Research on Data Security Governance of Industrial Information Service Platform

——Based on Information Ecology Theory

Cao Yue*[1], Bai Chen[1], ZhangYue[1] and Zhang Xuanxuan[1]

[1] Institute of Scientific and Technical Information of China, Fuxing Rd. 15, 100038 Beijing, China
caoyue@istic.ac.com

Abstract. Industrial information service platform gathers all kinds of data resources that are closely related to industrial development activities, and it is essential to guarantee the security of the whole life cycle of data for platform construction and operation services. In the face of the platform's large data volume, scattered storage, complex stakeholder relationships and environment, etc., the information ecology theory is introduced to construct the data ecosystem framework of the industrial information service platform based on three elements: data subject, data ontology and data environment, and to analyze the representative data security problems brought about by the interaction of each element with the element. Finally, the data security governance framework of industrial information service platform is constructed with the objectives of strengthening data security, exploring data value and guaranteeing data service, and the theoretical basis is proposed for enhancing the data security guarantee capability of the platform.

Keywords: Industrial Information Service Platform, Information Ecology, Data Ecology, Data Security, Data Security Governance

1 Introduction

At present, global data security incidents are frequent, and data security risks such as data leakage and data abuse are increasing day by day, posing a serious threat to national security, social stability, the rights and interests of organizations and the security of individual privacy. For example, the DDT company in the operation process to master a large number of national user information and other sensitive data, road information and other important data, and even the relationship between national security, national economic lifelines, important livelihood, major public interests and other national core data, so its illegal and illegal to go public in the United States by the behavior of the heavy punishment [1]. It can be seen that under the perspective of the overall national security concept, data security, as an important part of national security, has risen to the level of national strategy. In recent years, along with the introduction of laws, regulations and ordinances such as the Network Security Law, the Data Security

C. Bai et al. (eds.), *Proceedings of 2023 China Science and Technology Information Resource Management and Service Annual Conference (COINFO 2023)*, Advances in Economics, Business and Management Research 293,
https://doi.org/10.2991/978-94-6463-498-3_14

Law, the Personal Information Protection Law, the Measures for Network Security Review and the Regulations on the Security Protection of Critical Information Infrastructures, and the emergence of a series of socially hotly debated data security incidents such as the DDT company and China Knowledge, the data security of organizations in China with a large amount of user data, scientific and technological data, and key industry data, etc. is receiving focused attention.

Industrial information service platform mainly refers to the carrier that provides services for industries, governments, enterprises, universities and research institutes based on the strategic requirements of the state and government for the development of key industries and the development plans of science and technology in each region, etc., by gathering data resources such as papers, patents, institutions, talents and projects in key industrial fields into a single entity, and by adopting appropriate mechanisms and service modes[2]. Usually, the industrial information service platform aggregates data resources related to industrial development activities, and the relationship between individuals, organizations and other stakeholders and the environment in which they are formed is very complex. If the protection of data resources is not done properly, security incidents such as external network attacks and internal data leakage may not only affect the normal operation and services of the platform, causing negative impacts such as reputation crisis, customer loss and economic loss, but also compliance and legal risks. For example, the platform authority or construction department is penalized by the regulator due to violation; even the stable industrial environment may be affected due to data leakage, tampering or loss, so that the national and industrial security is adversely affected. In order to guarantee the normal and efficient operation and service of industrial information service platform, it is crucial to guarantee data security.

In the construction and operation of industrial information service platform, facing the characteristics of large quantity of information, many information subjects and complex information environment, it is very necessary to review and analyze the relationship between data protection, right confirmation and benefit distribution from the overall perspective, and to carry out sustained and effective data security governance to guarantee the security of data in its whole life cycle. Data security governance aims to ensure the security of data throughout its life cycle through a combination of organizational structure, technical system, management system and operational system. Under the perspective of information ecosystem theory, data security governance can be understood as safeguarding the safe use of data resources by informants, as well as the security of user information itself, by strengthening information technology and information environment [3]. This paper chooses the information ecosystem theory as the basic framework, and combines the experience of the previous project to propose the data security governance strategy of industrial information service platform.

2 Related Work

2.1 Industrial Information Service Platform

Ono, a Japanese scholar, put forward the concept of information platform in 2001, arguing that information platforms are responsible for creating, collecting, storing, exchanging, sharing and using information to support social life and research activities [4]. The industrial information service platform relies on the information platform to provide industry-related information services for the government, enterprises and other subjects. Foreign research and practice on information service was carried out earlier, and the corresponding information service system is also more perfect, such as Europe, America and Japan to promote the establishment of specialized government or private information service centers and carry out related business [5].

In recent years, in order to promote the circulation of industrial data elements, China has set up a number of industry-oriented service platforms relying on the government, enterprises, universities, libraries, scientific research institutions and other subjects [6]. Distinguished from traditional platforms such as logistics platforms and procurement platforms, industrial information service platforms integrate industry, data and the Internet in depth, acquire raw data through collection or purchase, and then form a variety of value-added data products and services through a series of processes such as aggregation, processing and processing, analysis and mining, and provide industrial services for the government and enterprise users, such as standard data resources, visual data products, data analysis reports and personalized consulting services, providing industrial services for the industrial industry chain, such as data resources, data analysis reports and personalized consulting services. The report and personalized consulting services empower decision-making upstream and downstream of the industry chain and promote industrial innovation.

