Gamification in Cybersecurity Education and the Enhancement of Professional Skills. Insights from the Cyber Sapere Initiative in Italian Higher Education Institutions

Paolo Micozzi[1], Fabiana Rocchi[2], Serena Montefusco[3]

[1] Ministry of University and Research, Italy
[2] Consorzio Cineca, Italy
[3] HSPI S.p.A., Italy

Abstract

The rapid evolution of cyber threats and the increasing number of security incidents targeting academic environments have emphasized the need to strengthen cybersecurity education in higher education institutions (HEIs) [1], [2]. Universities are not only responsible for preparing future cybersecurity professionals but also for ensuring that students, researchers, and administrative staff develop adequate awareness and skills to mitigate cyber risks. In this context, gamification is gaining attention as an innovative educational approach capable of improving learning effectiveness and supporting the development of a stronger cyber posture within academic institutions [3]. The need for cyber training has also been reaffirmed by recent European regulations on the topic such as Network and Information System Security. This paper explores the role of gamification in cybersecurity education and examines how game-based learning strategies can contribute to both student training and the upskilling and reskilling of institutional personnel [4]. Typical gamification elements, such as interactive learning, simulations of real cyber-attack scenarios, challenges, and reward systems, transform traditional learning processes into experiential activities where participants can actively apply theoretical knowledge and test different strategies in a safe and controlled sandbox environment [5],[6]. Given the dynamic nature of cybersecurity threats, the relevance of this approach is particularly significant in the context of continuous professional development, where organizations need to invest in professional development and reskilling initiatives. Within this context, the study focuses on the Italian Ministry of University and Research initiative known as the Cyber Sapere program, which contributes to the implementation of the National Cybersecurity Strategy [7]. The program promotes the transfer of cybersecurity knowledge, specialized training courses, and expert consultancy to higher education institutions. Its objective is to strengthen institutional resilience by fostering a systemic approach to cybersecurity education that involves students, researchers, and academic staff. Drawing on the experience of the Ministry of University and Research, this paper proposes a replicable and measurable best-practice model that can support policymakers, academic communities, and industry stakeholders in strengthening cyber resilience, promoting a culture of secure innovation, and enhancing digital skills across the research ecosystem.

Keywords: *Gamification, cybersecurity, education, upskilling, reskilling*

1. Introduction

Public and private institutions today face a landscape of growing exposure to cyber threats. The open nature of academic ecosystems, combined with a diverse user base and the strong interconnection between research, teaching, and administrative activities, makes Higher Education Institutions (HEIs) particularly vulnerable [1], [2]. Targeted attacks against academia have increased in recent years, highlighting vulnerabilities that are not exclusively technological but also involve the behaviors of individuals and organizational shortcomings. In this context, cybersecurity training becomes essential. Academia is not only responsible for preparing future cybersecurity professionals, but must also ensure that students, researchers, and administrative and technical staff adopt behaviors appropriate to managing cyber risk. However, traditional training models are often passive, comprising lectures and static e-learning modules, and show clear limitations in their ability to produce lasting behavioral change. In light of these weaknesses, gamification is becoming increasingly more established as an innovative approach in the field of education. Integrating game design elements into educational contexts turns learning into a more active and engaging process, encouraging user participation and interaction [3]. In the field of cybersecurity, this translates into the ability to simulate realistic scenarios, allowing

participants to test decisions and strategies in controlled environments through the use of learning platforms that also leverage Artificial Intelligence [4]. At the same time, digital transformation and evolving security frameworks are redefining competency requirements in academic research. Therefore, it is becoming necessary to promote structured upskilling and reskilling courses to face changing professional needs [5], [6].
Within this context, this study examines the "Cyber Sapere" initiative, promoted by the Italian Ministry of Universities and Research. The objective is to assess how much more effective gamified approaches are compared to traditional models in promoting behavioral change, contributing to skills development, and supporting the alignment of academic institutions with national and European cybersecurity strategies. Therefore, this paper aims to offer a systematic analysis and empirical evidence on a model that could potentially be replicated in complex settings.

