Influencing Factors and Cultivation Strategies for Data Security Literacy among Data Practitioners in Internet Enterprises*

Li Qingwei Liu Yan Zhou Hang

2026-07-24

ChinaRxiv

Abstract

Exploring the influencing factors and cultivation strategies of data security literacy among enterprise data practitioners not only helps improve the data security protection capabilities of Internet enterprises, but also provides important references for the career development of data practitioners. This paper adopts the grounded theory method to identify the influencing factors of data security literacy among data practitioners in Internet enterprises, and uses the structural equation modeling method to analyze and test these factors. The study finds that data practitioners'educational background, negative experiences such as improper use of data, and the data security management norms of their enterprises have significant impacts on the data security literacy of data practitioners in Internet enterprises. Accordingly, targeted cultivation strategies for data security literacy among data practitioners in Internet enterprises are proposed, with the aim of providing theoretical guidance and practical reference for cultivating data security literacy among data practitioners.

Full Text

[**Academic Focus: Literacy Development in the AI Environment**]

Influencing Factors and Cultivation Strategies for Data Security Literacy among Data Practitioners in Internet Enterprises*

Li Qingwei Liu Yan Zhou Hang
School of History and Culture, Hubei University, Wuhan, 430062

Abstract Exploring the factors influencing the data security literacy of enterprise data practitioners and corresponding cultivation strategies not only helps improve the data security protection capabilities of Internet enterprises, but also provides an important reference for the professional development of data practitioners. This paper adopts the grounded theory method to identify the factors influencing data security literacy among data practitioners in Internet enterprises, and uses structural equation modeling to analyze and test these influencing factors. The study finds that data practitioners' educational background, negative experiences such as improper use of data, and the data security management norms of their enterprises have significant effects on the data security literacy of data practitioners in Internet enterprises. On this basis, targeted cultivation strategies for data security literacy among data practitioners in Internet enterprises are proposed, with a view to providing theoretical guidance and practical reference for cultivating data security literacy among data practitioners.

[**Keywords**] data security literacy; Internet enterprises; data practitioners; influencing factors

[**Chinese Library Classification No.**] G258.6 [**Document Code**] A
[**Article ID**] 1003-7845 (2026) 03-0018-09

[**Citation Format**] Li Qingwei, Liu Yan, Zhou Hang. Research on influencing factors and cultivation strategies for data security literacy among data practitioners in Internet enterprises[J]. *Library Work in Colleges and Universities*, 2026(3): 18-26.

Introduction

With the full arrival of the digital economy era, data has become a key production factor alongside land, labor, capital, and technology, and is the core engine driving innovation and development in the economy and society[1]. As entities with the densest data resources, the most cutting-edge data applications, and the most active data innovation, Internet enterprises, while enjoying data dividends, also face unprecedented data security challenges. As the direct processors, users, and value extractors of enterprise data, data practitioners determine, through the level of their data security literacy, the solidity of an enterprise' s data security defense line[2]. The data life cycle includes data collection, processing, storage, analysis, and transmission[3], and the level and capability with which employees perform their work tasks mainly encompass multiple dimensions such as knowledge, skills, and motivation[4]. Based on this, this study holds that the data security literacy of data practitioners refers to the security management awareness, knowledge, and capabilities they possess in processes such as data collection, processing, storage, and use.

At present, scholars have carried out relatively extensive research on the influencing factors of data security literacy, and the identified factors mainly concentrate on two major dimensions: the micro-level individual dimension and the macro-level environmental dimension. At the micro individual level, research focuses on the shaping effects of individual psychological mechanisms[5-6], accumulated experience[7], and demographic characteristics[8-10] on data security literacy; at the macro environmental level, the factors influencing data security literacy mainly include external environmental factors such as family[11], school[12], and society[13-14]. Current research by scholars still has certain limitations: on the one hand, existing studies mostly target groups such as students and teachers, while insufficient attention has been paid to data practitioners in Internet enterprises who are truly on the front line of big-data production, and there are few studies on the data security literacy of Internet data practitioners; on the other hand, scholars have rarely adopted methods combining qualitative exploration with quantitative testing to study the factors influencing data security literacy. Therefore, this study takes data practitioners in Internet enterprises as its research subjects, uses grounded theory to extract the factors influencing data practitioners' data security literacy, and verifies them through structural equation modeling. On this basis, it proposes scientific and effective cultivation strategies for data security literacy, with a view to providing feasible practical guidance for Internet enterprises to improve employees' data security capabil-

ities, strengthen organizational data security defenses, and improve enterprise data security governance systems.