At the level of theoretical research, a series of discussions have been carried out at home and abroad around the construction of information service platform, information service mode and mechanism, and information service evaluation, etc. The main research directions are summarized in Table 1. It also includes the technology of information service platform construction (such as Web technology, ASP technology IPv6 network technology) and construction mode.

Table 1. Study on the Representativeness of Industrial Information Service Platforms

Field of research	Representative authors	Main research content
Construction of Industry Information Service Platform	Hu, et al. [7]	Analyze the functional structure and operation mechanism of Europe INNOVA industry information service platform, and study the construction principles, requirements and models of industry innovation-oriented information service platform.
	Xiao [8]	Put forward the construction idea of knowledge network platform for strategic emerging industries in Hubei Province, and

		put forward the construction strategy from the aspects of information technology, talents, management and financial strategy.
	Zhao, et al. [9]	Build the construction plan of information service platform for biomedical industry cluster, including expert think tank, thematic database, high-end information service platform and biomedical achievement transformation platform.
Industrial Information Service Models and Mechanisms	Xiong, et al.[1]	Proposed that the information service platform for strategic emerging industries under the big data environment should integrate the public information platform, information trading platform and information forum, etc., and put forward three information service models of platform commonality, personalization and specialization.
	James, et al.[10]	Carry out research on information integration and service reorganization for technological innovation, and put forward the information guarantee framework for enterprise innovation service.
	Sun[11]	Based on the information ecology theory, analyze the interactions and structural relationships among multiple ecological factors in the information service ecosystem of strategic emerging industries, and construct a comprehensive ecological model framework and its operation strategy oriented to the enhancement of the effectiveness of information services.
	Gao, et al. [12]	Constructed a hierarchical service model of information resources for strategic emerging industries from the three levels of industry commonality, enterprise individuality and product characteristics.
Evaluation of Industrial Information Service	Mao, et al. [13]	Take Jiangsu Province as a case study to analyze the usage rate and satisfaction of the new agricultural information service platform, agricultural information content and its sources, and put forward development countermeasures.
	Miao, et al. [14]	Elaborate the multivariate causal path relationship of users' continuous use willingness of financial information service platform,

	which helps the platform to subsequently provide targeted strategies more in line with users' needs.

2.2 Data Security Governance

Traditional data security management can no longer adapt to the new security needs under the wave of digitization, and how to protect the security of core data resources through the development of complete strategies and processes has become an important issue for many enterprises and organizations, and data security governance has emerged. Data Security Governance (DSG) is a set of security system construction methodology for data security issues, which was first proposed by analyst Marc at the Gartner 2017 Security and Risk Management Summit, covering the complete chain from the decision-making layer to the technical layer, from the management system to the tool support, and from the top down through the entire organizational structure[15].

Data security governance aims to provide comprehensive and systematic data security solutions for enterprises and organizations so that they can be more secure and reliable in the process of data use. Scholars at home and abroad have conducted extensive research in this field and made a series of progress. As the foundation of data security governance, foreign data security laws and policies are relatively perfect, and countries or regions such as the United States and the European Union have successively released a number of laws and strategic plans on data protection. For example, the General Data Protection Regulation (GDPR) issued by the EU in 2018 is a set of rigorous and detailed personal data protection framework developed by the EU legislature for the world, which regulates the authorization of personal data, strengthens the ability of data subjects to control their own data, and has now become the core framework of the EU data protection law. In addition, Japan, South Korea and other countries have also issued relevant policies for strengthening the control of data security. Some foreign scholars have analyzed the role and impact of data security laws and regulations and the comparison of data security models in different countries[16].

Domestic scholars mainly carry out research from different perspectives, such as policies and regulations, system frameworks, and technical tools for data security governance. Chen Xiaoyu [17] formed a systematic research framework for the data security risks that may exist in e-commerce platforms, and put forward governance recommendations for e-commerce platforms' data security risks from the relevant legal, technical and risk control levels. Dong Muxin et al. [18] studied the data security governance framework of digital transformation of state-owned enterprises from the perspective of information ecology, and established an enterprise information ecosystem model based on four elements: data resources, data subjects, data environment and data technology, constructed a data security governance framework and put forward the path of deepening the state-owned enterprises' data security governance from the national level, the social level, and the enterprise level. Most of the existing domestic and international research focuses on the system framework or technical solutions, and there is still a lack of research on systematic thinking about the data security of information platforms from the perspective of information ecosystem.

2.3 Information Ecology Theory

Information ecology refers to the flow of information and information mapping in the organization under the ecological perspective, which is used to express the correlation between the information ecology view and the complex and changing information environment, the survival and activity state of the information people in the information environment, and the unified whole of the information formed in the process of circulating and exchanging information in the cyberspace[19]. Information ecology theory originated from the interdisciplinary research of information science, system science and ecology in the 1970s, and Horton[20] proposed the concept of "information ecology" for the first time in 1978, and suggested that we can refer to the relevant theories of ecology, regard information as a kind of resource, and analyze the complex information environment and relationship.