2. Literature Review

Recent literature highlights how academic institutions are increasingly adopting structured frameworks for managing cybersecurity, often inspired by international standards and European guidelines [5]. However, these frameworks tend to focus on technology and institutional procedures, neglecting the human element, which represents one of the primary risk factors. This imbalance is part of the reason why, despite the adoption of advanced policies and tools, many organizations continue to experience vulnerabilities related to user behavior.
In this context, gamification emerges as a possible tool for addressing these limitations [2]. Established research shows that introducing interactive digital learning platforms into training can increase user engagement and motivation, encouraging more active participation [3], [7]. In cybersecurity, incorporating simulations, challenges, and interactive scenarios into training programs brings learning closer to real-world situations, helping participants develop practical skills more effectively. Despite this, traditional awareness programs remain widespread in academic institutions, and while they help educate participants, they often prove ineffective at changing user behavior in practice, particularly in the medium and long term. The literature highlights a persistent gap between theoretical knowledge and practical application, which represents one of the main weaknesses in cybersecurity management [8], [9]. At the same time, the development of digital skills is becoming increasingly important. The gap between the supply and demand for cybersecurity skills and STEM competencies in general is now widely acknowledged at the European level, prompting organizations to commit to continuous investment in training strategies. In this context, innovative approaches such as game-based learning can offer more flexible and adaptive solutions, capable of supporting tailored learning experiences [5], [6]. While gamification has attracted considerable attention in recent years, the literature still presents some significant gaps. In particular, empirical evidence on the long-term effectiveness of gamification remains limited, and models that integrate training, regulatory requirements, and organizational practices are still underdeveloped. Furthermore, no clear operational models have yet emerged that can be replicated in complex academic settings. This study aims to address these gaps through a systematic analysis of the "Cyber Sapere" case, both at the ministerial level and within individual universities and Higher Education Institutions (HEIs).

3. Methodology

This study aims to integrate quantitative and qualitative evidence to assess the effectiveness of the "Cyber Sapere" program. This approach makes it possible to document all measurable data regarding participation and user performance, as well as qualitative elements, such as the way the training experience is perceived by participants and any changes in their behavior [6].
The research data were collected during the implementation of the program across several Italian Higher Education Institutions and the Ministry of Universities and Research. The participating institutions vary considerably in size, digital maturity, and organizational model, providing a range of contexts in which to evaluate the program. Data sources include metrics generated by the training platform, results from gamified activities, satisfaction surveys distributed to participants, and qualitative feedback gathered through direct interactions with them. The analytical framework was built around three main factors: behavior — focusing on levels of engagement, knowledge retention, and the ability of users to develop safer habits; skills development — aiming to assess the extent to which the program contributes to upskilling and reskilling, both in terms of technical skills and broader competencies; strategic alignment and replicability of the model — focusing on consistency with European regulatory frameworks and the potential for adaptation across different organizational contexts.

The assessment of the program's effectiveness draws on an integrated set of indicators. Analysis of baseline data helps direct training toward institutions with the greatest need to improve their security posture and expand employee competencies, while data regarding the participants' performance in simulations allows for an assessment of their ability to apply skills in realistic scenarios. At the same time, qualitative analysis of feedback provides a complementary perspective, useful for understanding the impact of the training experience at both an organizational and cultural level.

4. Case Study: The “Cyber Sapere" Program

The "Cyber Sapere" program was developed by the Ministry of Universities and Research (MUR) in collaboration with the National Cybersecurity Agency (ACN), as part of the National Cybersecurity Strategy 2022–2026 [10]. The program is a joint cybersecurity initiative aimed at universities, Higher Education Institutions for Fine Arts, Music, and Dance (AFAM), and the MUR. The objective is to promote a culture of cybersecurity, enhance the digital skills of users, strengthen their security posture, and contribute to the overall resilience of the national academic system. The program is structured around three distinct areas. The first is training, which aims to improve the basic cybersecurity skills of students and staff at MUR, universities, and AFAM institutions through e-learning courses, instructional materials, training programs, and on-site workshops. This need is grounded in the awareness that basic cybersecurity skills — and STEM competencies in general — are of primary importance and require sustained investment. This is further supported by the literature, which highlights a significant skills gap in the Italian labor market [11].
The second area is prevention, aimed at strengthening the ability of staff at the Ministry, universities, and AFAM institutions to identify and counter cyber threats through hands-on exercises in the form of simulated phishing campaigns. The third area is analysis and monitoring. The initiative aims to establish a structured and ongoing framework of training and operational activities focused on analyzing and monitoring MUR assets, ensuring an accurate and up-to-date assessment of risks associated with applications in use.
Prior to the training, a skills assessment was conducted to identify the needs of the staff at the Ministry, universities, and AFAM institutions, measuring their average level of cybersecurity preparedness [6]. The results set the guidelines for the training plan, helping to identify content and topics aligned with the actual needs of the intended participants. The table below summarizes the results of the cybersecurity skills assessment questionnaire.

