Addressing Cybersecurity Issues Through Collaborative Digital PBL: A Case Study of University-Government-Industry Collaboration on Romance Scams

Shoji HAENO

SPARKJAPAN Co., Ltd., Miyazaki, Japan
Industry–Academia–Government Digital Education Initiative, Miyazaki Region

FUTUREd, Volume 1, Issue 1 (2026)

Pages: 69 – 75

ISSN: 2760-8263 (print)
ISSN: 2760-8271 (Online)

Keywords:

cybersecurity education, project-based learning, industry-academia-government collaboration, liberal arts, regional digital human resource development

Corresponding author(s):

Shoji Haeno
s-haeno@spark.ne.jp

CC BY

Abstract: This paper presented a qualitative case study of an industry–academia–government collaborative Project–Based Learning (PBL) initiative designed to raise awareness of romance scams in Miyazaki Prefecture, Japan. The study examined how interdisciplinary students from non-computing disciplines, including those with liberal arts backgrounds, contributed to regional cybersecurity awareness through structured collaboration informed by a helix-based framework. This study also situates the initiative within a Quadruple Helix framework of regional collaboration. The project integrated students' critical and contextual thinking with anonymized cybercrime data and technical guidance from an IT company. Students engaged in data interpretation, content development, and dissemination, producing awareness videos for regional audiences. Findings indicated that students applied interpretive capacity—the ability to discern social issues, translate them into context, and communicate them effectively—through interdisciplinary collaboration. The case shows that collaborative PBL enhanced participants' digital skills and regional cybersecurity awareness, while enabling students from non-computing disciplines, including those with liberal arts backgrounds, to act as contributors to solving social issues. Although limited in scale, the study highlighted the role of interdisciplinary education in the era of digital transformation.

1. INTRODUCTION

In recent years, rapid digital transformation has reshaped social, economic, and administrative systems worldwide. Alongside its benefits, digitalization has generated new forms of vulnerability, particularly in regional areas where resources and digital literacy may be unevenly distributed. Cybercrime, online fraud, and information security breaches increasingly affect local communities, underscoring the urgent need for comprehensive digital human resource development. In Japan, national strategies emphasize the cultivation of advanced digital professionals; however, regional disparities in

digital capacity remain a persistent concern. Universities located in regional areas are uniquely positioned to bridge this gap by fostering locally grounded yet globally informed talent.

Promoting digital transformation requires not only conventional approaches to digital human resource development but also an increased emphasis on the role of liberal arts education. In addressing complex social and technological challenges across organizations, regions, and society, technical expertise remains important; however, greater importance lies in the social mobilization of interpretive capacity—grounded in flexible thinking, critical reflection, collaboration, and the integration of knowledge within human-centered contexts. This study examines how such capabilities can be mobilized to address regional cybersecurity challenges.

This study examines a collaborative cybersecurity awareness initiative conducted in Miyazaki Prefecture, Japan. The project brought together police authorities, an IT company, and undergraduate students from non-computing disciplines to analyze regional cybercrime trends and develop public awareness materials. Participation in the project was voluntary and not formally integrated into the university curriculum. The purpose of this paper is to explore how interdisciplinary student participation contributes to regional cybersecurity awareness and institutional collaboration. The collaboration originated from the author's leadership of the Industry-Academia-Government Digital Education Initiative in the Miyazaki region. Together with students participating in the author's digital career support workshops, the author had gradually proposed a series of small-scale collaborative activities to the prefectural police. Through these continued efforts, trust was established among the stakeholders. At the same time, the police faced a growing need for new approaches to raise awareness of cybercrimes such as romance scams and were receptive to the flexible thinking and expressive abilities of non-specialist students. The alignment of trust-based relationships and institutional needs enabled the development of a full-scale collaboration. By documenting this initiative, the study contributes empirical insight into how regional multi-stakeholder collaboration can support cybersecurity awareness and digital resilience. Despite growing attention to cybersecurity education, relatively few studies have examined how students from non-computing disciplines can participate in regional cybersecurity initiatives through collaboration with public institutions and industry. In particular, empirical studies exploring such collaboration in regional contexts remain limited. This study particularly focuses on interpretive capacity as a core competence underlying such interdisciplinary engagement.

