Journal of Commercial Law Review
2025, VOL. 9, NO. 1, 139-142
DOI: 10.47297/wspjclrWSP2516-249730.20250901

Research on Corporate Compliance Governance and Cybersecurity Legal Responsibility in the Digital Economy Era

Rui Zhang

Beijing Kangda (Hai kou) Law Firm, Haikou, Hainan, 570208

ABSTRACT
The rapid development of the digital economy has brought unprecedented opportunities for enterprises, but also triggered many challenges in the fields of compliance governance and network security. Starting from the connotation and characteristics of the digital economy, this article deeply analyzes the necessity and core content of enterprises in compliance governance such as data protection, anti-monopoly, and anti money laundering, and explores in detail the complexity of legal responsibilities for network security and its multidimensional response strategies. By combining multiple practical cases, the article systematically proposes a theoretical and practical path for the integrated development of compliance governance and network security, and comprehensively puts forward future development suggestions from the perspectives of policy, enterprise, and technology, aiming to provide profound theoretical references and practical guidance for enterprises to build a scientific and efficient governance system.

KEYWORDS
digital economy era; Corporate compliance governance; Legal Liability for Cybersecurity

With the booming development of the digital economy, enterprise operations are gradually becoming digitized and networked. However, the widespread application of digital technology has also brought challenges in network security risks and legal responsibilities. Enterprises need to seek a balance between compliance governance and cybersecurity to ensure sustainable development and legitimate operations. The digital economy, while promoting industrial upgrading and optimizing resource allocation, also exacerbates risks such as information leakage and system vulnerabilities. In order to adapt to this new situation, enterprises must build a comprehensive and dynamic governance system based on compliance and guaranteed by network security. Starting from the background of the digital economy, this article delves into the current situation, challenges, and future paths of corporate compliance governance and legal responsibility for cybersecurity, aiming to provide constructive theoretical and practical support for policy makers and business managers.

1 Compliance Governance of Enterprises in the Context of Digital Economy

The digital economy is an economic form driven by digital technology as its core, characterized by informatization, interconnectivity, and intelligence. In this context, enterprises need to face more complex legal regulations and regulatory requirements. The necessity of corporate compliance governance is mainly reflected in the following aspects: Firstly, in the era of digital economy, countries have introduced relevant laws and regulations on data privacy protection, network security, etc. For example, the General Data Protection Regulation (GDPR) and the Cybersecurity Law impose higher compliance requirements on enterprises, which not only require them to comply with specific laws, but also require them to develop a comprehensive governance plan covering a wide range of business areas. Secondly, compliance governance has become an important means to enhance corporate reputation and market competitiveness, especially in the international market where compliance has become a "passport" to enter certain industries or regions. Finally, compliance governance can effectively identify and control potential legal and operational risks, laying a solid foundation for the long-term development of enterprises. The core content of enterprise compliance governance includes data protection compliance, ensuring the security and lawful use of personal data and sensitive information; Antitrust and fair competition, compliance with fair competition regulations, and avoidance of legal disputes arising from market behavior; And anti money laundering and financial transparency, establishing a sound financial compliance system to make financial data more transparent and comply with international standards.

2 Challenges and Responses to Legal Responsibilities in Cybersecurity

The legal responsibility for network security mainly includes the following aspects: data breach responsibility. If a company causes user data leakage due to poor management, it shall bear corresponding civil or administrative responsibilities; System security responsibility: When an enterprise's information system is attacked or has vulnerabilities that may have an impact on society, legal responsibility must be borne; Content management responsibility: Enterprises

need to review the content published on the platform to avoid spreading illegal or harmful information. These responsibilities also face highly complex issues, mainly reflected in the following aspects. Firstly, there are significant differences in the legal requirements for cybersecurity and data protection among different countries, and enterprises face the challenge of complying with multiple laws in cross-border operations. Secondly, the application of new technologies such as artificial intelligence and blockchain has brought many conveniences to enterprises, but it has also brought new challenges to legal supervision. Many current laws cannot fully cover the new problems brought by these technologies. In addition, enterprises also need to deal with increasingly complex network attacks and malicious behavior, such as using ransomware to steal critical data and demanding ransom. In order to effectively respond to legal responsibilities for network security, enterprises should improve their internal security systems, establish a sound network security management system, including specific measures such as data classification and grading, access control, etc; Regularly hire professional organizations to conduct comprehensive assessments of network security status and continuously update security strategies based on the latest threat trends; Enhance employees' awareness of network security, ensure legal and compliant operations, and thus build a defensive and adaptive security system; By utilizing technological means to enhance network security and aligning with laws and regulations, we ensure compliance with legal requirements while addressing new threats.

3 The integrated development of enterprise compliance governance and network security in the digital economy era

To effectively integrate compliance governance and cybersecurity, enterprises must address three core challenges: cross-border data flow compliance ,industry regulatory adaptability, and the application of intelligent technology.Cross-Border Data Flow Compliance.