1 Acquisition of Factors Influencing Data Security Literacy among Data Practitioners in Internet Enterprises

1.1 Sample Selection and Data Collection

This study adopts grounded theory to explore the factors influencing data security literacy among data practitioners in Internet enterprises. According to the 97 newly added digital occupations in the *Occupational Classification Code of the People' s Republic of China (2022 Edition)*[15], this study defines data practitioners in Internet enterprises as those who specialize in

---

* This article is one of the research outcomes of the National Social Science Fund Youth Project "Reshaping and Adaptive Optimization Strategies of the Academic Information Ecology by AI4S" (Project No.: 25CTQ035).

Author profiles: Li Qingwei, Ph.D., lecturer, master' s supervisor; research interests: information resource management, information ecology, and user information behavior. Liu Yan, master' s student; research interest: user information behavior. Zhou Hang, master' s student; research interests: user information behavior and information services.

Date received: 2026-02-14 Responsible editor: Yang Qianzi.

engaged in work related to data collection, processing, analysis, management, and utilization in the Internet field; using knowledge and skills from computer science, mathematics, and related areas; and applying Internet and big-data technologies to mine, analyze, and use massive amounts of data so as to extract valuable information and knowledge and support enterprises' business and management decision-making. Accordingly, the interviewees in this study were mainly drawn from core positions such as business data analysts, data-security engineering technicians, and database operations administrators, supplemented by practitioners in other data-related positions. To ensure the representativeness of the interviewees, this study required them to have work experience in data-related positions and to be familiar with enterprise data business processes and security specifications. On this basis, the authors recruited participants through their company, university alumni networks, and partner enterprises, and ultimately identified 27 interviewees from different organizations—mainly private enterprises, with some state-owned enterprises included. During the analysis, 22 sets of materials were first coded level by level to extract influencing factors, while 5 sets of materials were reserved for testing theoretical saturation, thereby ensuring the reliability of the research results. Based on literature analysis and preliminary interviews, this paper formulated an interview outline covering the following five dimensions:

(1) Current status of data-security literacy. The study investigated interviewees' attitudes toward and degree of attention to data security in their daily work; asked them to self-assess their own level of data-security literacy; requested examples of relevant professional knowledge and practical skills they had mastered; and asked about data-security risks and practical problems encountered in past work, as well as their personal responses.

(2) Influence of individual factors. The study explored how personal conditions such as personality traits and values affect the formation of data-security literacy; examined practitioners' subjective willingness to improve their security literacy through self-directed learning; clarified the core reasons driving their learning; and recorded the main channels and learning methods through which they acquire data-security knowledge in daily life.

(3) Influence of the enterprise environment. The study examined the construction of enterprise data-security rules and regulations, as well as employees' familiarity with these systems; investigated the content, forms, frequency, and actual effectiveness of enterprise security training; clarified the division of responsibilities for enterprise data-security positions and confirmed employees' own scope of duties; assessed the overall atmosphere of enterprise emphasis on data security and its guiding effect on employees' work behavior; examined the incentive mechanism for reporting hidden risks and its implementation effects; and asked about the impacts of past enterprise data-security incidents and the subsequent corrective and improvement measures.

(4) Influence of the external environment. The study focused on the impact of the overall social public-opinion atmosphere regarding data security on interviewees' data-security literacy; investigated interviewees' understanding of frontier security-technology trends in the industry, as well as the new demands for improving data-security literacy brought about by new technologies; and asked about the interference caused by insecure information on the Internet and how interviewees identify and respond to such information.

(5) Suggestions for optimizing literacy improvement. The study solicited feasible measures for enterprises to improve data-security literacy; proposed directions for supplementing the content and optimizing the forms of existing security training in light of actual work needs; explored effective methods for strengthening interviewees' initiative in attaching importance to data-security awareness; and collected suggestions for enterprises to cultivate a data-security culture and create a secure professional atmosphere.

This interview-based investigation was conducted mainly from July to August 2025. The interviews combined offline face-to-face semi-structured interviews with remote online video interviews. Each interview lasted 30–60 minutes. The basic information of the interviewees is summarized in Table 1.

Table 1 Basic information of the interviewees

Statistical item	Category	Number	Percentage/%
Gender	Male	11	40.74
Gender	Female	16	59.26
Age	Under 25 years old	2	7.41
Age	25–29 years old	19	70.37
Age	30–34 years old	4	14.81
Age	35 years old and above	2	7.41
Educational attainment	Bachelor' s degree or below	10	37.04
Educational attainment	Master' s degree	16	59.26
Educational attainment	Doctoral degree	1	3.70
Data-related position category	Database operations administrator	6	22.22
Data-related position category	Business data analyst	10	37.04
Data-related position category	Data-security engineering technician	5	18.52
Data-related position category	Other data positions	6	22.22
Years of employment	Less than 3 years	7	25.93
Years of employment	3–5 years	14	51.85
Years of employment	More than 5 years	6	22.22

1.2 Data Processing

1.2.1 Open Coding

In the open-coding stage, 94 concepts and 12 initial categories were obtained, as shown in Table 2.