2. BACKGROUND AND CHALLENGES

Japan's digital human resource strategy has begun to be updated in response to the era of AI. Public documents have started to emphasize the importance of foundational DX literacy for society at large and have proposed the role of business architects who require human and conceptual skills for addressing digital challenges (METI, 2024a; METI, 2024b; Digital Agency, 2026). However, individuals with flexible thinking and strong initiative - such as students from non-computing disciplines - remain insufficiently recognized as valuable contributors capable of effectively advancing organizational or regional digital initiatives, despite their potential. Regional communities face particular challenges. Limited access to digital education, demographic aging, and resource constraints heighten susceptibility to cybercrime. Moreover, collaboration between educational institutions, industry, and public agencies often remains fragmented. This case study was conducted with the expectation that, in order to mitigate such fragmentation, fostering career awareness among individuals expected to address regional digital challenges, together with the effective implementation of collaborative and practice-based learning through PBL, would function as a means of problem solving.

However, sustaining such industry-led experiential collaborative activities proved challenging. Although both industry and public agencies exhibited strong demand for student collaboration,

recruiting participants was difficult. In this case, student engagement relied primarily on the cooperation of participants from the digital learning sessions and digital career-support workshops organized by the author. While this approach was effective in attracting highly motivated participants, it remained insufficiently developed as an institutional foundation for the stable provision of PBL. Moving forward, it will be essential for industry and public sectors to raise awareness of such initiatives in order to recruit students more effectively. Ideally, continuous student participation would be secured through the allocation of academic credits.

From a theoretical perspective, collaborative initiatives involving universities, industry, government, and society can be interpreted through innovation ecosystem frameworks. The Triple Helix model conceptualizes innovation as interactions among universities, industry, and government (Etzkowitz & Leydesdorff, 2000). Carayannis and Campbell (2009) expanded this framework into the Quadruple Helix model by incorporating civil society as a fourth helix, emphasizing the role of public participation in innovation ecosystems. Recent studies have applied this perspective to digital society issues. For example, Kulikauskienė (2021) proposed a Quadruple Helix framework for addressing digital inclusion, highlighting the collaborative roles of academia, industry, government, and society in solving digital challenges. The present study interprets the Miyazaki initiative as a regional collaborative practice that reflects such a multi-stakeholder framework. In this sense, the initiative provides a small-scale empirical example illustrating how Quadruple Helix interactions can emerge in regional digital resilience initiatives.

3. METHODOLOGY

3.1. Research Design

This study was designed as a qualitative exploratory case study examining the implementation process and initial outcomes of a cybersecurity awareness initiative involving the participation of students from non-computing disciplines (including liberal arts) conducted in Miyazaki Prefecture through collaboration among police authorities, an IT company, and university students. The objective is to analyze how interdisciplinary student participation contributed to regional cybersecurity awareness and institutional collaboration. Given the small-scale and practice-oriented nature of the initiative, the study emphasizes contextual depth rather than statistical generalization. The project included a practice-based collaborative component in which police officials provided statistical data, while the effectiveness of the cybersecurity awareness video produced by the students was evaluated by both university faculty and police representatives from the perspective of public communication. In addition, the study offers an exploratory model of institutional collaboration within industry–academia–government partnerships for addressing regional challenges.

3.2. Participants

Approximately five undergraduate students majoring in non-computing disciplines, including liberal arts fields, participated in the project. Under the guidance of a director from an IT company, the students analyzed regional cybercrime trends, proposed awareness strategies, and produced informational videos.

3.3. Data Collection

The primary data consisted of anonymized internal cybercrime statistical data provided by the Miyazaki Prefectural Police under institutional agreement. The dataset included the number of incidents by crime category over a specified period. No personal data were accessed in the course of this study. Students analyzed statistical trends to extract regional characteristics and risk patterns. Their analytical results were submitted to police representatives, who provided expert review regarding interpretive validity and contextual appropriateness. This activity was implemented as an extended collaboration of a digital career support workshop organized by the author in partnership with the police. All participants joined voluntarily as a continuation of the aforementioned workshop, and although some university faculty members provided support and review, the activity

was not directly associated with formal university courses or curricula at the time. While the participating students did not necessarily possess advanced digital skills, they improved their competencies through guided instruction in the use of spreadsheet software such as Excel, presentation skills, the use of generative AI, information dissemination, and collaborative communication through chat-based tools. The study complied with relevant ethical standards governing research collaboration and data use. Several compliance-related considerations emerged in this study. The use of anonymized cybercrime data provided by the police required careful attention to data handling, privacy protection, and institutional agreements. In this sense, ensuring ethical compliance did not constitute a major barrier but rather functioned as an important learning opportunity. The collaboration enabled students to engage with real-world ethical standards, including data responsibility and communication ethics, thereby enhancing their understanding of compliance in practice.