With globalization and the digital economy, enterprises increasingly rely on cross-border data flows. However, varying data protection laws, such as the GDPR in Europe and CCPA in the United States, complicate compliance. Organizations must establish robust frameworks that balance regulatory adherence with operational efficiency. This includes leveraging tools like data anonymization, encryption, and consent management platforms to safeguard privacy and mitigate risks.

Industry Regulatory Adaptability

Industries face distinct regulatory requirements depending on their operational nature. For example, financial institutions must comply with stringent anti-money laundering (AML) regulations, while healthcare organizations prioritize patient data protection under frameworks like HIPAA. Achieving regulatory adaptability requires adopting tailored cybersecurity measures and compliance strategies that align with industry-specific mandates, thus fostering trust and operational resilience.

Application of Intelligent Technology

Artificial intelligence (AI) and machine learning (ML) have become indispensable in managing complex compliance and cybersecurity ecosystems. AI-powered tools enable real-time monitoring, threat detection, and compliance audits. For instance, natural language processing can help organizations quickly interpret regulatory changes and assess their implications. Meanwhile, ML models enhance threat prediction and automate responses, reducing vulnerabilities.

Strategic Integration for Future Resilience

To maximize the synergy between compliance governance and cybersecurity, enterprises should pursue integrated frameworks that combine policy development, technology adoption, and workforce training. Collaboration with regulators and stakeholders ensures that enterprises stay ahead of evolving challenges, while fostering innovation and maintaining competitive advantages in the digital economy. In the long run, this integrated approach not only mitigates risks but also contributes to sustainable growth in an increasingly interconnected world.

The Importance and Implementation Path of Compliance in Cross border Data Flow

With the continuous acceleration of globalization and the digital economy, cross-border data flow has become a core component of international trade and multinational enterprise operations. However, this also brings complex legal and security challenges. There are significant differences in the legal requirements for cross-border data flow among different countries and regions. For example, the European Union's General Data Protection Regulation (GDPR) sets strict conditions for cross-border data transmission, while the United States places more emphasis on protecting the commercial value of data. This legal divergence poses multiple regulatory risks for companies when it comes to data flow.

In order to ensure the security and legality of cross-border data transmission, enterprises need to strictly control and review every aspect of data usage, storage, and transmission. Firstly, a clear data classification and grading system should be established, with different access permissions and transmission conditions set according to the sensitivity of the data. Secondly, enterprises need to encrypt cross-border data transmission and ensure that it complies with the privacy protection standards of the destination country. For example, by adopting internationally recognized data protection

protocols such as EU Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), legal risks in cross-border data transmission can be effectively reduced. In addition, companies need to establish a dedicated cross-border data compliance team to regularly review and update their data protection strategies in response to increasingly complex legal changes worldwide.

The key role of industry regulatory adaptability

In high-risk industries such as finance and healthcare, data often involves sensitive areas such as customer privacy, financial information, and life and health. Therefore, these industries have put forward higher requirements for compliance governance and network security. For example, in the financial industry, companies need to comply with regulatory requirements such as anti money laundering (AML) and customer identification (KYC), while also ensuring the security and stability of financial transaction systems; In the healthcare industry, companies are required to comply with privacy protection laws such as the Health Insurance Portability and Accountability Act (HIPAA) to ensure that patients' medical information is not leaked during storage and transmission.

In order to meet the regulatory requirements of high-risk industries, enterprises need to invest more resources in compliance governance and network security. Firstly, it is necessary to establish an internal governance system that is highly compatible with industry regulatory requirements, including setting up dedicated compliance officers, conducting regular internal audits, organizing employee training, and other measures. Secondly, enterprises should strengthen communication and cooperation with regulatory agencies, timely understand and respond to the latest changes in regulatory policies. Taking the medical industry as an example, an international medical data company has successfully developed a medical data management system that meets HIPAA requirements through cooperation with regulatory agencies. This not only ensures data compliance, but also significantly improves system security and operational efficiency.

The Application of Intelligent Technology in Compliance Governance and Network Security

The application of intelligent technology provides strong support for the integrated development of compliance governance and network security. The introduction of cutting-edge technologies such as artificial intelligence (AI) and blockchain not only significantly improves the efficiency of enterprise compliance and security management, but also provides more possibilities for risk prevention and control. For example, blockchain technology provides new ideas for data protection and privacy compliance with its decentralized, tamper proof, and traceable features. By recording the usage and access of data on the blockchain, enterprises can achieve full process visualization management of data flow, effectively reducing compliance risks.

Artificial intelligence has played an important role in automated risk identification and response. AI technology can monitor the network environment of enterprises in real time, identify potential threats, and issue warnings before risks occur. For example, an international technology company has significantly improved its network security protection capabilities by introducing an AI driven threat monitoring system. In specific operations, the system can quickly analyze massive network log data, identify abnormal behavior, and automatically take corresponding protective measures. This not only reduces the risk of human error, but also greatly enhances the ability of enterprises to respond to complex network threats.

