Research on the Digital Transformation of University Security Management

Hailong Shen*

City Institute Dalian University of Technology, Dalian, 116102, China
**Corresponding author: shivy@sohu.com*

Abstract: *With the rapid development of information technology, the traditional university security management model can no longer meet current demands, and digital transformation has become an important development direction for university security management. This paper explores the necessity, current situation, and challenges of the digital transformation of university security management and proposes specific transformation strategies and pathways, aiming to provide valuable references for improving the level of university security management.*

Keywords: *university; security management; digital transformation; strategy*

Introduction

For many years, China has unswervingly implemented the strategies of invigorating the country through science and education and strengthening the nation with talent, achieving comprehensive and groundbreaking historical accomplishments in education, with the level of higher education massification significantly improved. However, with the continuous expansion of higher education and the increasing complexity of campus security environments, university security management is facing unprecedented challenges. The traditional security management model can no longer meet the growing security demands, making it urgent to enhance security management standards and efficiency through digital transformation.

Digital transformation is not only a technological innovation but also a reform of management concepts and models. By applying advanced information technology to campus security management, real-time monitoring, early warning, and rapid response to security risks can be achieved, improving the accuracy and effectiveness of security management. It also facilitates the integration and analysis of security data, providing a scientific basis for security management decision-making and promoting the development of university security management toward greater intelligence and refinement.

1. Necessity of Digital Transformation in University Security Management

1.1 Extreme Importance of Security Management

As important bases for talent cultivation, knowledge innovation, social services, cultural inheritance, and international exchange, universities shoulder the crucial responsibility of nurturing talent, and security is the prerequisite for the normal operation of all activities. Universities are densely populated, with numerous buildings and structures as well as complex equipment and facilities. Once a security incident occurs, it may result in enormous losses and significant impacts, diverting the institution's focus from its primary mission of education and teaching. Therefore, universities must pay close attention to security and security management issues, maintaining a high standard of security management and continuously improving its level. To achieve this, traditional methods have become inadequate, and digital transformation to enhance efficiency has become an effective and feasible solution.

1.2 Complex and Variable Security Threats

With the development of the times, universities are facing diversified security threats. In addition to the persistent traditional threats such as public security, laboratory safety, fire safety, food safety, and traffic safety, new security threats continue to emerge, with data security, cybersecurity, and mental

health becoming particularly prominent. The cultivation of safety awareness and emergency response capabilities among faculty and students also faces challenges, making the effective implementation of safety education and emergency drills an urgent issue. Digital transformation can leverage advanced technologies such as big data analysis, artificial intelligence, digital twins, the Internet of Things, and virtual reality to monitor and provide early warnings of various security risks in real time, enabling timely and effective countermeasures. It can conduct in-depth mining of campus security data to identify potential security risks; it can facilitate engaging safety education and virtual drills, reducing the difficulty of organizing drill activities; it can enhance the scientific, effective, and timely identification of risks, thereby eliminating potential safety hazards[1].

1.3 Management Efficiency Needs Improvement

At present, many universities still rely on paper and pen to record various security management data, resulting in low efficiency and poor timeliness, which can no longer meet the increasing demands of security management work. The adoption of digital technologies can enable real-time collection and rapid processing of campus security information, reduce the time cost of manual operations, lower the error rate, optimize management processes, reduce labor costs, improve work efficiency, and enhance the scientific basis for decision-making. For example, by using Internet of Things devices to monitor in real time the operational status of fire protection facilities and laboratory equipment on campus, management personnel can remotely check equipment conditions and promptly detect and handle abnormal situations.

1.4 Safety Needs of Faculty and Students Urgently Need to Be Met

With the development of China's economy and society, faculty and students have increasingly high expectations for campus security, hoping to study and live in a safe and convenient environment. Digital transformation can utilize advanced technological means to enhance the level of campus security management, creating a safer and more intelligent working, studying, and living environment for faculty and students. It can also provide more personalized security services, such as offering real-time safety alerts and emergency assistance functions through mobile applications, thereby enhancing the sense of security among faculty and students.

1.5 Need for Modernization of University Governance Capability

The essence of modernizing university governance capability lies in achieving high-quality educational development through optimizing resource allocation, improving decision-making efficiency, and strengthening risk response capability. There is a profound internal coupling between the modernization of university governance capability and the digital transformation of security management: the former provides the goal framework for the latter, while the latter offers technological empowerment and efficiency support for the former. In the face of increasingly complex security challenges, universities need to reconstruct the security management system through digital transformation, achieve data-driven security management, strengthen risk early warning and decision-making support, provide strong support for the modernization of university governance capability, and further promote the systematic upgrading of governance capability.