After decades of accumulation and development, the research of foreign scholars on information ecology has been relatively complete, covering the conceptual connotation of information ecology, theoretical system, practical application and information ethics, etc., especially in the field of libraries, e-commerce and social networks and other areas of practical application of the formation of a large number of research results, such as Garcia-Marco based on the theory of information ecology, research on the environmental changes in the field of libraries, found the need to pay attention to the universality of information management. It is found that it is necessary to pay attention to the process of information management universality, digital convergence, technology standardization and leveraging [21]. Domestic research on information ecology started late, but developed rapidly, further deepening the formation of information ecological niche, information ecological chain and other concepts, which enriched the connotation of information ecology theory. For example, Zhang Jiankun [6] applied the information ecology theory to the information service platform, analyzed the information ecological characteristics of the information service platform, put forward the measurement and model of the information ecological niche of the information service platform, and analyzed the state of the information ecological niche of the different information people and its potential impact on the information service platform, and constructed an overlapping model of the information ecological niche for the information service platform to propose corresponding optimization strategies for perfecting the information service platform.

With the continuous enrichment of research by scholars at home and abroad, the discussion on the composition of information ecosystem elements has been gradually deepened. At present, the mainstream academic views on the elements of information ecosystem mainly include two elements (informant-information environment), three elements (informant-information ontology-information environment) and four elements (informant-information ontology-information environment). -information technology - information environment) [3]. Although the academic community has not yet reached a unified perception of the elements of the information ecosystem, they have affirmed the wholeness of the information ecosystem and the organic connection between the elements, and emphasized the fundamental position of information and information environment in the whole information ecosystem. In the information services provided by the information platform, the service provider, the served and the service environment constitute a complete and interconnected information ecosystem. Information service is essentially to realize the reasonable deployment of information resources through information technology, and the information ecology theory also advocates the promotion of the reasonable use of information through the regulation of the interaction between information people and the information environment, and many researches regard the information service platform as an information ecosystem, and carry out the research on information service based on the information ecology theory.

To sum up, the information ecology theory emphasizes the mutual influence and synergistic development of the elements in the information environment, which plays a crucial role in understanding and managing data security in industrial information service platforms. From the perspective of information ecology, industrial information service platform is not only the distribution center of industrial data resources, but also the ecological environment of multiple information interaction. By constructing an information ecosystem, the data flow and security risks of industrial information service platforms can be understood more comprehensively, so that more targeted security strategies can be proposed. Therefore, based on the information ecology perspective, this paper constructs the information ecosystem of industrial information service platform, and explores the data security problems from the perspective of information ecological elements, and formulates targeted data security governance strategies, so as to find out an effective way to solve the data security problems.

3 Data Ecosystem of Industrial Information Service Platform

3.1 Constituent Element

The information ecosystem is a dynamic system in which internal elements are interconnected and interact with each other. In order to comprehensively consider the data flow and interaction in the industrial information service platform, we take the "three elements" information ecosystem as the theoretical basis, and construct the data ecosystem of the industrial information service platform by focusing on the three basic elements of the information subject (data subject), the information ontology (data ontology), and the information environment (data environment) as shown in **错误!未找到引用源。**.

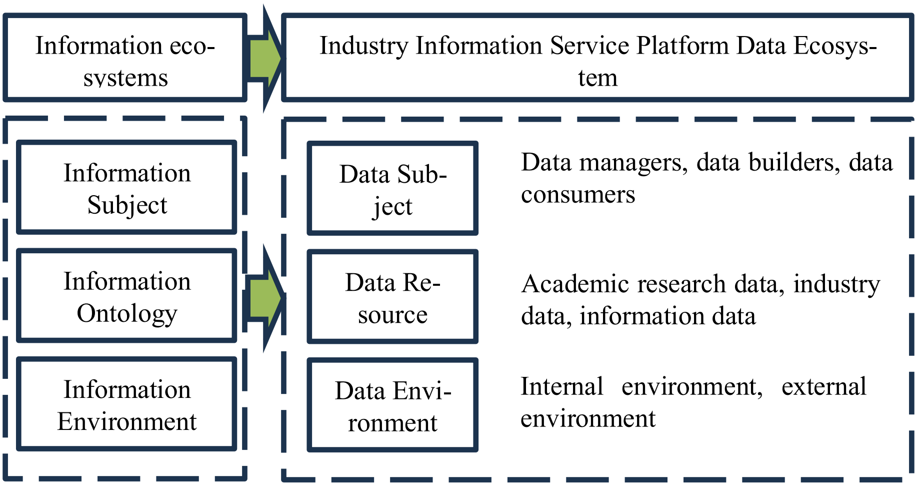
Information eco-systems
Industry Information Service Platform Data Ecosystem
Information Subject
Information Ontology
Information Environment
Data Subject
Data Resource
Data Environment
Data managers, data builders, data consumers
Academic research data, industry data, information data
Internal environment, external environment

Fig. 1. Industry Information Service Platform Data Ecosystem Constituent Element

Data Subject.

The information subject in the information ecosystem refers to all the information closely related and involved in information activities of a single person or a social organization composed of multiple individuals, including the information subject and the object with which the information is transmitted and exchanged, and as the dominant party decides the direction of the whole system. In the data ecosystem of industrial information service platform, the data subject includes all relevant parties of data resources in the process of construction and operation services, which can be specifically divided into data managers, data builders and data consumers.