Practical case: Integration effect of compliance governance and network security

The integration effect of compliance governance and network security has been verified in multiple fields. Taking an international technology company as an example, the company successfully responded to the regulatory requirements of GDPR by implementing data classification protection and privacy policy compliance. At the same time, it introduced real-time network threat monitoring technology, significantly improving the overall level of network security. In this process, the enterprise not only established a comprehensive compliance governance framework, but also integrated technological means into daily operations, achieving a deep integration of compliance and security.

In the financial industry, a well-known financial institution has established a comprehensive security management system through cooperation with a cybersecurity company. This system not only includes traditional firewalls and encryption technologies, but also combines blockchain and AI technologies to ensure the integrity and security of transaction data. In addition, the institution regularly conducts compliance risk assessments and adjusts its governance strategies in a timely manner, significantly reducing the risk of data breaches and improving regulatory compliance efficiency.

Future prospects: Multi party collaboration to promote integrated development

In the future, the integration of compliance governance and network security will continue to move towards multi-party collaboration. At the policy level, the country should further improve its legal and regulatory system and promote international cooperation in data protection and cybersecurity; At the enterprise level, organizations should build a compliance culture internally and enhance their cybersecurity capabilities through technological innovation; At the technical level, we should continue to explore the potential of new technologies such as artificial intelligence and blockchain to provide more efficient solutions for enterprises.

In summary, the synergistic effect of compliance governance and network security is the core driving force for enterprise management in the digital economy era. Through the joint efforts of policies, technology, and corporate practices, enterprises can not only effectively respond to current compliance and security challenges, but also open up broader space for their own development.

4 Future Development Path and Suggestions

At the policy level, it is necessary to improve the legal and regulatory system and strengthen the legal norms for network security and compliance governance in the digital economy. For example, establishing a unified global legal framework for the digital economy to reduce cross-border operational difficulties caused by legal differences; Promote international cooperation, coordinate data flow and cybersecurity governance through multilateral mechanisms, and develop globally applicable standards. At the enterprise level, compliance awareness should be established internally, and a compliance management mechanism involving all employees should be formed; Enhance network security protection capabilities through independent research and development or technology introduction; Strengthen the compliance governance capabilities of the supply chain and partners, and enhance the overall security of the entire ecosystem; Collaborate with government, technology service providers, and industry partners to build a secure ecosystem. At the technical level, data encryption and privacy protection should be strengthened to enhance the security of data during transmission and storage. For example, zero knowledge proofs and other technologies should be used to ensure that data remains usable even in an encrypted state; Adopting an automated compliance review and risk warning system to improve management efficiency while reducing the risks caused by human operational errors.

5 Conclusion

The compliance governance of enterprises in the digital economy era is intricately linked to the legal responsibilities associated with network security. With the rapid advancement of digital technology, enterprises face unprecedented opportunities for growth, but also significant challenges in addressing cybersecurity threats and meeting stringent compliance requirements. To navigate this complex landscape, enterprises must establish a robust, scientific, and efficient governance system that operates within the dual framework of legal regulations and technological safeguards. Such a system is essential for mitigating risks, safeguarding sensitive information, and ensuring sustainable growth in an increasingly interconnected digital environment.

Strengthening policy coordination is a critical step in achieving this goal. Governments must work to harmonize regulatory frameworks across jurisdictions to reduce conflicts and uncertainties for businesses operating on a global scale. At the same time, enterprises should actively engage in shaping and adhering to these policies, demonstrating their commitment to ethical practices and legal compliance. The integration of innovative technologies, such as artificial intelligence and blockchain, further enhances the capacity of enterprises to monitor, detect, and respond to cybersecurity threats in real-time, while also ensuring compliance with complex regulations like the General Data Protection Regulation (GDPR).

International cooperation is another cornerstone of effective governance in the digital economy. Collaborative efforts between nations, industries, and institutions can foster the development of standardized practices and mutual understanding, creating a safer and more predictable environment for digital business operations. In this collaborative ecosystem, enterprises not only enhance their competitiveness but also contribute to broader societal benefits by setting benchmarks for ethical conduct and technological resilience.

References

[1] Sherman A T , Delatte D , Neary M ,et al.Cybersecurity: Exploring core concepts through six scenarios[J].Cryptologia, 2017, 42(4):1-42.DOI:10.1080/01611194.2017.1362063.

[2] Ulrich P S , Stockert F .IT Governance and IT Compliance in Family Firms – the Special Case of Cyber Security[J].Procedia Computer Science, 2023, 225:2781-2789.DOI:10.1016/j.procs.2023.10.270.

[3] Teodoro N ,Luís Gonçalves,Carlos Serrão.NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements[C]//2015 IEEE Trustcom/BigDataSE/ISPA.IEEE, 2015.DOI:10.1109/Trustcom-BigDataSe-ISPA.2015.402.

[4] Davis T A .The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite[J].Columbia Business Law Review, 2015, 2015.DOI:10.7916/cblr.v2015i2.1756.

[5] Henderson D B .IT security controls: a guide to corporate standards and frameworks[J].Computing reviews, 2023.