Table 2 Concepts and initial categories formed through open coding (examples)

Initial category	Concepts
b1 Educational background	a1 Professional background; a2 Courses studied; a3 Educational level
b2 Work experience	a4 Industry; a5 Nature of position; a6 Professional experience; a7 Work content
b3 Personality traits	a8 Cautious personality; a9 Meticulous personality
.....	.....
b10 Enterprise data-security training system	a74 Data-security testing; a75 Mandatory data-security course for all employees; a76 Enterprise-platform data-security courses
b11 Legal and regulatory system	a77 Legal safeguards; a78 Normative guidance; a79 Clarification of data-processing norms; a80 Principle of legality; a81 Protection of subject rights and interests; a82 Division of responsibilities for data-security supervision; a83 Legal boundaries of data processing; a84 Methods for compliant data collection and use; a85 Data-security laws and regulations
b12 Data-security governance	a86 Identification of data assets; a87 Assessment of threats and vulnerabilities; a88 Analysis of threat impacts and probabilities; a89 Risk-management strategies; a90 Real-time monitoring; a91 Periodic assessment; a92 Monitoring and reporting; a93 Emergency response; a94 Public-opinion monitoring

1.2.2 Axial Coding

By further merging the initial categories, this study inductively derived five higher-level main categories, as shown in Table 3.

Table 3 Main Categories Formed through Axial Coding

Main Category	Initial Category	Connotation of the Initial Category
B1 Individual attributes	b1 Educational background	Includes educational attainment, major, school, and performance at school, reflecting an individual' s knowledge structure and academic ability.
B1 Individual attributes	b2 Work experience	An individual' s position, job responsibilities, industry experience, and performance achievements.
B1 Individual attributes	b3 Personality traits	An individual' s behavioral patterns, psychological characteristics, and emotional responses.
B2 Negative experiences	b4 Data security threats	Situations in which data are tampered with, deleted, or leaked during storage, transmission, or processing, resulting in data incompleteness or loss of security.
B2 Negative experiences	b5 Improper use of data	Acts of illegally accessing, using, or disclosing data without authorization or in violation of laws and regulations, ethical norms, or other rules.
B3 Individual cognition	b6 Perception of data security risks	The degree of awareness and vigilance regarding data security risks, including identifying potential threats, assessing the magnitude of risks, and evaluating possible consequences.

Main Category	Initial Category	Connotation of the Initial Category
B3 Individual cognition	b7 Self-efficacy	An individual' s evaluation of their own competence and confidence in the field of data security.
B4 Enterprise data security environment	b8 Enterprise data security management norms	Rules, procedures, and requirements formulated by an enterprise for data security management.
B4 Enterprise data security environment	b9 Enterprise data security technical requirements	Technical standards and requirements that an enterprise must meet in relation to data security.
B4 Enterprise data security environment	b10 Enterprise data security training system	A training system established by an enterprise to enhance employees' awareness and capabilities in data security.
B5 Data security regulatory system	b11 Legal and regulatory system	Laws, regulations, and policy documents on data security formulated by a country or region.
B5 Data security regulatory system	b12 Data security governance	Management and monitoring activities carried out to ensure data security.

1.2.3 Selective Coding and Test of Theoretical Saturation

In the process of selective coding, this paper analyzes the relationships among these categories. The typical relationship structures of the core category and representative statements are shown in Table 4. At the same time, the five reserved case materials were coded, and no new concepts or categories were found. The logic among the categories was consistent with the previous analytical results, indicating that this study has reached theoretical saturation.

Table 4 Typical Relationship Structures of the Core Category and Representative Statements

Typical Relationship Structure	Connotation of the Relationship Structure	Representative Statements from Respondents
Individual attributes → data security literacy	Educational background, work experience, and personality traits influence data security literacy.	S10: The younger generation usually comes into contact with digital technologies and the Internet earlier, may adapt more quickly to new technologies and new tools, and has a certain awareness of the security of online behavior. Older people may encounter challenges when learning new technologies and tools, but this does not mean that their data security literacy is low; older people usually have rich experience and deep industry knowledge.

Typical Relationship Structure	Connotation of the Relationship Structure	Representative Statements from Respondents
Negative experiences → data security literacy	Negative experiences involving data security threats and improper use of data influence data security literacy.	S08: In life, I have encountered situations in which my personal information was stolen, which also falls under data leakage. I feel strongly averse to this because it involves personal privacy and confidential information. To guard against such risks, when choosing platforms on which to display personal information, I pay more attention to their protection and confidentiality; if sufficient safeguards are lacking, I will not provide personal information.
Individual cognition → data security literacy	Perception of data security risks and self-efficacy influence data security literacy.	S13: I believe that the illegal or improper use of data may lead to serious consequences, including economic losses, privacy leakage, loss of reputation and trust, and social and ethical issues. This risk awareness makes me attach greater importance to data protection and has enhanced my awareness of data security.