(1) Data manager. Data manager is the role of managing, maintaining, supervising and securing the whole life cycle of data resources, covering the overall responsible team of the platform as well as the team and individuals dedicated to data management. Data managers play a core role in the data ecosystem of the industrial information service platform and are responsible for formulating data management strategies, planning data resources, and supervising and managing the entire data ecosystem.

(2) Data builder. Data builders are internal and external roles involved in the construction and maintenance of platform data resources, including data suppliers, system developers, technicians, etc. externally, and platform data collection personnel, data processing personnel, system operation and maintenance personnel, data service personnel, etc. internally. In the data ecosystem of the industrial information service platform, the data builders comply with the systems and regulations formulated by the data managers, continuously update and optimize the data resources, and ensure the security and integrity of the data in the construction process.

(3) Data consumers. In the industrial information service platform, data consumers interact with data through the use of data resources, data products and data services, and further feedback and optimization. Data consumers can include government,

enterprises, think tanks, universities, research institutions users or individuals, as well as industrial analysts within the platform. Data consumers' demand and feedback on data help drive the development and optimization of the entire data ecosystem.

Data Ontology.

In information ecology theory, information ontology is a collection of useful information that has been selected, organized and ordered, which is the key to the orderly operation of information ecosystem and the link between informants and the information environment. In the data ecosystem of industrial information service platform, data ontology, i.e. data resources, is the foundation and core of industrial information service.

From the perspective of data source, data resources can be categorized into self-collected data, commercial procurement data and exchange data. From the perspective of data resources, they can be divided into academic research data, including domestic and foreign journal/conference papers, patents, technical reports, project data, etc.; industrial data, including macro industrial statistical information, institutional information, talent information, policy and regulation information, etc., which is an important basis for the current status of the industrial development environment and the judgment of the future trend; and information and dynamic data, including technological breakthroughs, news and information, survey interviews, Information dynamic data, including technological breakthroughs, news information, survey interviews, media public opinion, enterprise annual reports/prospectuses, investment, financing and M&A information, etc.

In the whole ecosystem, there are a large number of data resources, from different sources, in various forms and with a wide range of contents. Data managers and data builders gather, process, manage and serve these data resources to ensure that the raw data are transformed into valuable information and knowledge to be provided to data consumers.

Data Environment.

The information environment is the background and place where the information ecology exists, taking the information medium as the structural framework and the information model as the organizational core, and is related to various factors of information activities. Based on the concept of information environment in the information ecology theory, data environment refers to all the factors that have an impact on the data subject and data ontology of the industrial information service platform, which can be divided into internal environment and external environment. Among them, the internal environment includes information infrastructure, information technology, management system, organizational construction, etc., which is relatively controllable and its stability can be strengthened through human intervention; the external environment refers to the social environment in which the platform is located, including the political environment, economic environment, cultural environment, legal environment and technical environment, etc., which is the legitimacy safeguard and constraints for the flow and application of data, and is able to penetrate into the full life cycle of data chain management, which has an indirect impact on the data security of the platform.

In the data ecosystem of industrial information service platform, the data environment can provide basic support for data subjects to safely and reliably obtain and use data services, and conversely, data subjects influence and improve the data environment through various ways. For example, data managers and data builders can optimize the internal environment by enhancing information technology, improving management system and other measures. At the same time, the data environment provides the necessary support and guarantee for the collection, storage, transmission, processing and utilization of data resources.

3.2 System framework

In the data ecosystem of the complete industrial information service platform, the elements are interconnected and interact with each other. Under the role of data environment, different data subjects such as data managers, data builders and data consumers are closely connected through the flow relationship of data ontology. On the basis of in-depth analysis of the specific connotation and characteristic attributes of different elements, this paper explores the relationship, influence and role of each element in the entire industrial information service platform data ecosystem, so as to construct the industrial information service platform data ecosystem based on the information ecology theory, whose framework is shown in **错误!未找到引用源。**.

