Exploring the Practical Path of Cybersecurity Governance in Media Organizations: Postprint

Authors: Ling Yunyi

Date: 2025-07-09T00:00:00+00:00

Abstract

【Objective】 To investigate cybersecurity governance in news organizations, explore solutions for cybersecurity governance, and adapt to the needs of the cybersecurity governance environment in the all-media and intelligent media era.

【Method】 Utilizing Information System Security Level Protection assessment, cybersecurity technology and management to achieve secure operation under cybersecurity protection.

【Result】 Through cybersecurity governance, systematic improvement in security posture and security operations capability is achieved, ensuring secure system operation.

【Conclusion】 Cybersecurity, like operational security, is a fundamental guarantee. Through practical exploration of cybersecurity governance, this provides a reference for cybersecurity governance work in industry organizations.

Full Text

Exploring Practical Pathways for Cybersecurity Governance in Media Organizations

Hainan Nanhai Net Media Co., Ltd., Haikou, Hainan 570100

Abstract

This study examines cybersecurity governance in news organizations to explore viable solutions that meet the demands of the all-media and intelligent media era. Employing information system security classified protection evaluation alongside cybersecurity technologies and management practices, the research achieves secure operations under cybersecurity safeguards. Through systematic

governance, organizations can enhance their security posture and operational capabilities, ensuring safe production. The findings demonstrate that cybersecurity, like operational security, constitutes a fundamental safeguard. This practical exploration provides a reference for cybersecurity governance across the industry.

Keywords: cybersecurity; classified protection; information systems; media convergence; information security
Chinese Library Classification: G2223
Document Code: A
Article Number: 1671-0134(2025)03-35-05
DOI: 10.19483/j.cnki.11-4653/n.2025.03.006
Citation Format: Ling Yunyang. Exploring Practical Pathways for Cybersecurity Governance in Media Organizations [J]. China Media Technology, 2025, 32(3):

The cybersecurity posture of media organizations has evolved in tandem with their development needs. Organizations primarily using print media, with paper-based distribution and relatively slower dissemination efficiency, faced information security issues such as confidentiality, information accuracy, and production system failures. Their information systems were mainly deployed on internal networks for internal users, resulting in relatively small security perimeters. With appropriate VPN virtual channels and network isolation measures, their external attack surface remained comparatively limited, sharing similarities with OA systems, financial systems, and CRM platforms.

The implementation of China' s Cybersecurity Law, Data Security Law, and Personal Information Protection Law, along with related cyberspace governance regulations, has elevated cybersecurity to a national strategic priority, strengthening its connection to national security. The rapid development of the digital economy and next-generation information technologies has accelerated societal progress while intensifying cybersecurity challenges. Media organizations such as broadcast television, online media, and new media have enhanced their capabilities to serve end-users, expanding system exposure and increasing complexity. Simultaneously, the difficulty of isolating internal and external systems has risen, with cybersecurity incidents causing greater impact and faster propagation. As platforms become increasingly feature-rich, sensitivity to cybersecurity incidents has grown rapidly, reducing cybersecurity fault tolerance and escalating costs. Media organizations perform ideological work intrinsically linked to national security. The proliferation of new media platforms and emerging information technologies has exponentially increased both the number and scale of online platforms, while cybersecurity threats have grown at an equally rapid pace. Throughout this evolution, inadequate cybersecurity governance and shifting cyberspace environments—both internal and external—have presented unprecedented challenges.

1. Review of Cybersecurity Governance History

1.1 First Stage of Cybersecurity Governance Development

Media organizations' cybersecurity capabilities have developed synchronously with their operational needs. Different communication carriers and production modalities create distinct cybersecurity contexts, with varying impacts and losses from security incidents driving different security requirements. Traditional print-media organizations, for instance, primarily deployed information systems on internal networks for internal users, resulting in relatively small security perimeters. With appropriate VPN virtual channels and network isolation measures, their external attack surface remained comparatively limited, sharing similarities with OA systems, financial systems, and CRM platforms.

