Journal of Contemporary Educational Research, 2025, Volume 9, Issue 9
http://ojs.bbwpublisher.com/index.php/JCER
ISSN Online: 2208-8474
ISSN Print: 2208-8466

Research on the Collaborative Governance Path for the Digital Transformation of Community Cybersecurity Education in Foshan

Zhuqing Chen*, Jinfeng Li, Tianjiao Wang

School of Computing, Neusoft Institute Guangdong, Foshan 528225, Guangdong, China

**Author to whom correspondence should be addressed.*

Abstract: The proliferation of smart communities in Foshan has led to increasingly diverse and prevalent cybersecurity risks for residents. This trend has rendered traditional cybersecurity education models inadequate in addressing the challenges of the digital era. Guided by the theory of collaborative governance and the framework of digital transformation, this paper examines the multi-stakeholder collaborative mechanism involving the government, businesses, community organizations, universities, and residents. It subsequently proposes a series of implementation strategies such as digitizing educational content, intellectualizing platforms, contextualizing delivery methods, and refining management precision. Studies demonstrate that this model enables effective resource integration, improves educational precision, and boosts resident engagement. It represents a fundamental shift from unilateral dissemination to multi-party interaction and from decentralized management to collaborative synergy, offering a replicable "Foshan Model" for digital governance at the community level.

Keywords: Collaborative governance path; Digital transformation; Community cybersecurity education

Online publication: Oct 22, 2025

1. Introduction

The ongoing development of smart communities in Foshan has led to a substantial proliferation of digital infrastructure. Concurrently, cybersecurity threats have become increasingly characterized by their diversity and high frequency. Issues such as online fraud, data breaches, and smart device flaws are becoming increasingly prominent, posing major challenges to both the daily safety of residents and the effectiveness of grassroots governance. Relying on one-way instruction and centralized training, the traditional cybersecurity education model has limited coverage and fails to cope with increasingly complex and dynamic digital threats. Consequently, a substantial disconnect exists between the educational material and residents' real-world needs.

Hence, the digital transformation of community cybersecurity education anchored in a collaborative governance model that seamlessly integrates government, enterprise, community, academic, and citizen

resources has become the linchpin for effectively elevating public cybersecurity awareness. Drawing upon the empirical context of Foshan's smart community construction, this article interrogates the confluence of digital transformation and collaborative governance mechanisms within cybersecurity education. It seeks to articulate a novel community education model fit for the digital era. Thereby, it contributes a replicable practice sample for enhancing grassroots digital governance in Foshan and establishes a conceptual-reference framework for cybersecurity pedagogy innovation in smart communities, with implications for the Greater Bay Area and beyond.

2. Literature review and theoretical framework

Community cybersecurity education has become a critical element of grassroots digital governance. Previous research has predominantly concentrated on the cybersecurity awareness of specific demographics, such as university students or the elderly. These studies emphasize enhancing protective capabilities through diverse support systems, scenario-based simulations, and legal education [1]. However, a common limitation among these studies is their oversight of the unique characteristics and diversity of general community residents, particularly within geographically defined communities. Moreover, they seldom provide a systematic exploration of the digital transformation pathways for the educational models themselves [2].

Digital transformation unlocks new potential for community cybersecurity education, manifesting in three key dimensions. Firstly, it enhances precision by leveraging AI and big data to create resident risk profiles and personalized content delivery. Secondly, it boosts engagement through immersive learning experiences and trusted incentive systems built with tools like VR and block-chain [3]. Thirdly, it ensures sustainability by adopting platform-based, data-driven approaches that reduce long-term operational costs [4].

Collaborative governance theory emphasizes how multiple stakeholders, including governments, businesses, social organizations, and citizens has created public value through cooperation and resource sharing [5]. Applied to community education, this approach helps address inherent problems in traditional governance models, such as fragmented resources, ambiguous accountability, and slow response times. It establishes a collaborative network that clarifies roles and mechanisms for coordination, thereby forging a powerful synergy for educational initiatives.

Accordingly, this study advances an analytical framework synthesizing the forces of collaborative governance and digital transformation. This framework employs collaborative governance theory as its institutional foundation, defining the roles and collaborative methods of diverse stakeholders to address the questions of "who governs and how they collaborate". Simultaneously, it adopts digital transformation as its technical pathway to advance the intelligent and contextualized evolution of educational content, platforms, and methodologies, thereby solving the problems of "what technology to use and how to educate".

3. Current situation and problems of community cybersecurity education in Foshan

Currently, community cybersecurity education in Foshan remains in a nascent stage of development. It faces significant challenges in the content design, multi-stakeholder collaboration, the technology adoption, and resident engagement, which renders it ill-equipped to cope with the increasingly complex digital risk environment.