Typical Relationship Structure	Connotation of the Relationship Structure	Representative Statements from Respondents
Enterprise data security environment → data security literacy	Enterprise data security management norms, enterprise data security technical requirements, and enterprise data security training systems influence data security literacy.	S14: Enterprises have very high requirements for data security technologies, including data encryption, firewalls, intrusion detection, and so on. These requirements prompt me to continuously learn and master the latest data security technologies and methods, so as to improve my own data security knowledge and ability to respond to data risks.
Data security regulatory system → data security literacy	The legal and regulatory system and data security governance influence data security literacy.	S13: I believe that the promulgation of laws and regulations helps enhance the data security awareness of data practitioners. These laws, regulations, and policies provide us with clear data security guidance and norms, enabling us to more clearly recognize the importance of data security and specific practical methods.

2 Verification of Influencing Factors of Data Security Literacy among Data Practitioners in Internet Enterprises

2.1 Research Hypotheses on the Influencing Factors of Data Security Literacy among Data Practitioners in Internet Enterprises

2.1.1 Individual Attributes Individual attributes include educational background, work experience, and personality traits. The educational background of data practitioners, especially a professional background related to information

technology or law, may equip individuals with a more solid foundation of knowledge about data security, thereby influencing their data security literacy[16]. Data practitioners with richer professional experience have more opportunities to hone their data security capabilities in practice; by handling various complex data security issues, their abilities to identify, prevent, assess, process, and control data security risks are continuously improved[17]. Personality traits refer to an individual' s behavioral style, psychological qualities, and emotional responses. Prudent and meticulous data practitioners are more careful when handling data, which helps avoid potential data security risks. Based on this, this study proposes the following hypotheses:

H1a: The educational background of data practitioners in Internet enterprises has a significant positive effect on their data security literacy.

H1b: The work experience of data practitioners in Internet enterprises has a significant positive effect on their data security literacy.

H1c: The personality traits of data practitioners in Internet enterprises have a significant positive effect on their data security literacy.

2.1.2 Negative Experiences Negative experiences include data security threats and improper use of data. Experiences of data security threats can strengthen individuals' cognitive appraisal of the severity of threats, thereby promoting improvements in data security literacy[18]. Experiences of improper data use can trigger a significant increase in privacy-risk perception and willingness to protect, thus positively driving individuals' security behaviors and compliance awareness[19]. For data practitioners in Internet enterprises, personally experiencing such negative events can deepen their understanding of data security issues and stimulate their protective motivation. Based on this, this study proposes the following hypotheses:

H2a: Negative experiences involving data security threats have a significant positive effect on the data security literacy of data practitioners in Internet enterprises.

H2b: Negative experiences involving improper use of data have a significant positive effect on the data security literacy of data practitioners in Internet enterprises.

2.1.3 Individual Cognition Individual cognition includes data security risk perception and self-efficacy. Data security risk perception is reflected in data practitioners' assessment of the harms of data leakage, their perception of their own vulnerability to data security threats, and their degree of concern about potential privacy losses or asset damage[20]. Protection Motivation Theory points out that when individuals believe data security risks are high and their impacts are severe—that is, when they truly perceive data security risks—they tend to adopt proactive data security behaviors[21]. Therefore, the perceived likelihood of data security risks affects data practitioners' willingness to improve

their data security literacy: the more likely they perceive risks to be, the more inclined data-position practitioners are to improve their data security literacy. Self-efficacy refers to data practitioners' confidence and belief in their own capabilities in data security; it is their self-assessment of whether they can take effective measures to protect data security[22]. Protection Motivation Theory points out that the generation of individual protective behavior depends on the interaction between threat appraisal and coping appraisal, in which self-efficacy is a key variable for predicting behavioral motivation. Some interviewees stated that they could identify and handle potential data security risks through data analysis tools and technologies, and complete their own duties rigorously and efficiently. Other interviewees stated that, despite their efforts, they still could not avoid data leakage and believed that the risks they faced exceeded the scope of their own capabilities[23]. Therefore, higher self-efficacy may encourage data practitioners to actively improve their data security literacy, whereas lower self-efficacy may cause them to give up improving their data security literacy. Based on this, this study proposes the following hypotheses:

H3a: Data security risk perception among data practitioners in Internet enterprises has a significant positive effect on their data security literacy.

H3b: Self-efficacy among data practitioners in Internet enterprises has a significant positive effect on their data security literacy.