During this period, constrained by policy environments, domestic and international conditions, network contexts, organizational circumstances, and market factors, most media organizations underwent a cybersecurity governance evolution from non-existence to establishment—a systemic phenomenon. This trajectory directly and indirectly related to the nature of media organizations, their institutional mechanisms, and technological environments. As cybersecurity constitutes supportive work—like many operational maintenance tasks—it plays a critical role behind the scenes. Moreover, cybersecurity governance carries high costs without generating direct financial returns. These two factors initially prevented senior leadership from fully prioritizing cybersecurity, resulting in insufficient initiative, inadequate attention, limited investment, and talent shortages that caused considerable damage. Particularly problematic were information overload, frequent system vulnerabilities, and immature governance mechanisms and legal frameworks. Many organizations operated systems in an unprotected or minimally protected "running naked" state, offering virtually no defense against cyberattacks.

Consequently, cybersecurity incidents such as webpage defacement, server privilege escalation, reverse shell control, DNS tampering, malware injection, DDoS attacks, weak password exploitation, database exfiltration, hidden links, and SEO black-hat activities proliferated. A culture of resigned acceptance emerged within media organizations, with problem-solving approaches remaining crude and simplistic—such as system shutdowns, backend restrictions, and backup restoration. This phenomenon within media organizations arguably reflects the broader trajectory of China' s internet and cybersecurity development.

1.2 Second Stage of Cybersecurity Governance Development

As society and technology advanced, the media ecosystem transformed, and the legal framework matured, cybersecurity governance rapidly ascended to national strategic status. The legislative system' s improvement created top-down governance structures. For media organizations, heightened responsibilities—particularly for ideological security—combined with organizational reforms and evolving network environments significantly elevated cybersecurity awareness,

especially among principal leaders. This foundation enabled progress in cybersecurity governance, with organizations gradually developing awareness and concrete initiatives.

The maturation of cybersecurity legislation, digital economy growth, and information technology advancement rapidly elevated public cybersecurity consciousness. From organizational leadership to ordinary netizens, collective contributions fostered a social environment conducive to cybersecurity governance. Technological progress in cybersecurity and supporting fields—such as cloud computing and cloud security—along with systematic upgrades to industry supply chains, particularly state investment in cybersecurity and related information industries, reduced costs and enabled financially constrained media organizations to invest in cybersecurity.

Simultaneously, intensified regulatory oversight and evolving enforcement environments injected execution momentum into media organizations' cybersecurity governance, creating comprehensive, systematic safeguards that elevated high-quality development. After approximately a decade of development, media organizations achieved substantial progress during this second stage, gradually resolving many first-stage problems. Leadership and organizational cybersecurity concepts improved, with corresponding investments made where possible —a process of accumulated experience across leadership generations. However, cybersecurity work remains cyclical, continuously generating new problems during problem-solving. Long-term governance requires exploring sustainable pathways and methods, which constitutes this paper' s core focus.

Throughout these two developmental stages, many issues have been resolved while others persist. Confronted with rising cybersecurity awareness, system vulnerabilities, insufficient investment, incomplete institutions, management deficiencies, talent shortages, and R&D limitations, media organizations must continuously strive to enhance systematic governance capabilities, gradually achieving modernization of cybersecurity governance standards and capabilities for the new era.

2. Cybersecurity Governance Process

2.1 Cybersecurity Governance Expectations

As a costly endeavor, cybersecurity governance requires standardized definitions of objectives: what goals to achieve, how to achieve them, what specific tasks are necessary, and what investments are required. Media organizations generally face revenue pressures, making reasonable cybersecurity governance expectations crucial. Unrealistic expectations generate excessive costs, impede implementation, and waste investments, while overly low expectations fail to meet substantive needs, leaving production and external security at high risk.

From a systemic perspective, cybersecurity governance demands operational feasibility under standardized frameworks. Security requirements must be defined

within these frameworks, then operationalized through project-based implementation. Tasks should be executed in phases and batches according to organizational realities. These requirements guide subsequent work and should remain within reasonable bounds without exceeding actual needs. So how should standardized cybersecurity requirements or expectations be defined?