3.1. Lack of scenario-based and personalized educational content

Existing programs depend heavily on traditional methods like posters, brochures, and group lectures, offering only general-purpose information rather than content differentiated by age, occupation, or digital literacy level. Key risk scenarios, including seniors' difficulty with smart devices, adolescents' vulnerability to harmful content, and online shoppers' susceptibility to phishing scams has lack of tailored educational interventions. This lack of specific focus has created a gap between educational content and actual risks, resulting in low resident engagement and ineffective translation of knowledge into practice.

3.2. Inadequate inter-agency coordination and prominent resource dispersion

Cybersecurity education involves multiple stakeholders, including cyberspace regulators, civil affairs departments, subdistrict offices, property management firms, and private enterprises. However, the absence of an effective coordination mechanism and a unified platform hinder collaborative efforts. Departmental responsibilities lack clear delineation, data sharing is hampered by administrative barriers, and educational resources are inefficiently allocated, resulting in both duplication of effort and critical gaps in coverage. For example, datasets from the Civil Affairs Department on vulnerable populations, property access logs, and corporate risk alerts remain untimely. This lack of integration leads to inefficient targeting and outreach to high-risk groups.

3.3. Lagging technology application and limited digital transformation

Despite the progressive enhancement of smart community infrastructure in Foshan, the integration of technology into cybersecurity education remains inadequate. Existing educational platforms offer limited functionality, primarily serving as information dissemination channels. They lack cutting-edge intelligence modules such as AI-driven scenario simulation, immersive VR training, and blockchain-based incentive systems while acute data fragmentation keeps educational-behavior records, risk-case libraries, and resident profiles locked in isolated silos. This impedes precision education and dynamic assessment, preventing the formation of a cohesive digital education ecosystem.

3.4. Limited resident participation and an absence of incentive mechanisms

Community members predominantly adopt a passive stance toward cybersecurity education, showing low engagement propensity in training initiatives. The prevailing education model lacks sustained and effective motivational mechanisms. Its failure to link learning activities with community service benefits, credit points, or tangible rewards makes it difficult to establish a virtuous cycle of learning, contribution, and reward. Furthermore, volunteer programs and community mutual-aid systems remain underdeveloped. Consequently, residents' potential as key actors are not fully leveraged, undermining the long-term sustainability of educational outcomes.

Collectively, these challenges constrain both the efficacy and reach of Foshan's community cybersecurity education, necessitating urgent resolution through synergistic digital transformation and collaborative governance innovation.

4. Developing digital transformation pathways through a collaborative governance lens

Grounded in collaborative governance theory, this study develops innovative pathways for Foshan's community

cybersecurity education through dual dimensions: multi-stakeholder coordination mechanisms and digital transformation strategies (see **Figure 1**).

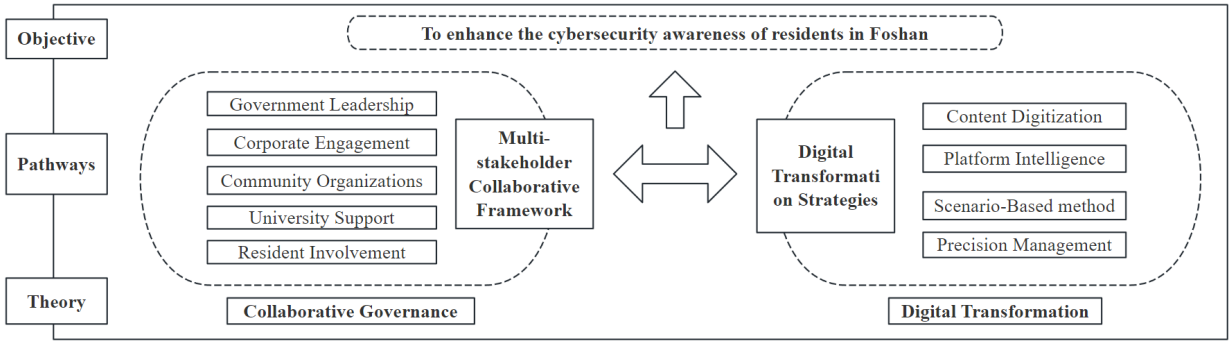

Figure 1. Developing digital transformation pathways through a collaborative governance lens.

4.1. Multi-stakeholder collaborative framework

Effective cybersecurity education must transcend traditional single-actor dominance by establishing a collaborative governance framework involving five key stakeholders, including government, enterprises, community organizations, universities, and residents. This requires clearly defining roles and coordination mechanisms to maximize efficacy.

4.1.1. Government leadership

The government should play a central role in top-level design and resource orchestration. Specifically, the Municipal Cyberspace Administration ought to spearhead the development of a digital strategy for community cybersecurity education. This includes clarifying departmental responsibilities, establishing inter-agency data-sharing protocols, and allocating funding to deploy integrated security monitoring platforms. Furthermore, incorporating cybersecurity metrics into grassroots-level performance evaluations will strengthen oversight and assessment.