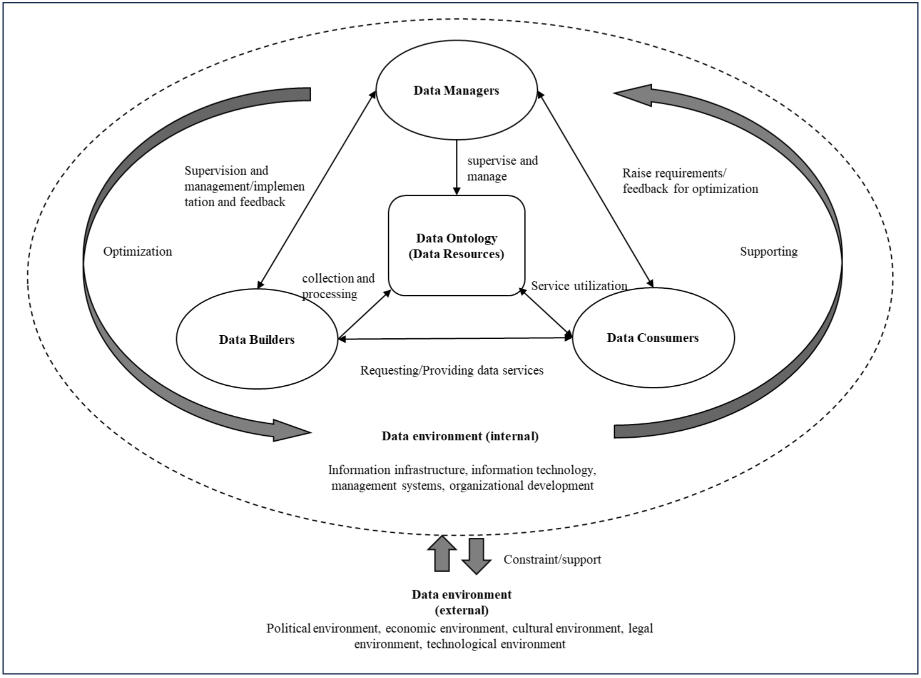
Data Managers
Supervision and management/implementation and feedback
supervise and manage
Raise requirements/ feedback for optimization
Optimization
Data Ontology (Data Resources)
Supporting
collection and processing
Service utilization
Data Builders
Data Consumers
Requesting/Providing data services
Data environment (internal)
Information infrastructure, information technology, management systems, organizational development
Constraint/support
Data environment (external)
Political environment, economic environment, cultural environment, legal environment, technological environment

Fig. 2. Industrial Information Service Platform Data Ecosystem Framework

The industrial information service platform data ecosystem is essentially an information ecosystem containing three elements, and the elements within the system interact with each other and realize dynamic stability in order to maintain the healthy and sustainable operation of the platform information service. In each of the basic elements constituting the data ecosystem of the industrial information service platform, whether it is the data subject, the data environment or the data resources, data security is what needs to be focused on. Targeted analysis of the security problems faced by each basic element is conducive to the development of corresponding data security strategies for industrial information service platforms to ensure data integrity and availability, and prevent data leakage and data abuse.

4 Data Security Problems of Industrial Information Service Platforms

4.1 Representative Data Security Problems of System Elements

Data Subject Perspective.
The construction and operation of the industrial information service platform lasts a long time and involves many people, and the data manager is mainly responsible for formulating relevant systems, decision-making and supervision. If the data manager pays insufficient attention to data security, it may cause a series of top-level design problems such as incomplete organizational structure, weak management system, inadequate protection technology, incomplete sorting of risk points, and a lack of contingency plans, which makes it difficult to cope with data security risks such as external attacks and internal data leakage, and so on. This makes it difficult to cope with data security risks such as external attacks and internal data leakage.

In the process of platform construction and operation, data builders are responsible for specific data provision or collection, processing and services, etc. Any intentional or unintentional irregularities may lead to data security risks within the platform. Therefore, whether data builders have sufficient data security awareness and whether they can strictly implement the data security strategies formulated by data managers is crucial to safeguarding the security and integrity of the full life cycle of data.

The data security problems faced by data consumers mainly lie in the interaction with the data ontology, after commissioning and acquiring platform data, data products or services, such as improper use may cause the leakage of the entire platform data, industrial information analysis results, for example, some analysis results in industrial analysis reports and briefing products may be more sensitive. At the same time, data consumers may also cause leakage of personal privacy information due to insufficient awareness of their own data security.

Data Ontology Perspective.
From the perspective of data ontology, the data security issues faced by the data ecosystem of industrial information service platforms involve multiple links in the life cycle of data collection, data transmission, data storage, data utilization, data exchange and data destruction.

From the viewpoint of data types, academic research data and industrial data may contain important enterprise, talent, project and technology information, and their characteristics and attributes also make the risk of data security leakage higher; information and dynamic data are more numerous and faster updated, so if the sources are not carefully screened and false data are injected into the data, it may bring about the security problem of data forgery, and the lack of authenticity and accuracy may cause deviations in the industrial analysis and decision-making judgment of the consumers of the subsequent data. The lack of authenticity and accuracy will cause bias in the analysis and decision-making judgment of the subsequent data consumers. From the perspective of the full data lifecycle, data collection is the initial and one of the most important aspects of the entire lifecycle. Data security risks may be triggered by non-compliance of data collection and imperfect commercial procurement system. For example, because data pricing mechanisms and data ownership have not yet formed a standard, and the data transaction system is not perfect, it is easy to have procurement risks. In particular, the current lack of effective evaluation standards for data suppliers makes it easy for the procured data to be ineffective and unable to satisfy industrial information services due to the supplier's own risks, data quality deviations or updating mechanisms.

Data Environment Perspective.

In the data ecosystem of the industrial information service platform, the security of the data environment covers multiple dimensions of the internal and external environments, thus directly or indirectly affecting the entire ecosystem. In the internal environment, the possible existence of information infrastructure such as low versions of data hardware and software, weak firewalls, and technical protection problems make it difficult to protect against external threats; in addition, the lack of management systems, standard systems, and organizational construction for industrial information service platforms may result in internal security risks, such as abuse by insiders, illegal access to enterprise, talent, and project data, and illegal profits.