To address systemic governance requirements, China promulgated the Regulations on the Security Protection of Computer Information Systems in 1994—commonly known as Classified Protection 1.0—along with various other policies providing systematic standards. The revised Classified Protection 2.0 offers a comprehensive guide for cybersecurity governance, establishing clear benchmarks. By combining these regulatory requirements with organizational needs and cybersecurity risk assessments, organizations can essentially define their cybersecurity requirements (see framework diagram [Figure 1: see original paper]).

2.2 Cybersecurity Governance Measures

From a macro-strategic and traditional security perspective, most media organizations conduct cybersecurity governance within the Classified Protection framework. Many equate compliance with legal obligations—purchasing and configuring cybersecurity hardware or products, guided by assessment companies, and obtaining evaluation reports with passing scores—as fulfilling cybersecurity requirements. However, systems that merely achieve legal compliance through such reports remain highly vulnerable to cyber threats. Classified Protection scores represent only minimum requirements, far from adequate for actual risk profiles and security needs.

Furthermore, many media organizations build protection-centric governance systems, focusing disproportionately on external threats over internal networks. This incomplete or biased protection pattern creates significant vulnerabilities, evident in many recent cybersecurity incidents. Simultaneously, other cybersecurity systems—such as monitoring, talent, and institutional frameworks—receive insufficient attention due to complex factors not explored here.

Additionally, many media organizations adopt outsourcing models for cybersecurity governance, relying entirely on vendors through procurement of devices, products, and services. This trust-transfer approach fails to genuinely resolve cybersecurity issues. Many organizations also lack sufficient cybersecurity expertise, preventing them from effectively utilizing advanced security products. These products require compliant environments to maximize effectiveness, yet organizations' cybersecurity management and information system compliance levels often remain low.

This discussion does not negate the necessity of cybersecurity systems but rather advocates for scientific governance approaches. We must still conduct micro-level governance practices under national macro-level guidance.

3.1 Root Cause Cybersecurity Governance

As previously discussed, media organizations' development has often failed to implement the "three synchronizations" —synchronized design, construction, and operation—in system development and maintenance. Early systems were primarily purchased, with insufficient subsequent investment to update and patch vulnerabilities. Many systems can no longer receive technical support, making vulnerability remediation impossible. Therefore, building cybersecurity systems requires root cause governance from the "three synchronizations" principle throughout the full lifecycle, with long-term adherence during iterative development.

Internally, organizations must prioritize fundamental vulnerability remediation, upgrading legacy systems and enhancing security levels. Externally, they should focus on cybersecurity industry trends and threat intelligence acquisition. By dynamically advancing both aspects, organizations can achieve timely, dynamic security and fundamentally enable secure operations. However, management issues—which we will address separately—cannot be ignored. There is no cheapest or most expensive security, only the most appropriate security.

Root cause, systematic cybersecurity governance involves technical R&D capabilities, management capabilities, financial resources, and other dimensions. Organizations must make reasonable decisions based on their actual circumstances.

3.2 Specific Technical Practices in Cybersecurity Governance

Based on Classified Protection 2.0 standards, this paper does not intend to discuss the entire system but rather focuses on several specific aspects identified through practice.

3.2.1 Security Management Systems

The author' s organization established a cybersecurity management system in 2014 under Classified Protection 1.0, defining cybersecurity management personnel and supporting regulations. As cybersecurity has evolved, the system has continuously improved through annual assessments, security drills, inspections, and regulatory requirements, forming a relatively complete institutional framework. Media organizations must also comply with additional regulatory provisions from national and local cyberspace administrations, communications authorities, and public security departments, particularly regarding content review and content security compliance beyond technical specifications.

However, many media organizations face challenges with voluminous institutional frameworks where policies and execution diverge. Institutional operation and maintenance costs are high, yet from a compliance perspective, systems are essential as top-level design and guidance for cybersecurity work.