Type of entity	Entities involved	Users involve	Certificates issued	Awareness level
Universities AFAM Ministry	103 129 1	11.413 1.299 141	14/25 14/25 13/25	Intermediate Intermediate Intermediate
Totals & Media	233	12.853	14/25	Intermediate

Tab 1. Key results of the cybersecurity skills assessment questionnaire

The program offers two complementary training formats: e-learning courses and in-person classes. In both cases, participants were required to complete a skills assessment test and a satisfaction survey at the end of each course.

4.1 E-learning Training Courses

The first format consisted of both synchronous and asynchronous e-learning sessions. Synchronous e-learning sessions took place on Microsoft Teams, open to a large group of users specifically selected by each institution and the MUR. Given the large number of participants, interaction was limited to the chat function, with responses provided by the instructor. The course totaled 32 hours, divided into 8 sessions of 4 hours each. The table below presents the key KPIs for the synchronous e-learning courses, including user satisfaction scores.

Type of entity	Entities involved	Users involve	Certificates issue	Satisfaction questionnaires	User satisfaction
Universities AFAM	100 148	1.151 781	974 435	426	3.52 / 5.00
Ministry	1	38	35	24	3.83 / 5.00
Totals & Media	249	1.969	1.444	450	3.54 / 5.00

Tab 2. Key KPIs for synchronous e-learning training courses

Asynchronous e-learning sessions were reserved for MUR staff only, with the course being conducted on CyberGuru, an e-learning platform built around a multimedia micro-learning approach. The course was structured into modules organized with increasing difficulty to support the gradual development of skills and ensure participants stay current with evolving cyber threats. The course totaled 27 hours. The table below presents the key KPIs for the asynchronous e-learning courses, including user satisfaction scores at the time of writing.

Type of entity	Entities involved	Users involved	Certificates issue	Satisfaction questionnaires	User satisfaction
Ministry	1	390	264	59	4.49

Tab 3. Key KPIs for asynchronous e-learning training courses

4.2 In-person Classes

During in-person training sessions, the "Cyber Sapere" program adopted an innovative method based on the principles of edugaming — a tool for active learning. Each session begins with a preliminary phase in which major cyber threats are contextualized through an analysis of data drawn from operational arrangements provided by the National Cybersecurity Agency [9], with specific concern for the field of education.
Participants are then directly involved in a structured competition covering important cybersecurity topics, designed to stimulate learning through gamification. Specifically, participants are asked to use the Kahoot! platform to answer a series of questions on the topic. Individual performance is assessed on the basis of two criteria: the accuracy of answers and the speed of completion.
Following each question, the topics covered in the test are explored further through multimedia materials and micro-lessons delivered by qualified instructors to consolidate the knowledge acquired while encouraging critical reflection on the subjects.
Finally, to recognize and reward the top performers, the three participants with the highest rankings receive prizes in the form of promotional materials and branded merchandise provided by the program organizers.
This approach was adopted to encourage active participation and greater engagement, based on the premise that game-based learning can offer advantages over conventional teaching methods [12].
At the time of writing, 11 in-person training events have been held at the Ministry, universities, and AFAM institutions, each lasting 2 hours. The table below presents the key results of the in-person training courses, while subsequent tables provide a breakdown by institution for courses held at specific universities and AFAM institutions, organized by geographic area (North, Central, and South Italy).