2. Current Situation and Challenges of the Digital Transformation of University Security Management

The digital transformation of university security management refers to the systematic reform process in which higher education institutions utilize digital technologies such as the Internet of Things, big data, and artificial intelligence to reconstruct the processes, mechanisms, and systems of security management, achieving data-driven, real-time, and intelligent risk identification and early warning, emergency preparedness and response, hidden hazard investigation and control, as well as operational monitoring and decision-making. The digital transformation of university security management can be regarded as a strategic reform of university security management. It involves not only technological upgrades but also dynamic and continuous changes in organizational structure, regulations, and safety culture. Ultimately, through technological empowerment, it breaks the information barriers and response delays inherent in traditional university security management, establishing a security management model characterized by comprehensive linkage and proactive defense.

2.1 Current Situation of the Digital Transformation of University Security Management

2.1.1 Certain Progress in Infrastructure Construction

In recent years, many universities have begun to explore and practice the digital transformation of security management. Numerous universities have strengthened the construction of campus network infrastructure and established basic digital facilities such as digital security monitoring systems and intelligent access control systems. Some universities have also introduced Internet of Things systems, providing hardware support for the digital transformation of security management.

2.1.2 Preliminary Application of Security Management Software Systems

Some universities have introduced security management information systems that include functional modules such as security incident registration, hidden hazard investigation and control, and fire safety management. However, due to the complexity of security management and the involvement of multiple departments—such as the security department managing public security and fire safety, the student affairs department managing student behavior and mental health, the logistics department managing food hygiene and construction safety, and the laboratory management department managing laboratory safety—data remain highly fragmented. Consequently, issues such as low system integration and poor data sharing still exist[2].

2.1.3 Low Rate of Automatic Data Collection

Although some universities have introduced security management systems, the data circulated within these systems are usually management data that require manual input, resulting in incomplete data and poor timeliness. For example, food hygiene management data are typically recorded as "daily control," "weekly inspection," and routine "spot checks," with the data manually entered by inspection personnel. This leads to two problems: on the one hand, the entered data are filtered by inspection personnel, which may cause data distortion or incompleteness; on the other hand, poor timeliness prevents immediate intervention to eliminate potential safety hazards. Ideally, intelligent digital devices should be used to conduct real-time monitoring of violations of safety regulations—such as cafeteria staff not wearing masks—so that violations can be recorded immediately, and real-time alerts can be sent to on-site management personnel.

2.1.4 Low Degree of Data Utilization

Although universities have accumulated a large amount of security-related data in daily management, the mining and analysis of these data are still insufficient, and their role in security management decision-making, risk identification, and prediction has not been fully utilized. For example, although video surveillance coverage on university campuses is now almost comprehensive, many abnormal student behaviors—such as students climbing through windows into dormitories after doors are locked at night or wandering in hallways late at night—are neither analyzed nor addressed.

Therefore, overall, the digital transformation of university security management is still at an early stage and faces many problems.

2.2 Challenges Faced in the Digital Transformation of University Security Management

2.2.1 Insufficient Top-Level Design

Although university leaders at all levels attach great importance to security management and have established various security management leadership groups and other corresponding organizational structures, comprehensive and systematic planning and design for the digital transformation of university security management through these organizations are rarely seen. There is a lack of long-term planning and sustained investment in the digital transformation of security management.

2.2.2 Severe Data Island Phenomenon

The data-sharing mechanisms among different departments within universities are inadequate, resulting in data being scattered across different systems and making interconnection difficult. Security management equipment and software from different manufacturers may have compatibility issues, preventing effective data integration and sharing, which affects the overall management effectiveness.

2.2.3 Insufficient Technical Application Capability

The digital transformation of security management requires interdisciplinary talents proficient in

both security management and information technology. However, such composite talents are relatively scarce, and the application of digital technologies remains superficial, failing to fully leverage their advantages. Some security management staff have low information technology literacy and insufficient mastery of new technologies, and relevant skills training is inadequate, making it difficult for them to adapt to new working models[3].

2.2.4 Limited Financial Investment

The digital transformation of security management requires substantial funding for purchasing equipment, building systems, and training personnel. Moreover, due to the rapid development of information technology, universities need continuous investment to update equipment and upgrade technologies to maintain the advancement and effectiveness of security management systems. However, many universities face difficulties in funding allocation and mobilization, making it hard to meet the financial demands of digital transformation.