3.2.2 Security Technology Environment

Regarding technical security encompassing physical, communications, boundary, application, and environmental security, media organizations should employ dedicated cybersecurity professionals or staff with comprehensive cybersecurity knowledge and expertise. Cybersecurity cannot be built on abstract foundations but must manifest in practical details.

Cloud computing development has transformed cybersecurity approaches, with cloud providers assuming responsibility for physical, communications, boundary, and environmental security. However, organizations must still comprehensively master relevant knowledge and capabilities rather than simply outsourcing all security responsibilities, which abdicates accountability and introduces outsourcing risks.

Based on earlier discussions, media organizations building cybersecurity systems often focus on protection while neglecting monitoring and auditing systems, as well as management systems, inadvertently reducing governance effectiveness. Particularly at the application security level, auditing functions often lack high commercial value and frequently go undeveloped. Yet cybersecurity monitoring and auditing capabilities significantly impact governance levels. Without them, unknown aspects of cybersecurity expand, leaving security personnel without complete visibility into 24-hour system status. This information deficit undermines subsequent emergency response, situational assessment, and decision-making, reducing scientific validity.

Many organizations still exhibit obvious "shell" patterns and should, where possible, promote integrated cybersecurity systems guided by systems thinking and principles like the barrel theory to minimize gaps between application security and security devices, preventing systems from going live or operating with inherent flaws. Cybersecurity teams must conduct thorough evaluations of products and solutions during procurement to maximize investment returns.

3.3 Management Issues in Cybersecurity Governance

Management issues in cybersecurity governance—essentially security operations under the Classified Protection 2.0 framework—represent high-cost endeavors. Most media organizations lack capacity to build complete security operations systems, often 勉强 operating within compliance frameworks to maintain basic institutional and technical protection systems.

From earlier analysis, cybersecurity governance without security operations system support constitutes passive governance. The author' s organization faces this challenge, with cybersecurity work remaining ambiguous, particularly during non-working hours. Cybersecurity governance fundamentally requires proactive operations. Given that cybersecurity incident losses cannot be standardized, many matters require predictive, proactive responses rather than passive experimentation, which carries unacceptable costs and conditions in reality.

Management issues partly reflect senior leadership commitment and implementation of organizational development strategies. The principle that cybersecurity relies "30% on technology, 70% on management" remains unrealized in many media organizations. In practice, technical implementation effectiveness—including security policy management, system configuration, and baseline compliance—ultimately depends on management resolution. However, many media leaders lack technical backgrounds, while technically proficient leaders often fail to achieve consensus with other executives, causing many cybersecurity incidents to originate at the management level, such as information leakage, patch management, vulnerability remediation, and weak passwords resulting from failure to "actively" manage.

Therefore, building a proactively driven security operations management system is crucial for current cybersecurity governance in media organizations. Passive approaches are unsuitable for cybersecurity governance, where incident losses are immeasurable and many issues require proactive, predictive responses.

4. Research on Key Issues in Cybersecurity Governance

4.1 Continuous Learning of Policies, Regulations, and Cybersecurity Technologies

Cybersecurity governance is a long-term undertaking corresponding to the lifecycle of information systems and organizations. Media organizations and their technical teams must continuously update their knowledge systems, particularly regarding policies, regulations, cybersecurity trends, and emerging technologies. Externally, they must maintain compliance and situational awareness; internally, they must meet security assurance and operational requirements.

Organizations must achieve mastery rather than superficial understanding of policies and regulations. For instance, cybersecurity regulations and confidentiality regulations must be applied in tandem, as different regulations have distinct focuses that may conflict in practice. Solutions should address specific issues within the regulatory framework. Larger media organizations conducting diverse businesses face multiple security compliance scenarios.

Cybersecurity technology learning should follow applicability principles to address organizational governance needs rather than blindly pursuing new technologies. Additionally, organizations should deepen research into media-specific technologies, such as the "three reviews and three proofreads" mechanism unique to media organizations.

4.2 Cybersecurity Governance Under Dynamic Operations Support

During development, media organizations should establish their own cybersecurity operations systems. Long-term, dynamic cybersecurity governance—particularly supported by emerging technologies like artificial intelligence and big data—represents the necessary solution path.