Type of entity	Entities involved	Users involved	Certificates issue	Satisfaction questionnaire	User satisfaction
Universities AFAM Ministry	8 2 1	235 30 39	235 30 39	212 30 37	4.60 / 5.00 4.88 / 5.00 4.28 / 5.00
Totals & Media	12	272	272	192	4.58/ 5.00

Tab 4. Key KPIs for in-person training courses

University	Users involved	Satisfaction questionnaire	User satisfaction
Universities in Central Italy	40	-	-
Universities in Northern Italy	35	-	-
Universities in Northern Italy	23	23	4.54 / 5.00
Universities in Southern Italy	23	23	4.69 / 5.00
Universities in Northern Italy	17	17	4.37 / 5.00
Universities in Southern Italy	35	35	4.48 / 5.00
Universities in Central Italy	38	38	4.61 / 5.00
Universities in Central Italy	80	77	4.69 / 5.00
Totals & Media	272	212	4.60 / 5.00

Tab 5. Key KPIs for in-person training courses at universities (by geographic area)

AFAM	Users involved	Satisfaction questionnaire	User satisfaction
AFAM Institutions in Southern Italy	20	20	4.86 / 5.00
AFAM Institutions in Northern Italy	10	10	4.90 / 5.00
Totals & Media	30	30	4.88 / 5.00

Tab 6. Key KPIs for in-person training courses at AFAM institutions (by geographic area)

5. Discussion

A detailed analysis of user satisfaction data across the three training formats tested within the "Cyber Sapere" program — synchronous e-learning, asynchronous e-learning, and in-person sessions structured around edugaming concepts — shows that participants clearly favor in-person training experiences featuring interactive game-based dynamics. In particular, the in-person edugaming format achieved an overall user satisfaction score[1] of 4.54 out of 5, approximately 30% higher than the 3.54 out of 5 scored by the synchronous e-learning course, and 2% higher than the 4.49 out of 5 scored by the asynchronous e-learning course.
Based on data from all three course types, the results are illustrated in the diagram below.

[1] The satisfaction score for each course was calculated as a weighted average of the ratings received and the number of completed questionnaires.

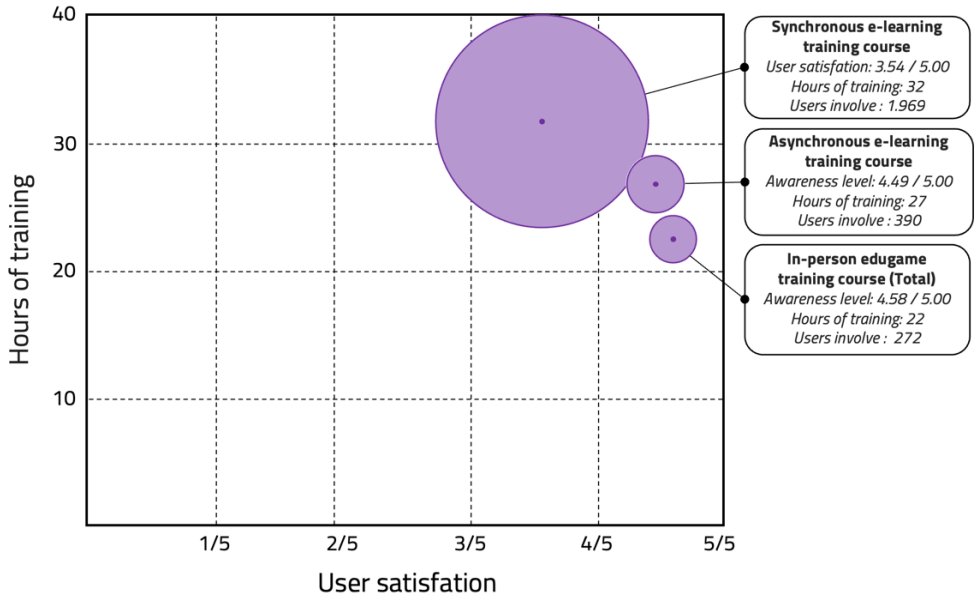

Fig. 1. Relationship between course satisfaction levels, number of training hours, and number of users involved across the training formats of the "Cyber Sapere" program

The chart illustrates the relationship between three key variables: course satisfaction levels, number of training hours, and number of users involved — the latter represented by bubble size. Specifically, the size of each bubble is proportional to the number of participants trained. The distribution of points on the chart also allows for a joint interpretation of training volume and perceived learning effectiveness. Points in the upper right area represent situations marked by a high number of training hours combined with higher satisfaction levels. In summary, the best results are represented by the largest bubbles in the upper right area, as they simultaneously reflect broad participation, intensive training activity, and a positive assessment of the learning experience.