In the external environment, the political and economic environments may indirectly affect data security, for example, unstable social and economic environments may lead to an increase in external attacks, internal leakage and other data security incidents; the cultural environment may affect the data subject's understanding and cognition of the value of the data, thus affecting the awareness of data security; the legal environment provides regulatory constraints on data security, and the strength of penalties in laws and regulations, and the soundness or otherwise of policies and regulations will all affect the security of data. The legal environment provides regulatory constraints for data security, and the strength of penalties in laws and regulations, and the soundness or otherwise of policies and regulations will affect the frequency of data security incidents; the technical environment is another key factor, and the new technologies such as artificial intelligence, big data, knowledge graph, user profiling, intelligent recommendation and data visualization used for industrial information services may bring new security threats, which also put forward higher requirements for the old security measures.

4.2 Representative Data Security Problems of Factor Interaction

The data ecosystem of the industrial information service platform has a dynamic process of mutual interaction among the data subject, data ontology and data environment, and its data security problems are manifested as diversified, complex and intertwined. In the face of the complexity and variability of the data environment, it is difficult for data subjects to strike a balance between effective data utilization and security risks. For example, the external environment of a variety of data protection laws and regulations, policies and industry data security standards continue to be introduced, the emergence of new technologies, data managers, data builders who do not timely study, update the platform data security management system and technical means, may cause serious data compliance issues, face penalties. Due to various risks in the internal environment, such as unsound organizational structure, imperfect management system, and weak technical system, the data ontology lacks favorable support, and it may be difficult to resist cyber-attacks, ransomware, internal leakage, and phishing email attacks.

For the interaction process between data subjects and data ontology, the data in the industrial information service platform are many and scattered, involving different industrial fields and industrial chains, and the data itself may not be sensitive, but after processing and integration, it becomes more sensitive, for example, the data related to industrial talents are processed to form a talent portrait. If the access rights of different data builders are not clearly delineated, and the data classification and grading and management strategies are not clear, it is easy to cause illegal data access, ultra vires access, tampering and leakage. In addition, if data consumers do not set up effective protection measures after acquiring data or data products, it may also lead to data abuse or leakage.

To summarize, the behavior of data subjects, the nature of the data ontology and changes in the data environment, as well as their interaction processes may generate data security problems. In order to better solve these problems, it is necessary to grasp the operating law of the data ecosystem as a whole, improve the adaptability and foresight of laws and regulations, strengthen the awareness of data security, improve the data management system, focus on technical protection, and build a comprehensive and three-dimensional data security governance system.

5 Data Security Governance for Industrial Information Service Platforms

Industrial information service platforms may involve important data in key industries such as national defense, industry, telecommunications, transportation, natural resources, health, finance, etc., as well as sensitive information on China's major projects, important scientific and technological achievements, and the dynamics of key technologies, etc. These characteristics put forward a strong demand for data security governance and the construction of an all-round data security system, with the key to maintaining the integrity of the data and promoting the creation of value of the data in balance. The key lies in maintaining data integrity and security and promoting data value creation, i.e., balancing development and security. In order to strengthen data security, explore data value and safeguard data services, it is necessary to synthesize the data subject, data ontology and data environment.

Data security governance is a more general set of measures that requires comprehensive consideration from the aspects of organizational structure, management system, technical system and operation system. Combining the characteristics of the data ecosystem of the industrial information service platform to build a robust and efficient data security governance system is very critical for realizing the effective protection and rational use of data. Based on the above research, the data security governance framework of industrial information platform constructed in this paper is shown in **错误!未找到引用源。**.

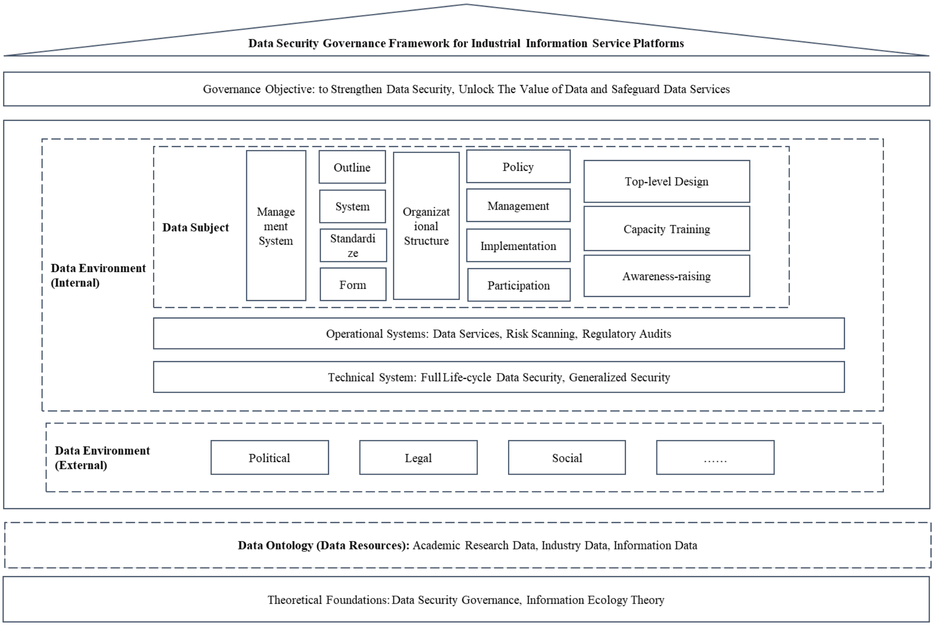
Data Security Governance Framework for Industrial Information Service Platforms
Governance Objective: to Strengthen Data Security, Unlock The Value of Data and Safeguard Data Services
Data Environment (Internal)
Data Subject
Manage ment System
Outline
System
Standardi ze
Form
Organizat ional Structure
Policy
Management
Implementation
Participation
Top-level Design
Capacity Training
Awareness-raising
Operational Systems: Data Services, Risk Scanning, Regulatory Audits
Technical System: Full Life-cycle Data Security, Generalized Security
Data Environment (External)
Political
Legal
Social
……
Data Ontology (Data Resources): Academic Research Data, Industry Data, Information Data
Theoretical Foundations: Data Security Governance, Information Ecology Theory