2.1.4 Enterprise Data Security Environment The enterprise data security environment includes enterprise data security management norms, enterprise data security technical requirements, and enterprise data security training systems. The data security management norms formulated by enterprises provide data practitioners with clear behavioral rules and operational guidelines, guiding them to comply with relevant regulations in their daily work and helping to improve their awareness and literacy regarding data security[24]. The technical standards and requirements that enterprises must meet in data security are directly related to the technical abilities and knowledge that data practitioners need to master in actual work. They prompt data practitioners to continuously learn and master new data security technologies and tools, thereby ensuring the security and integrity of enterprise data; this process also improves employees' data security literacy. The training system established by enterprises to enhance employees' data security awareness and capabilities is an important pathway for improving data practitioners' data security literacy. Through systematic training and education, data practitioners can gain an in-depth understanding of the importance of data security, relevant regulations and standards, and security techniques and methods in practical operations[25]. Based on this, this study proposes the following hypotheses:

H4a: Enterprise data security management norms have a significant positive effect on the data security literacy of data practitioners in Internet enterprises.

H4b: Enterprise data security technical requirements have a significant positive

effect on the data security literacy of data practitioners in Internet enterprises.

H4c: Enterprise data security training systems have a significant positive effect on the data security literacy of data practitioners in Internet enterprises.

2.1.5 Data Security Regulatory System The data security regulatory system includes a system of laws and regulations and data security···

governance. Data practitioners need to understand and comply with laws, regulations, and policy documents on data security formulated by the state or region, so as to ensure that their work meets national and regional regulatory requirements [26]. In this process, data practitioners accumulate foundational knowledge of data security, thereby improving their data security awareness. Data security governance refers to the management and monitoring activities carried out collaboratively by multiple actors, such as governments, enterprises, and relevant organizations, to ensure data security, including data classification, data protection, data access control, and data security auditing [27]. An effective data security governance mechanism can enhance data practitioners' data security awareness and sense of responsibility, prompting them to adopt stricter and more prudent data-processing measures [28]. Based on this, the following hypotheses are proposed:

H5a: The legal and regulatory system has a significant positive impact on the data security literacy of data practitioners in Internet enterprises.

H5b: Data security governance has a significant positive impact on the data security literacy of data practitioners in Internet enterprises.

2.2 Questionnaire Design and Distribution

With reference to scale designs in the relevant literature, this study developed a measurement scale for factors influencing the data security literacy of data practitioners in Internet enterprises. The scale includes 38 items across dimensions such as educational background, work experience, personality traits, and data security threats. A five-point Likert scale was used for scoring. The specific variables, measurement indicators, and reference sources are shown in Table 5.

Table 5 Variables, Measurement Indicators, and Reference Sources

Variable	Measurement Indicator	References
Data security literacy	I am well aware of the importance and sensitivity level of business data.	Li Yihui [23]; Deng Lijun et al. [29]

Variable	Measurement Indicator	References
Data security literacy	I am well aware that problems such as leakage and improper use may occur during the collection, processing, analysis, and storage of business data.	Li Yihui [23]; Deng Lijun et al. [29]
Data security literacy	I am well aware of the laws, regulations, and industry standards that must be observed when obtaining and using data at work.	Li Yihui [23]; Deng Lijun et al. [29]
Data security literacy	I am well aware of the scope of protection for information and data under the *Personal Information Protection Law of the People' s Republic of China* and the *Data Security Law of the People' s Republic of China*.	Li Yihui [23]; Deng Lijun et al. [29]
Data security literacy	I can identify whether data and information at work have been altered or damaged, and can ensure the authenticity and integrity of data.	Li Yihui [23]; Deng Lijun et al. [29]
Data security literacy	I can correctly set strong passwords for operating systems, install antivirus software, regularly organize and back up important materials, and store them on secure media.	Li Yihui [23]; Deng Lijun et al. [29]
Educational background	The major I studied is highly related to data security.	Luo Li [30]

Variable	Measurement Indicator	References
Educational background	I have systematically studied data security-related courses through multiple channels, such as school education, online courses, and offline training.	Luo Li [30]
Educational background	I have a higher-education background and a relatively high level of education.	Luo Li [30]
Work experience	The nature of my position is highly related to data security.	Huo Mingkui et al. [17]
Work experience	I have rich professional experience in Internet data positions, such as data security engineering technicians, business data analysts, and database operations administrators.	Huo Mingkui et al. [17]
Personality traits	The data I come into contact with at work are relatively sensitive.	Self-developed
Personality traits	I am cautious and meticulous in character, and strictly follow norms in every stage of data processing.	Self-developed
Personality traits	I have a strong sense of responsibility and regard data security as an important duty.	Self-developed
Data security threats	I have experienced or learned about incidents in which data were tampered with or destroyed.	Fan Chunzhu et al. [31]