Cybersecurity governance demands high technical capabilities, especially in R&D and technical management. Media organizations should invest resources in building core technical capabilities, independently developing systems where possible to establish "three synchronizations" mechanisms that proactively address cybersecurity issues. For procured systems, organizations should leverage their own technical capabilities alongside vendor cooperation to jointly advance cybersecurity solutions, particularly avoiding problem-ignoring behaviors.

Under dynamic operations systems, media organizations must not separate security from operations. Both are 保障性 endeavors for long-term system operation, closely connected and inseparable. System availability and reliability concern both operations teams and cybersecurity metrics, serving identical objectives. Simultaneously, cybersecurity work must be granted sufficient authority to ensure high-quality operations under security assurance.

Based on years of practical experience and reflection on specific issues in media organization cybersecurity work, combined with analysis of internal and external environments and regulatory policies, this paper examines key points rather than comprehensively covering the entire cybersecurity system. After years of exploration, the author' s organization has achieved progress: specific analysis and resolution of problems have reduced vulnerabilities, lowered cybersecurity incident rates, and steadily improved security assurance capabilities. Media organizations bear important ideological dissemination responsibilities, making ideological security paramount. Only with cybersecurity as the foundation can they achieve high-quality development under secure conditions.

References

[1] Wu Caiyu. "Research on the Implementation of the Legal System for Network Information Security Supervision"[J]. Journal of Political Science and Law, 2024(2): 29-37.
[2] Dai Zongkun, Tang Sanping. VPN and Network Security [M]. Beijing: Publishing House of Electronics Industry, 2002.
[3] Song Lingmei. Application of Virtual Network Technology in Computer Network Security [J]. China Media Technology, 2021(2): 105-107.
[4] Zhao Peng. Research on Network Security Issues in the Context of Media Convergence [J]. Science and Technology Communication, 2016(1): 198-200.
[5] Han Xiaoguang, Wang Ruosong, Tang Jincai. Research and Practice on IT Operations Management Systems in the New Era [J]. China Media Technology, 2024(6): 150-155.
[6] Wang Lin. Technical Risks and Response Strategies for Media Space Governance [J]. China Media Technology, 2022(10): 68-71.
[7] Zheng Lianqing. Introduction to Network Security [M]. Beijing: Tsinghua University Press, 2015.
[8] Sun Yuan. How to Ensure Information Security in the Context of Media Convergence Construction [J]. Western Radio and TV, 2018(23): 46-47.
[9] Shen Changxiang. "Cloud Computing Security and Classified Protection"

[J]. Information Security and Communications Privacy, 2012(1): 16-17.
[10] Wang Yunbo. Thoughts on Network Security in the Context of Media Convergence [J]. Media Forum, 2019(21): 94.
[11] Wang Shiwei. On Information Security, Network Security, and Cyberspace Security [M]. Beijing: Social Sciences Academic Press, 2015.
[12] Huang Jie. Discussion on New Technology Applications in Network Security and System Operations [J]. Communications World, 2024(3): 30-32.
[13] Wang Jiatong. Analysis of Network Security Technology for Information Systems [J]. Cyberspace Security, 2024(2): 45-48.
[14] Wu Honghui. Research on Data Center Network Security Hardening Construction Based on Media Convergence [J]. China Media Technology, 2021(3): 114-116.
[15] Zhu Lei. Research on the Application of Big Data Technology in Network Security Analysis [J]. Digital Users, 2023(29): 40-42.
[16] Wang Dapeng. "Exploration of Computer Network Security Management and Effective Operation" [J]. China New Technologies and Products, 2013(7): 12.

Author Biography

Ling Yunyang (1986–), male, from Tianshui, Gansu, Senior Engineer (Deputy Chief Engineer, in charge), Hainan Nanhai Net Media Co., Ltd. Research interests: media convergence, technology management, project management, software engineering, cybersecurity, etc.

(Executive Editor: Li Yansong)

Note: Figure translations are in progress. See original paper for figures.