4.1.2. Corporate engagement

Technology companies are critical drivers of technological empowerment. By leveraging expertise in AI, big data, and blockchain, they can develop tailored cybersecurity tools for communities. Through public-private partnerships and pilot programs, they facilitate technology adoption, provide cost-effective and lightweight maintenance, contribute to establishing security standards and data privacy protocols, and ultimately reinforce the overall cybersecurity infrastructure.

4.1.3. Community organizations

Community organizations which include the neighborhood committees, property management firms, and social work stations, serve as critical implementation nodes. They should establish cybersecurity community hubs to conduct specialized training such as fraud prevention workshops for seniors and cyber safety summer camps for youth. Customized content should then be disseminated through WeChat official accounts, while implementing resident cybersecurity profiles with point-based reward systems.

4.1.4. University support

Universities leverage their cybersecurity academic strengths and research resources to professionalize community education. This involves developing tiered curriculum systems, spearheading standardized community cybersecurity guidelines, establishing joint university-community training centers and practicum bases, systematizing educational content, and providing sustained scientific resources and intellectual capital to communities.

4.1.5. Resident involvement

Residents serve not only as recipients of education but also as active agents in governance. By spearheading anti-fraud advocacy teams, co-leading immersive VR training sessions, and promptly flagging suspicious activity, residents are moving from passive compliance to proactive guardianship and cultivating a community safety ethos built on collective engagement and shared resilience.

4.2. Digital transformation strategies

Digital transformation serves as the core enabler for educational efficacy enhancement, requiring intelligent, scenario-based, and precision-driven reforms across four dimensions, including content, platforms, methodologies, and management.

4.2.1. Content digitization

Leveraging intelligent algorithms, educational teams generate personalized cybersecurity content. By providing targeted anti-fraud scenarios, interactive quizzes, and VR simulation modules based on residents' digital profiles, they implement truly individualized instruction strategies.

4.2.2. Platform intelligence

Spearheaded by the Municipal Cyberspace Administration, a unified city-wide cloud platform for community cybersecurity education integrates multi-source datasets and intelligent tools. This platform enables online learning, risk simulation, incident reporting, and points-based reward management, eliminating data silos while establishing cross-system interoperability.

4.2.3. Scenario-based method

Community organizations embed cybersecurity knowledge into daily-life touch points access control systems, elevator displays, and parcel lockers. Meanwhile, tech firms develop culturally immersive VR experiences featuring local traditions like Foshan's lion dance, collaboratively realizing seamless integration of pervasive cybersecurity pedagogy.

4.2.4. Precision management

The management team has established a dynamic profiling system to assess residents' cybersecurity capabilities. By implementing tiered training programs with certification and integrating blockchain-based incentive points with community services, they have created a continuous cycle of learning, application, and reward that enhances the sustainability of the education initiative.

By fusing its multi-stakeholder governance model with cutting-edge digital transformation, Foshan can forge a resilient, three-pillar cybersecurity education paradigm that seamlessly integrates institutional frameworks, technological innovation, and a culture of shared vigilance. This paradigm will fundamentally

transform education from one-way instruction to two-way interaction and passive response to proactive prevention.

5. Retrospect and prospect

The dual-driven framework integrating collaborative governance and digital transformation provides a systematic solution for community cybersecurity education in Foshan. Empirical evidence demonstrates that this model effectively consolidates multi-stakeholder resources, enhances educational precision and resident engagement, facilitating a shift from unidirectional dissemination to multi-party interaction and from fragmented governance to systematic coordination.

Subsequent initiatives ought to investigate the deeper assimilation of generative artificial intelligence and related technological advances within grassroots governance frameworks. This necessitates fostering institutional creativity and cultural amalgamation, refining mechanisms for cybersecurity authentication and credit interoperability, while concurrently broadening the implementation domains of traditional culture within digital education platforms, thereby generating enduring impetus for the development of a sustainable community cybersecurity ecology.

Funding

2025 Foshan Social Science Planning Project, "Research on Pathways for Enhancing Cybersecurity Awareness Among Foshan Community Residents Empowered by Digital and Intelligent Technologies" (Project No.: 2025-GJ091)

Disclosure statement

The authors declare no conflict of interest.

References

[1] Zhu H, Hu P, 2018, Research on Problems and Countermeasures of University Campus Network Security Management. Social Sciences of Hunan, 2018(05): 98–109.

[2] Liu X, 2024, A Study on the Intervention of Group Work in Enhancing Cybersecurity Awareness Among the Elderly, thesis, Xihua University.

[3] Blažič J, Blažič B, 2024, Teaching and Learning Cybersecurity for European Youth by Applying Interactive Technology and Smart Education. Education and Information Technologies, 30(7): 1–28.

[4] Bulmer J, Lanng E, Clarke S, et al., 2024, Using Game-Based Learning to Teach Young People About Privacy and Online Safety. Interactive Learning Environments, 32(10): 6430–6450.

[5] Li H, 2014, An Analysis of Collaborative Governance Theory. Theory Monthly, 2014(01): 138–142.