Variable	Measurement Indicator	References
Data security threats	I have experienced or learned about man-in-the-middle attacks or replay attacks.	Fan Chunzhu et al. [31]
Data security threats	I have experienced or learned about incidents in which data-collection software was modified.	Fan Chunzhu et al. [31]
Improper use of data	I have experienced or learned about incidents in which, after data were leaked and sold, they were illegally abused or improperly exploited by others.	He Jianping et al. [18]
Improper use of data	I have experienced or learned about incidents in which, after digital accounts were stolen, related data were used without authorization or handled in violation of regulations.	He Jianping et al. [18]
Improper use of data	I have experienced or learned about incidents at work in which data were illegally accessed, used, or disclosed.	He Jianping et al. [18]
Perceived data security risk	I am well aware of the security hazards faced by data at work, such as leakage, loss, damage, and distortion.	Lu Miaomiao [32]
Perceived data security risk	I am well aware of the security risks existing in data at work, such as virus transmission, system-platform vulnerabilities, and hacker intrusions.	Lu Miaomiao [32]
Self-efficacy	I believe that I have the ability to protect the security of data at work.	Li Yihui [23]; Jiang Bingbing [24]

Variable	Measurement Indicator	References
Self-efficacy	I believe that I possess certain skills and can prevent data security risks.	Li Yihui [23]; Jiang Bingbing [24]
Self-efficacy	If data are threatened, I believe that I know what to do.	Li Yihui [23]; Jiang Bingbing [24]
Enterprise data security management norms	The enterprise where I work has sound data security management regulations.	Zhu Lingling et al. [33]
Enterprise data security management norms	The enterprise where I work has a sound data security supervision mechanism.	Zhu Lingling et al. [33]
Enterprise data security management norms	The enterprise where I work has a sound punishment mechanism for data security violations.	Zhu Lingling et al. [33]

Table 5 (continued)

Variable	Measurement Indicator	Reference
Enterprise data-security technical requirements	Strict management of data permissions in the respondent' s enterprise	Self-developed
Enterprise data-security technical requirements	Strict access control in the respondent' s enterprise	Self-developed
Enterprise data-security technical requirements	Strict device management in the respondent' s enterprise	Self-developed
Enterprise data-security training system	The respondent' s enterprise conducts data-security training relatively frequently	Wu Zhixiang et al. [26]
Enterprise data-security training system	The data-security training content in the respondent' s enterprise is comprehensive	Wu Zhixiang et al. [26]

Variable	Measurement Indicator	Reference
Enterprise data-security training system	The data-security training assessment requirements in the respondent' s enterprise are strict	Wu Zhixiang et al. [26]
Legal and regulatory system	I believe that the current system of laws and regulations related to data security is sound and provides sufficient protection for data security	Huo Mingkui et al. [17]
Legal and regulatory system	I believe that the current dissemination and popularization of laws and regulations related to data security is relatively high	Huo Mingkui et al. [17]
Data-security governance	I believe that the current data classification and grading system is relatively sound	Self-developed
Data-security governance	I believe that the current accuracy and coverage of data-security public-opinion monitoring are relatively high	Self-developed

2.3 Questionnaire Collection and Statistics

To ensure the reliability of the questionnaire, before the large-scale formal distribution of the questionnaire, this study selected 100 data practitioners from different Internet enterprises to conduct a small-scale pilot survey. In the formal investigation stage, data were collected through a combination of online and offline methods. A total of 320 questionnaires were recovered. After excluding invalid samples such as those with abnormal response times and obvious response patterns in the results, 269 valid questionnaires were finally determined. Table 6 presents the statistical characteristics of the basic sample information.

Table 6 Statistics of Basic Sample Information Characteristics

Statistical Item	Option	Frequency	Percentage/%
Gender	Male	206	76.58
Gender	Female	63	23.42
Age	Under 25 years old	27	10.04
Age	25–29 years old	108	40.15
Age	30–34 years old	84	31.22
Age	35 years old and above	50	18.59
Educational background	Bachelor' s degree or below	193	71.75
Educational background	Master' s degree	54	20.07
Educational background	Doctoral degree	22	8.18
Job category	Database operation administrator	34	12.64
Job category	Business data analyst	31	11.52
Job category	Data-security engineering technician	165	61.34
Job category	Other data-related position	39	14.50
Length of employment	Less than 1 year	34	12.64
Length of employment	1–2 years	27	10.04
Length of employment	3–5 years	103	38.29
Length of employment	5 years or more	105	39.03

2.4 Data Analysis and Model Validation

2.4.1 Reliability and Validity Testing and Model Fit The Cronbach' s Alpha values for all dimensions of data-security literacy studied in this paper are above 0.7, indicating that the questionnaire has relatively high reliability.