The quantitative results show that edugaming-based teaching methods foster a stronger perception of learning effectiveness. This finding is consistent with the literature on experiential learning and gamification, which suggests that incorporating game-based elements into educational contexts can stimulate intrinsic motivation, facilitate the understanding of complex concepts, and encourage active participation [12].

By contrast, e-learning formats — while offering significant advantages in terms of flexibility, accessibility, and scalability — appear to generate lower levels of perceived satisfaction in the context analyzed. In particular, asynchronous sessions, while useful for independent learning, are less effective at supporting interaction and peer exchange, whereas synchronous sessions allow for real-time interaction but fall short of fully replicating the experiential and immersive quality of in-person activities. Interactions with participants and institutional leadership where in-person training took place revealed a significant level of interest in the adopted edugaming method. This was further reflected in the willingness expressed by institutions to plan future training initiatives based on the same approach. Overall, these findings appear to support the hypothesis that users prefer an edugaming format.

6. Conclusion

It should be noted that this study was conducted on a purposive and diverse sample of academic institutions and organizations. While not fully representative of the entire academic landscape, the sample of training participants is statistically significant, both in terms of the number of institutions involved and the number of participants. The academic background shared by participants helps contain intra-sample variability, strengthening the internal validity of the analysis and improving the reliability of the empirical findings. In particular, the consistency of the professional profiles of the participants facilitates data normalization, reducing the incidence of confounding factors and increasing the overall robustness of the results.

Overall, user satisfaction data suggest that integrating innovative teaching methods based on edutainment and gamification, tested in in-person training contexts, may represent a key factor in improving the perceived effectiveness of training programs. These findings support the adoption of

hybrid teaching models in which the digital component is complemented and enhanced by immersive and interactive experiences, aiming to maximize learning outcomes and user satisfaction.
Despite clear empirical evidence of a higher level of satisfaction with edugaming-based solutions among training participants, the "Cyber Sapere" program initially chose to reserve this approach exclusively for in-person activities. On the one hand, this choice fosters closer interaction between participants and instructors with positive effects on learning and teaching dynamics; on the other hand, it introduces a significant scalability limitation, as it reduces both the number of course hours and the number of participants that can be reached. While this choice is entirely sustainable, this constraint could become particularly relevant if the initiative were to be expanded with the goal of extending the training offering to a broader audience or making the format replicable in non-academic settings as well.
A further relevant aspect in assessing the effectiveness of edugaming solutions and training programs in general concerns whether the learning experience can generate significant and lasting changes in organizational culture and individual behavior, but measuring the impact of specialized training courses on the overall security posture of the academic system — one of the program's strategic objectives — is particularly complex. This is due to the highly dynamic nature of cyber threats and the limited size of the participant sample. This complexity reflects the inherent limitations of training impact assessment models [13] and the evaluation of return on investment (ROI) [14]. In particular, assessing the effects on organizational behavior and, above all, on systemic outcomes presents significant challenges, especially in complex and constantly evolving contexts such as cybersecurity. While it is reasonable to assume that individual training sessions produce positive effects on participants, it is equally clear that a systemic and ongoing approach to training is necessary. Therefore, it is essential to ensure that training is consistent, widespread, and sustained over time, reaching all members of the academic community — including administrative and technical staff, faculty, and leadership — in order to bring about structural change in security culture and organizational behavior.
As the program's implementation period draws to a close, and in light of the analysis of further training activities planned within the "Cyber Sapere" initiative, it seems appropriate to consider introducing additional measures to complement those already implemented. In particular, the adoption of e-learning edugaming solutions could be considered, with the goal of expanding the participant base while maintaining an adequate level of immersiveness. This approach would combine the benefits of edugaming in terms of engagement and interactivity with greater scalability and accessibility, while also expanding the content beyond basic training to include highly specialized courses.
A further area of intervention concerns the introduction of a cyclical assessment process to measure progress in security posture, building on the initial assessment conducted as part of the initiative. This activity should be conducted according to a structured methodology framework to ensure the consistency, replicability, and reliability of results.
Finally, it is proposed that training activities be supported by systematic awareness-raising initiatives aimed at engaging the main representatives of academia. The objective is to promote greater awareness of the importance of continuous, widespread, and pervasive cybersecurity training, in line with the strategic goals of the program.