2.2.5 Imperfect Management System

Under the context of digital transformation, the existing university security management systems may lag behind. Current regulations fail to clearly define the responsibilities and authorities of different departments in digital security management, resulting in unclear accountability and mutual shirking of responsibilities. In the processes of data collection, storage, and utilization, the lack of sound data security protection mechanisms increases the risk of data leakage and other security issues.

3. Strategies and Pathways for the Digital Transformation of University Security Management

University security management is a complex system engineering project involving multiple dimensions and multiple stakeholders. It requires scientifically defining management boundaries, integrating human-machine collaborative technologies, and establishing coordinated governance mechanisms to ultimately build a modern digital security management system characterized by the integration of "institution–technology–culture."

3.1 Building an Integrated Digital Security Management System

3.1.1 Conducting Top-Level Design for Security Management

A unified university-level leadership organization should be established to carry out regular work; a long-term plan for the digital transformation of security management should be formulated, with clear definitions of human-machine management boundaries; standardized construction of management mechanisms should be implemented, including hierarchical standards for the management responsibility system, standardized operating procedures, standardized models for safety education, standardized mechanisms for evaluation and improvement, and standardized emergency response plans; data governance should be carried out to standardize data content, format, and the data collection process; and a construction plan for digital infrastructure for security management should be developed.

3.1.2 Strengthening Security Infrastructure Construction

Establishing a security infrastructure network that covers the entire campus (including both physical space and virtual network space) and operates 24/7, together with corresponding software systems, is fundamental to achieving the digital transformation of security management. The ubiquitous campus-wide security infrastructure network should include, but is not limited to: basic campus network facilities and corresponding cybersecurity facilities; security protection systems, including closed-circuit television monitoring systems, anti-theft alarm systems, automatic fire alarm systems, perimeter security systems, access control management systems, electronic patrol systems, public broadcasting and intercom systems; building and laboratory safety facilities, including ventilation and exhaust systems, emergency lighting and evacuation indication systems, automatic fire extinguishing systems, and water, electricity, and lighting facilities; as well as other sensor networks based on the Internet of Things[4].

3.1.3 Integrating Campus Security Data

Campus security data are distributed across various subsystems and should be integrated to reduce the phenomenon of data silos. Since campus security data involve a high level of confidentiality, it is imperative to build a unified and secure campus security data platform, distinct from the smart campus

data platform. This platform will enable centralized storage and management of all types of campus security data, breaking down data silos, ensuring secure data storage, fast data processing, and convenient data utilization, thereby facilitating data analysis and mining to generate value from the data.

3.1.4 Improving Security Management Systems

Security management systems compatible with digital transformation should be established, clearly defining the responsibilities and divisions of labor among departments in the process of digital transformation. Security management processes should be redesigned to meet the requirements of the new digital environment and facilities. A data security assurance system should be established to ensure security throughout the entire process of data collection, storage, and utilization. For example, the responsibilities of the data management department should be specified to ensure data security and accuracy.

3.1.5 Establishing a Collaborative Working Mechanism

University security management is not solely the responsibility of the security department. Strengthening collaboration among different departments within universities and forming joint efforts are essential to establishing a relatively sound security management system. For instance, the security department should establish regular communication mechanisms with the student affairs department, logistics department, and others to jointly address campus security issues.

3.1.6 Forming a Closed Loop and Continuous Improvement

The digital transformation of security management is not static and requires the introduction of iterative optimization mechanisms to continuously evaluate, assess, and improve the security management system, while consistently introducing new technologies to enhance management effectiveness. For example, the PDCA cycle proposed by American quality management expert Walter A. Shewhart—Plan, Do, Check, and Act—can be adopted to continuously optimize the security management system.

3.2 Enhancing Data Mining and Application

3.2.1 Strengthening Data Analysis Capability Building

Multiple data sources, such as Internet of Things devices, video surveillance, and access control systems, should be integrated, and professional intelligent data analysis and simulation tools, as well as specialized personnel, should be introduced to conduct in-depth mining and analysis of campus security data. For example, in risk prediction, time-series analysis (LSTM networks) can be used to forecast high-risk periods for incidents (such as peaks of psychological crises during final exams), while spatial clustering (DBSCAN algorithm) can be employed to identify potential hazard areas. In behavior pattern recognition, computer vision technology (YOLO model) can be used to automatically detect abnormal behaviors in surveillance videos, such as crowd gathering or falling incidents.