This study used confirmatory factor analysis (CFA) to test the measurement model of the influencing-factor model for data-security literacy. The results show that all model fit indices (χ^2/df = 1.198, RMSEA = 0.027, CFI = 0.979, TLI = 0.974) reached an ideal level, demonstrating that the overall model fit is good. Most standardized factor loadings of the items are above 0.730, and all standardized coefficients are greater than 0.5, indicating strong correlations between the items and their corresponding latent variables; thus, all items can effectively measure their corresponding latent variables. The AVE values are all above 0.600, indicating that these latent variables can be more effectively explained by their observed variables. In terms of composite reliability (CR), the composite reliability of all latent variables is above 0.750, indicating good internal consistency among the observed variables under each latent variable. Meanwhile, in the influencing-factor model of data-security literacy in this study, the square root of the AVE for every latent variable is greater than its correlation coefficients with other latent variables, indicating good discriminant validity.

2.4.2 Structural Equation Model Testing This study used AMOS 23.0 software to test the structural equation model of the influencing factors of data-security literacy. The results show that all model fit indices (χ^2/df =

1.198, RMSEA = 0.027, CFI = 0.980, TLI = 0.976) meet the recommended standards. The model is highly consistent with the sample data, has an ideal fitting effect, and can be used for subsequent hypothesis testing.

2.4.3 Analysis of Hypothesis Results The test results of the path coefficients are shown in Table 7. The S.E. values of all variables are greater than 0, indicating that there is no collinearity problem among the measurement variables under each dimension. The data analysis shows that work experience, personality traits, and perceived data-security risk have no significant effect on data-security literacy (p values are all greater than 0.05), so hypotheses H1b, H1c, and H3a are not supported; the remaining latent variables have significant positive effects on data-security literacy, so the remaining hypotheses are supported.

Table 7 Results of Path Coefficient Testing

Path	Standardized coefficient	S. E.	C. R.	p	Validation result
Data security literacy ← Educational background	0.127	0.049	2.383	0.017	Supported
Data security literacy ← Work experience	0.073	0.056	1.314	0.189	Not supported
Data security literacy ← Personality traits	0.043	0.027	1.289	0.197	Not supported
Data security literacy ← Data security threats	0.114	0.046	2.384	0.017	Supported

Path	Standardized coefficient	S. E.	C. R.	p	Validation result
Data security literacy ← Improper use of data	0.117	0.057	2.106	0.035	Supported
Data security literacy ← Perceived data security risk	0.072	0.039	1.603	0.109	Not supported
Data security literacy ← Self-efficacy	0.130	0.055	2.366	0.018	Supported
Data security literacy ← Enterprise data security management norms	0.230	0.051	4.573	***	Supported
Data security literacy ← Enterprise data security technical requirements	0.100	0.046	2.228	0.026	Supported

Path	Standardized coefficient	S. E.	C. R.	p	Validation result
Data security literacy ← Enterprise data security training system	0.143	0.048	3.305	***	Supported
Data security literacy ← Legal and regulatory system	0.140	0.043	3.432	***	Supported
Data security literacy ← Data security governance	0.139	0.043	3.219	0.001	Supported

Work experience, personality traits, and perceived data security risk have no significant effect on data security literacy. In combination with the interview materials, the reasons for these three unsupported research hypotheses are discussed as follows. First, according to the interview materials, some senior employees have long been engaged in repetitive work and have not experienced real data security incidents, whereas some new employees, although having less work experience, have personally experienced negative security incidents such as data leaks and system attacks, and thus instead show stronger data security vigilance and response capabilities. Meanwhile, the rapid iteration of Internet technology makes it difficult for the experience accumulated by senior employees in the early stage to effectively cope with current new types of data security threats, thereby weakening to some extent the positive effect of work experience on data security literacy. Second, employees' data security behaviors are more constrained by the rules, regulations, and technical processes of Internet enterprises; differences in individual personality are difficult to manifest, resulting in an insignificant effect of individual personality traits on data security literacy. Finally, the interview materials show that data practitioners in Internet enterprises often regard data security as the work of the technical department and

believe that they themselves lack coping measures. Therefore, although these employees can perceive data security risks, they do not possess protective capabilities, causing perceived data security risk to remain merely at the level of anxiety rather than being transformed into actual data security literacy. This may lead to the insignificant effect of perceived data security risk on data security literacy. In summary, the security literacy of data practitioners in Internet enterprises depends more on the triggering of critical incidents and support from the enterprise environment than on personal traits or the accumulation of qualifications. Accordingly, this study deletes the above three nonsignificant paths.

