise, laboratory support, hands-on practice, and institutional support each play a meaningful role in shaping how effective ethical hacking education is perceived to be. When considered jointly through multiple regression, these factors explained a substantial share of the variance in perceived effectiveness, with institutional support standing out as the only statistically significant unique predictor. This suggests that while curriculum and instructional quality lay the groundwork for student learning, sustained institutional investment — in the form of laboratory infrastructure, certification support, industry engagement, and budget allocation — may be the most decisive lever available to program administrators seeking to strengthen ethical hacking education outcomes.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Reijus M. Cruz *et al*, Volume 15, Issue 8, August 2026, pg. 22-38
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Given the study's total-enumeration sample of 20 classmates from a single MIT cohort, these findings should be interpreted as reflective of this particular program and context rather than generalized broadly; replication with larger, more diverse samples across institutions is recommended. Nonetheless, the results offer administrators, curriculum developers, and instructors a clear, evidence-based starting point: reinforcing institutional support structures alongside existing strengths in curriculum and instruction is likely to yield the greatest gains in how students experience and benefit from ethical hacking education.

References

[1]. Pike, R. E. (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management, 22*(4), Article 4. https://doi.org/10.58729/1941-6679.1021

[2]. Aldwairi, M. (2022). *Evaluating virtual laboratory platforms for supporting on-line information security courses*. arXiv. https://doi.org/10.48550/arXiv.2208.12612

[3]. Zeng, Z., Deng, Y., Hsiao, I., Huang, D., & Chung, C.-J. (2018). Improving student learning performance in a virtual hands-on lab system in cybersecurity education. *2018 IEEE Frontiers in Education Conference (FIE)*. https://doi.org/10.1109/FIE.2018.8658855

[4]. Towhidi, G., & Pridmore, J. (2022). Increasing cybersecurity interest and self-efficacy through experiential labs. *Issues in Information Systems, 23*(2), 119–131. https://doi.org/10.48009/2_iis_2022_110

[5]. Laitinen, S., Christopoulos, A., Laitinen, P., & Nieminen, V. (2024). Relationships between self-efficacy and learning approaches as perceived by computer science students. *Frontiers in Education, 9,* Article 1181616. https://doi.org/10.3389/feduc.2024.1181616

[6]. Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How universities teach cybersecurity courses online: A systematic literature review. Frontiers in Computer Science, 6, Article 1499490. https://doi.org/10.3389/fcomp.2024.1499490

[7]. Alabab, B., Cubol, J., Pascual, M. A., & Ubaldo, E. (2023). Cybersecurity awareness of college students in a private higher education institution. CGCI International Journal of Administration, Management, Education and Technology.

[8]. Aquino, J. M. D. (2025). Best practices of high performing higher education institutions in the Philippines towards the development of harmonized quality-assured instructional leadership framework. Frontiers in Education, 10, Article 1663289. https://doi.org/10.3389/feduc.2025.1663289

[9]. De Ramos, N. M., & Esponilla, F. D., II. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education, 11(3), 1198–1209. https://doi.org/10.11591/ijere.v11i3.22863

[10]. Kebande, V. R. (2024). The impact of virtual laboratories on active learning and engagement in cybersecurity distance education. arXiv. https://doi.org/10.48550/arXiv.2404.04952

[11]. Magulod, G. C., Jr. (2019). Learning styles, study habits and academic performance of Filipino university students in applied science courses: Implications for instruction. Journal of Technology and Science Education, 9(2), 184–198. https://doi.org/10.3926/jotse.504

[12]. Miranda, J. P. P., Tayag, M. I., & Canlas, J. D. (2025). Cybersecurity skills in new graduates: A Philippine perspective. arXiv. https://doi.org/10.48550/arXiv.2512.14778

[13]. Palao, B., Cruz, N. A., Lualhati, G. L., Pascual, E., & Santos, J. M. (2026). The human firewall: Evaluation of cybersecurity awareness among students of Bulacan State University. Journal of Critical Social Sciences and Review, 1(1), 1–10. https://doi.org/10.5281/zenodo.19413443