3.4. Analytical Approach

Analysis was conducted using descriptive and interpretive methods. Crime frequency, financial damage, distribution patterns, category–based tendencies, and temporal changes were organized into comparative categories and time-series trends and examined. From these observations, thematic interpretations regarding regional digital risk and social vulnerability were derived. Basic indicators - including year-on-year increases in financial damage, monthly crime-type frequencies, and patterns of peak occurrence—were used to identify high-risk categories and trends in crime victimization.

3.5. Modelling a Collaborative Framework for Regional Cybersecurity Awareness

The project was implemented through collaboration among a university (students from non-computing disciplines), a regional IT company, and the Miyazaki Prefectural Police, with the broader community positioned as the target of cybersecurity awareness activities. This structure represents a practical configuration of the Quadruple Helix model, encompassing academia, industry, government, and civil society in a regional context. Within this framework, each stakeholder assumed complementary roles, and the integration of data analysis, contextual interpretation, and public communication was achieved.

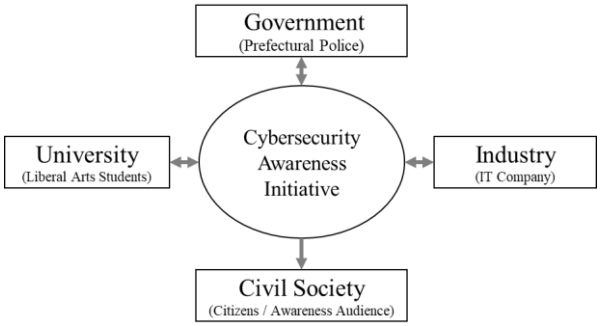

Figure 1 - Collaborative framework illustrating the application of the Quadruple Helix model in the Miyazaki cybersecurity awareness initiative

4. PROJECT DESIGN AND IMPLEMENTATION

The initiative was structured around tripartite collaboration among Miyazaki Prefectural Police, a regional IT company, and university students. Police authorities provided anonymized cybercrime statistics and contextual explanations. The IT company offered technical and strategic guidance. Students conducted analysis and developed awareness materials, including video content tailored to regional audiences. Workshops facilitated iterative discussion, enabling participants to integrate statistical evidence with contextual understanding. This collaborative design emphasized practical engagement and mutual learning. This collaboration was designed by the author as an extension of a workshop-based PBL initiative following a consultation request from the police in June 2025. Prior to the end-of-term examinations, students were provided with an explanation of the project and their willingness to participate, as well as preferred implementation schedules, were confirmed. The activity was conducted outside formal class time and began in earnest after the examinations, continuing into the summer vacation period. The initial draft was completed within approximately one week, followed by a short period of stakeholder review,

and was largely finalized by September. The completed materials were broadcast on a local public display system in November, and in December, the participants received a letter of appreciation from the police and the project was covered by local media.

5. OUTCOMES

The project yielded several observable outcomes. First, students increased their awareness of regional cybercrime patterns and developed a sense of the urgency of cybercrime as a critical issue even in local cities in Japan. Second, they gained experience in interpreting real crime statistics provided under ethical considerations within social contexts and communicating their findings to society based on creative perspectives. Third, the collaboration demonstrated a practical example of communication among regional institutions, private companies, and educational organizations. Fourth, awareness materials were produced and disseminated, contributing to increased public awareness of cybercrime and the development of digital human resources in the region.

Furthermore, participating students gained practical experiences of success through recognition from the police and coverage by local media, which allowed them to perceive that their activities had a tangible impact on society. They also received feedback from friends and family, including praise for their activities and recognition of the importance of cybercrime awareness. Although exploratory in scale, these outcomes indicated that PBL initiatives such as this case could enhance both the development of individuals capable of recognizing and promoting solutions to digital challenges and regional engagement.

6. BENEFITS, LIMITATIONS, AND REPLICABILITY

The initiative demonstrates several advantages. It leverages liberal arts competencies—critical thinking, ethical reflection, and communication—to complement technical cybersecurity efforts. It also fosters institutional trust among academia, industry, and public authorities.

Although context-dependent, the model may be adaptable to other regional settings, provided that stakeholders commit to collaborative engagement and data-sharing frameworks. In this case, the initiative originated from trust-building through the accumulation of small-scale collaborative activities led by private-sector digital professionals engaged in cross-sectoral support across academia, industry, and government. This was followed by the clarification of mutual benefits and alignment with institutional needs, which enabled project implementation and knowledge transfer. Once the project gained momentum, the capabilities of public institutions and students exceeded initial expectations. Such regionally embedded leadership can provide role models for the next generation and facilitate skill transfer, suggesting that similar approaches may be applicable in other regional contexts.