3.2.2 Fully Exploring the Potential of Existing Facilities

Currently, universities are generally equipped with various security protection facilities, but their potential has yet to be fully explored. For instance, according to past fire protection design codes for buildings, most university dormitories are not equipped with temperature or smoke detectors inside rooms, making it difficult to detect a fire at the earliest stage, which can easily lead to greater losses. However, by fully utilizing the video surveillance cameras installed in dormitory corridors to monitor smoke generation in real time, fires can be detected at an early stage.

3.2.3 Establishing Risk Early-Warning Models

Based on the actual needs of campus security and with data-driven approaches as the core, multidimensional risk analysis should be conducted, including environmental, equipment, personnel, and psychological risks. Risk characteristic indicators should be extracted to establish early-warning models for various foreseeable incidents in universities. For example, by analyzing data of faculty and students who have fallen victim to telecom fraud, victim profiling can be created, and an early-warning model based on psychological assessment can be established to enable early psychological intervention, thereby reducing the incidence rate of telecom fraud.

3.2.4 Achieving Intelligent Decision Support

Focusing on "data-driven decision-making," artificial intelligence technologies should be employed to build an intelligent and visualized command platform. This platform should integrate functions such as risk identification and early warning, security incident detection and verification, one-click initiation of emergency plans, and resource allocation, providing intelligent decision support for security management[5].

3.3 Improving Digital Literacy of Personnel

3.3.1 Strengthening Training and Education

Regular training should be organized for faculty, students, and management personnel to enhance their acceptance and application capabilities of digital technologies. The digital skills level of faculty and staff should be incorporated into the work evaluation system. For example, regular training sessions should be conducted for faculty and staff on topics such as an introduction to digital transformation in security management, training on the use of security information systems, and training on data analysis tools, enabling them to adapt to the new digital security management system.

3.3.2 Cultivating Digital Thinking

Specific cases should be compiled and widely disseminated through publicity materials, lectures, and other forms to cultivate digital thinking among faculty, students, and management personnel, enabling them to actively use digital technologies to solve campus security problems. For instance, experts can be invited to share successful cases of digital security management to inspire innovative thinking.

3.3.3 Establishing Assessment and Incentive Mechanisms

The digital transformation of security management and its practical application should be incorporated into individual and departmental performance assessments to encourage active participation in digital security management practices and innovation. Individuals or teams who perform exceptionally in digital security management should be recognized and rewarded.

3.4 Increasing Financial Investment to Ensure Smooth Transformation Implementation

3.4.1 Securing Government and Social Support

Efforts should be made to actively seek government special funding support and social donations to expand funding sources. For example, universities can cooperate with enterprises to jointly carry out digital security management projects.

3.4.2 Optimizing Fund Allocation

The use of funds should be reasonably planned, with priority given to the construction of key systems and the procurement of essential equipment. For instance, priority funding should be allocated to the construction of university data platforms and the establishment of Internet of Things sensor networks.

3.4.3 Exploring Sustainable Development Models

Sustainable development models for the digital transformation of security management should be explored. Efficiency improvement and cost savings brought about by the application of new technologies should be leveraged to achieve a self-circulating funding mechanism. For example, by reducing the size of the management team and improving management efficiency through intelligent security management systems, the funds saved can be reinvested in the digital construction of security management.

Conclusion

The digital transformation of university security management is a key pathway to improving the level of security management. By building an integrated digital security management system, optimizing data utilization, and enhancing the digital literacy of personnel, current problems in security management can be effectively addressed, and management efficiency can be improved, thereby creating a campus-wide, proactive, and collaborative security management model. In the future,

universities should further strengthen the application and innovation of digital technologies, promoting the development of security management toward greater intelligence and refinement, and creating a safer and more harmonious campus environment for faculty and students.

References

[1] Qiao Yuanhui. "Research on AI-Empowered Campus Security Governance in the New Era." Journal of Tianjin Vocational Institutes Union, 2023, 25(12), 78-81+87.
[2] Liu Hesheng. "Promoting the Standardization and Scientification of Campus Security Education and Management." Safe Campus, 2023(9), 6-11.
[3] Wang Hongyu. "Research on Influencing Factors and Countermeasures of Campus Security Management in Universities." Zhengzhou: Zhengzhou University, 2013.
[4] Xu Jin, Qian Xiao. "Construction of University Campus Security Management System Based on Digital Infrastructure." Modern Information Technology, 2022, 6(15), 34-36.
[5] Ding Yushan, Chen Jintao, Wang Dingchen, et al. "Practical Research on the Construction of a University Security Big Data Platform: A Case Study of Beijing Normal University." University Logistics Research, 2024(3), 55-57.