Fig. 3. Data security governance framework for industrial information service platforms

5.1 Data Subject: Strengthen Data Security Control and Enhance Data Security Awareness

The data ecosystem subject of industrial information service platform is complex, which not only needs to pay attention to internal data security management, but also needs to guarantee external security services. "Three parts technology, seven parts management" is a famous viewpoint in the field of network security. For the data security of industrial information service platform, from the perspective of data subjects, it is crucial to strengthen the top-level design of data security and enhance the awareness of data security. Data managers need to first improve their understanding of data security governance methods and practice levels, and do a good job in organizational structure construction, management system development, data security training, technical protection, risk combing, etc., in order to strengthen the data security awareness of data builders and data consumers while at the same time constraining them.

In terms of organizational structure, a special data security team should be set up, with data managers as the decision-making and management layer, data builders as the execution layer, and data consumers as the participation layer, and an alliance structure for data sharing should be established to manage the source, transmission, and use of data, and to protect the data rights and interests of users. In terms of management system, data managers should establish a set of standardized data security management norms and standards applicable to the characteristics of industrial data under the broad scope of satisfying laws and regulations, management regulations, and industry standards, specifically including the general outline of management, management system, process operation and normative documents, form documents, etc., so as to control the whole process of data collection, data access control, data classification and grading of industrial information service platform. control. At the same time, the screening and auditing of sources and the use of data also need to be regulated to prevent malicious data acquisition and abuse. In addition, data builders and data consumers need to raise their awareness of data security and enhance it by regularly attending data security training to understand the importance of data security, data security governance processes, data security management systems, and methods for handling data leakage.

5.2 Data Ontology: Standardize the Data Collection Process and Guarantee the Safe Flow of Data

The data resources in the industrial information service platform are an important part of the operation of the system platform, and the safe flow of data is the basis for ensuring the normal operation of the business. For data resources, it is necessary to set up data security policies based on the whole life cycle of data collection, transmission, storage, use, exchange and destruction as well as based on business scenarios in order to realize the safe flow of data. In particular, in the process of data collection, due to the different situations involving data from different sources such as self-collection, commercial procurement and exchange data, corresponding data security policies should be set up to control them respectively.

Considering further, the industrial information service platform needs to establish corresponding standards around data value assessment and data supplier evaluation in commercial data procurement to ensure the reasonableness of data transactions and avoid the problem of invalid data due to the data quality deviation or update mechanism that makes the data unable to satisfy the industrial information service. Currently, for the entire data factor market, data rights and pricing mechanism are research hotspots. The value of data can be reflected in its generation, utilization and sale, etc. For different types of data, it is necessary to ensure the rights and interests of data supply and demand parties, as well as to promote the fair realization of data value. Standardizing the data collection process and promoting the research of data pricing mechanism will also help the industrial information platform party to gain in the service process. Through well-defined rights and interests attribution, fair pricing mechanism, and comprehensive data security management, the value of the data ontology can be more effectively explored and realized, and at the same time, the responsibility and obligation of data security can be better fulfilled.

5.3 Data Environment: Building a Secure Data Environment and Optimizing Data Service Ecology

Building a safe data environment is crucial for the industrial information service platform to guarantee operational services. In terms of the technical system, the industrial information service platform needs to build data security measures that can support new technologies such as artificial intelligence, big data processing, cloud computing, blockchain, etc., and implement strict security protection in the whole life cycle of the data, including the use of data sandboxes and other technologies to ensure that the data resources are safe and effective in the whole environment. In addition, data security is not a quick fix, but requires long and continuous operation and management. The industrial information service platform needs to implement regular data security checks, regular backups and conduct security audits. For possible data leakage, tampering, etc., it is necessary to form a rapid response emergency mechanism to deal with possible data security incidents in a timely manner and minimize losses.

In addition, optimizing the data service ecosystem requires the construction of an open, collaborative, efficient and secure data-sharing environment, which promotes the development and utilization of data while safeguarding data security. The core of industrial information service platform is to provide data-based industry-specific forward-looking insights, on-demand customized industrial analysis services, etc., aiming to comprehensively explore and enhance the value of data, and provide decision-making support for users. For industrial development, necessary data sharing helps to form a healthy data service ecosystem and maximize the use of data resources, and it is necessary to promote data opening and sharing under the premise of ensuring data security. In short, building a safe, efficient and orderly data environment and continuously optimizing the data service ecosystem can maximize the excavation and in-depth use of data resources on the basis of balancing the relationship between security and development, so as to truly realize the value-added data of the industrial information service platform and contribute to the promotion of industrial development.