However, this study has several limitations. The small number of participants and the single-region case design limit the generalizability of the findings. The study does not include control groups or pre–post comparisons; therefore, causal claims regarding educational effectiveness remain limited. Nevertheless, the research provides meaningful insight into interdisciplinary collaboration under real institutional conditions.

7. FUTURE DIRECTIONS

Ideally, the continuous recruitment of student participants would be institutionally secured by integrating the program into the formal curriculum and granting academic credit, thereby establishing a stable and sustainable cycle of human resource development. At present, participation is fostered primarily through voluntary mechanisms such as regional digital skills workshops and digital–sector career support programs. While this approach cultivates highly motivated participants, it remains underdeveloped as a long–term institutional foundation. Future efforts should expand collaborative partnerships, secure financial and human resources, and align the initiative with broader policy frameworks—such as Japan's Digital Agency policies and METI's digital human resource strategies—to connect regionally developed talent with national digital human

resource strategies.

Furthermore, while this case involved students from non-computing disciplines, increasing participation by students majoring in digital and information security fields would enable more substantive interdisciplinary exchange and contribute to the further development of PBL design. Interaction between non-computing students and digital specialists can generate intellectual stimulation, enhance mutual understanding, and promote the resolution of regional challenges. At the same time, such interaction can raise awareness of roles and career paths that contribute to problem-solving in the AI era, and serve as a model for developing individuals capable of interpreting, collaborating on, and contributing to the resolution of social issues.

8. CONCLUSION

The Miyazaki initiative demonstrates how collaboration among universities, public institutions, private-sector actors, and local communities can contribute to enhancing cybersecurity awareness and strengthening digital resilience at the regional level. The project further clarifies that collaborative education emphasizing critical thinking and interpretive capacity can function as a practical approach to addressing digital risks while strengthening connections between higher education and local society.

This case study aimed to prevent cybercrime through regional collaboration among academia, industry, government, and society, involving students from non-computing disciplines. Such problem-solving initiatives enhance recognition of these students—whose potential as future advanced digital human resources has not been sufficiently acknowledged—and provide them with practical experiences of success. In doing so, the initiative expands the social foundation of advanced digital human resource development beyond a sole reliance on technical expertise. In contrast to conventional digital human resource development models that emphasize technical specialists and system-oriented responses, it highlights human agency—grounded in interpretive capacity, critical thinking, and collaboration—as well as the active participation of diverse stakeholders, including the public. In this respect, the initiative is consistent with METI's concept of the "business architect." Furthermore, expanding participation to include students specializing in digital fields can generate constructive interdisciplinary interaction and support more robust human resource development.

From a theoretical perspective, these findings can be interpreted through the framework of innovation studies. This study adopts the Quadruple Helix model to account for the role of civil society, particularly local communities and students, as active participants in regional cybersecurity awareness and digital resilience, building on the Triple Helix model, which conceptualizes innovation as interactions among universities, industry, and government (Etzkowitz & Leydesdorff), while the Quadruple Helix model further incorporates civil society as a key participant in innovation ecosystems (Carayannis & Campbell, 2009). In this sense, the Miyazaki initiative represents a practical example of the Quadruple Helix in action, where academia, industry, government, and society collaboratively address challenges of the digital era, particularly in the areas of cybersecurity awareness and digital inclusion. Although exploratory in scale, this case suggests that liberal arts–based collaborative education can function as a practical mechanism for activating Quadruple Helix relationships in regional digital governance.

REFERENCES

Etzkowitz, H., & Leydesdorff, L. (2000).

The dynamics of innovation: From national systems and "Mode 2" to a triple helix of university–industry–government relations. Research Policy, 29(2), 109–123. https://doi.org/10.1016/S0048-7333(99)00055-4

Carayannis, E. G., & Campbell, D. F. J. (2009).

"Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. International Journal of Technology Management, 46(3/4), 201–234.

https://doi.org/10.1504/IJTM.2009.023374

Kulikauskienė, K. (2021). The theoretical quadruple helix model for digital inclusion increase. Management of Organizations: Systematic Research, 85(1), 13–32. https://doi.org/10.1515/mosr-2021-0002

National Police Agency of Japan. (2023).Overview of Reported Cases and Arrests Related to Special Fraud and SNS-Based Investment and Romance Scams https://www.npa.go.jp/publications/statistics/sousa/sagi.htm

National Police Agency of Japan. (2023). Cybercrime situation report. https://www.npa.go.jp/publications/statistics/cybersecurity/

Ministry of Economy, Trade and Industry (METI). (2024a).

Digital skill standard (DSS). https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html

Digital Agency. (2023).Digital society initiative. https://www.digital.go.jp/policies/digital_human_resources