REFERENCES

[1] Barruga, M.B. «SYSTEMATIC REVIEW OF CYBERSECURITY FRAMEWORKS FOR HIGHER EDUCATION INSTITUTIONS: CHARACTERISTICS, COMPONENTS, AND CHALLENGES», Int. J. Appl. Math., 2025, vol. 38, fasc. 4S, pp. 1180–1198, doi: 10.12732/ijam.v38i4s.299.

[2] Agenzia per la Cybersicurezza Nazionale. 2026. Operational Summary – March 2026. https://www.acn.gov.it/portale/documents/20119/1176749/Operational_Summary_mar26_CLEAR.pdf

[3] Amjad K., Ishaq K., Nawaz N. A, Rosdi, F., Dogar A. B., e Khan F. A., «Unlocking Cybersecurity: A Game-Changing Framework for Training and Awareness—A Systematic Review», Hum. Behav. Emerg. Technol., vol. 2025, fasc. 1, 2025, doi: 10.1155/hbe2/9982666.

[4] De Angel R. M., Ramos R. F., Magcuyao J. P. H., Calimbo A. L., Lagman A. C, «AI-Driven Gamification for Cybersecurity Literacy in Higher Education», in 2025 International Workshop on Artificial Intelligence and Education (WAIE), set. 2025, pp. 95–100. doi: 10.1109/WAIE67422.2025.1138110]8.

[5] Kallonas C., Piki A., Stavrou E., «Empowering Professionals: A Generative AI Approach to Personalized Cybersecurity Learning», in 2024 IEEE Global Engineering Education Conference (EDUCON), mag. 2024, pp. 1–10. doi: 10.1109/EDUCON60312.2024.10578894.

[6] Montefusco S., Bernardini M., Micozzi P., «Improving the Safety Posture of Italian Research Sector in Light of New European Regulatory Frameworks», In 15th International Conference New Perspectives in Science Education (18 March 2026 Online Event; 19-20 March 2026 in Florence, Italy), vol. 1, pp. 118–126, 2026, doi: https://doi.org/10.82075/NPSE_2026_15_PAG.118 .

[7] Matovu R., Nwokeji J. C., Holmes T., Rahman T., «Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges», in 2022 IEEE Frontiers in Education Conference (FIE), ott. 2022, pp. 1–9. doi: 10.1109/FIE56618.2022.9962519.

[8] Pramod D., «Gamification in cybersecurity education; a state of the art review and research agenda», Journal of Applied Research in Higher Education, vol. 17, fasc. 4, pp. 1162–1180, giu. 2024, doi: 10.1108/JARHE-02-2024-0072.

[9] Xiao H., Wei H., Liao Q., Ye Q., Cao C., Zhong Y., «Exploring the gamification of cybersecurity education in higher education institutions: An analytical study», SHS Web of Conf., vol. 166, p. 01036, 2023, doi: 10.1051/shsconf/202316601036.

[10] Agenzia per la Cybersicurezza Nazionale. 2022. "Strategia nazionale di cybersicurezza 2022–2026." https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

[11] Micozzi, P., Montefusco, S. (2025). Digitalization of Services and the Creation of New Barriers: Upskilling and Reskilling as a Way to Mitigate the Digital Divide. In Firenze Pixel, The Future of Education Conference Proceedings 2025. Filodiritto Publisher. 561-567. doi: https://doi.org/10.26352/L625_2384-9509

[12] Wang, LH., Chen, B., Hwang, GJ. et al. “Effects of digital game-based STEM education on students’ learning achievement: a meta-analysis.” IJ STEM, 2022, Ed 9, 26. https://doi.org/10.1186/s40594-022-00344-0

[13] Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating training programs: The four levels* (3rd ed.). Berrett-Koehler.

[14] Phillips, J. J. (2003). *Return on investment in training and performance improvement programs* (2nd ed.). Butterworth-Heinemann.