6 Conclusion

Based on the information ecology theory, this paper carries out an in-depth study on the data security of industrial information service platform. The data ecological framework of industrial information service platform is constructed by the three elements of data subject (data manager, data builder and data consumer), data ontology (data resources) and data environment (external environment and internal environment), and the representative data security problem is analyzed from the actual situation of the constituent elements and element interactions, and the data security of industrial information service platform is constructed with the goals of strengthening data security, exploring the value of data and guaranteeing data services. Finally, it constructs the data security governance framework of industrial information service platform with the goal of strengthening data security, exploring data value and guaranteeing data service.

From the data subject dimension, it is recommended that data managers strengthen the top-level design of data security, enhance data security control from the perspectives of organizational construction, management system, etc., and data builders and data consumers pay attention to improving data security awareness; from the data ontology dimension, it is recommended to promote the research of data rights and pricing mechanism, standardize the data collection process, and ensure the safe flow of data throughout the life cycle; from the data environment dimension, it is recommended to build a secure data security governance framework through the technical system and operation system, and to build a secure data security system through the technical system and operation system. From the dimension of data environment, it is recommended to build a safe data environment through technical system and operation system, promote data opening and sharing, and optimize the ecology of industrial data service.

References

1. Wang Haitao. Research on Data Security Issues of Enterprise Mobile Application Software under National Security Perspective. Graduation Thesis, People's Public Security University of China, Beijing (2023).
2. Xiong Huixiang, Feng Shan, Hu Chun, et al. Research on Service Mode Innovation of Information Service Platform for Strategic Emerging Industries under Big Data Environment. Intelligence Theory and Practice, Journal 43(7):81-87(2020).
3. Yang Yujiao, Yuan Qinjian. Information ecology theory and its application and prospect in the field of information system research. Modern Intelligence, Journal 42(05):140-148(2022).
4. Ono K, Maruyama K .Information platform: Concepts and research topics. nii journal(2001).
5. Sun Qing. International experience and inspiration of macro management of strategic emerging industries. Science and Technology Progress and Countermeasures, Journal 30(10):51-54(2013).
6. Zhang Jiankun. Research on information ecological niche and its evolution model for information service platform. Graduation Thesis, Beijing Institute of Technology, Beijing(2010).
7. Hu Changping, Zhang Min. The Practice of Information Service Platform for Supporting Industry Innovation in the European Union and Its Implications. Library Forum, Journal 06:187-191(2007).
8. Xiao Hui. Research on the Construction of Knowledge Network Platform for Strategic Emerging Industries in Hubei Province. Graduation Thesis, Huazhong Normal University, Hubei(2018).
9. Zhao Yingying, Zhang Han, Zhao Yuhong. Constructing an information service platform for biomedical industry clusters. Chinese Journal of Medical Library and Intelligence, Journal 25(3):8-12(2016).
10. James C. French, Sylvia Spengler, Science and Engineering Information Integration and Informatics (SEIII). https://www.nsf.gov/pubs/2004/nsf04528/nsf04528.htm, last accessed 2004/12/15.
11. Sun Zhen. Research on Information Service Model of Strategic Emerging Industries. Graduation Thesis, Nanjing Agricultural University, Jiangsu(2014).
12. Gao Jie, Xiao Haiqing, Yi Ming. Research on Information Resource Layered Service Mode for Strategic Emerging Industries. Intelligence Theory and Practice, Journal 46(07):33-43(2023).

13. Mao Yihong, Yang Yuanyuan, Huang Shuiqing. Empirical analysis of user utilization of new agricultural information service platform. Journal of National Library, Journal 22(05):68-73(2013).
14. Miao Chun, Zhu Peng. A study on the grouping of factors influencing users' willingness to continue using financial information service platform. Intelligence Science, Journal 40(12):88-95(2022).
15. Li Xueying, Zhang Ruiqing, Yang Bo, et al. Data Security Governance Practices. Information Security Research, Journal 8(11):1069-1078（2022).
16. Lv Mingyuan, Gong Yanan. China's Data Security Governance Development Trends, Problems and Foreign Data Security Governance Experience. Science and Technology Management Research, Journal 43(2):21-27(2023).
17. Chen Xiaoyu. Research on data security risk governance of e-commerce platform. Graduation Thesis, Heilongjiang University, Heilongjiang(2023).
18. Dong Muxin, Xu Yude. Data Security and Governance Path in the Digital Transformation of State-Owned Enterprises - Based on Information Ecology Perspective. Finance and Accounting Monthly, Journal 13:132-136(2022).
19. Kang Li, Zeng Rong. Research Status and Prospect of Information Ecosystem in China[J]. Library and Intelligence Work, Journal 64(4):113-124(2020).
20. Forest W. Horton jr. Information ecology. Journal of Systems Management, Journal 29(9):32–36(1978).
21. Francisco-Javier García-Marco. Libraries in the digital ecology: reflections and trends. The Electronic Library, Journal 29(1):105-120(2011).