3 Strategies for Cultivating Data Security Literacy among Data Practitioners in Internet Enterprises

3.1 Optimize full-cycle talent management and strengthen the foundation of individual security literacy

In terms of individual attributes, educational background affects the data security literacy of data practitioners in Internet enterprises. Therefore, enterprises need to optimize full-cycle management of data-practitioner talent and form a closed loop from recruitment and training to career development [34]. First, at the talent recruitment stage, enterprises may cooperate with universities to establish special scholarships, thereby attracting targeted professionals related to data security; situational simulation tests may also be introduced in recruitment to examine candidates' emergency response capabilities. Second, at the training stage, enterprises should implement graded and tiered training for in-service personnel. Junior data practitioners should focus on training in basic skills, while intermediate and senior data practitioners should concentrate on learning cutting-edge technologies. A "online + offline" training model should be adopted, making good use of online course resources on internal enterprise learning platforms as well as expert lectures, case seminars, and other activities organized offline. Finally, at the career development stage, enterprises should build dual promotion channels for technical experts and management, and establish a scientific and reasonable performance appraisal mechanism, incorporating indicators such as the incidence of data security incidents into performance appraisal [35].

3.2 Strengthen incident review and psychological support to promote the positive transformation of negative experiences

In terms of negative experiences, data security threats and the improper use of data affect the data security literacy of data practitioners in Internet enterprises. Therefore, enterprises should strengthen the review of data security incidents and psychological counseling for negative experiences, so as to promote the positive transformation of negative experiences. On the one hand, Internet enterprises should establish professional teams to conduct full-process

reviews of data security incidents that have already occurred, deeply analyze the technical and managerial problems present in those incidents, strengthen warnings through special-topic discussions and case publicity, regularly organize data security emergency drills and include them in assessments, and give commendations and rewards to individuals and teams with outstanding performance. On the other hand, enterprises should establish a comprehensive psychological support system, set up consultation hotlines, hold health lectures, build sharing platforms to encourage employees to exchange experiences, and optimize management processes based on employee feedback, while rewarding active participants. This can both strengthen security awareness and reduce employees' anxiety about negative events

psychological burdens and promote the shared growth of teams in Internet enterprises.

3.3 Build a diversified incentive system and enhance self-efficacy and cognitive level

In terms of individual cognition, self-efficacy affects the data security literacy of data practitioners in Internet enterprises. Therefore, enterprises should build an adaptive incentive and cultivation system centered on strengthening practitioners' perception of their capabilities and enhancing their confidence in securely performing their duties, fully stimulating data practitioners' work enthusiasm and subjective initiative, and improving their self-efficacy. First, enterprises should establish a positive value-recognition mechanism, focusing on practitioners'performance in fulfilling data security responsibilities, the effectiveness of risk assessment, and adherence to compliance, and should grant them honor-based recognition, public commendation, and affirmation of their value. Through psychological identification, enterprises can strengthen data practitioners' sense of professional value and confidence in their abilities, thereby consolidating the psychological foundation of their self-efficacy. Second, enterprises should provide data practitioners with clear and explicit pathways for improving data security capabilities and with professional guidance, and formulate personalized career development plans in light of employees' individual characteristics. At the same time, enterprises should implement an internal mentorship system featuring "one-to-one" guidance, organize knowledge competitions and customized course training, stimulate employees' initiative, and support the comprehensive improvement of professional competence and cognitive level.

3.4 Advance the systematic construction of the enterprise environment and strengthen internal security defenses

With regard to the enterprise data security environment, enterprise data security management norms, enterprise data security technical requirements, and enterprise data security training systems all affect the data security literacy of data practitioners in Internet enterprises. Therefore, enterprise environmental construction should be advanced from three aspects: institutions, technology, and

training. At the institutional level, enterprises should build a data full-lifecycle management framework, implement graded and classified protection and dynamic updating mechanisms, and formulate differentiated protection measures for data at different levels. At the same time, dedicated positions should be established to carry out regular audits, and security indicators should be incorporated into performance appraisal. At the technical level, enterprises should strengthen data security governance technologies covering the full process of data cleaning, exchange, integration, and other links, thereby building an intelligent and proactive data security protection system for enterprises [36]. At the training level, targeted data security training courses should be designed: management should focus on the formulation of strategy, technical posts should strengthen practical training, and ordinary employees should focus on learning basic knowledge. Meanwhile, a learning platform for resource integration should be established to fortify the enterprise' s internal security defenses.

3.5 Improve the data security regulatory system and create a sound external environment

In terms of the data security regulatory system, the legal and regulatory system and data security governance affect the data security literacy of data practitioners in Internet enterprises. Therefore, it is necessary to improve the construction of the data security regulatory system. In publicity and education on laws and regulations, official channels, social media, and other platforms may be used to publicize regulations; knowledge may be popularized through short videos, lectures, and other forms; and data security knowledge may be integrated into basic education and higher education. In terms of data security governance, regulatory departments may use technical means such as big-data analysis and artificial intelligence to achieve real-time monitoring and precise early warning of risks such as data leakage, tampering, and cyberattacks. At the same time, an industry threat-intelligence sharing mechanism should be established to promote joint prevention and control of security threats between government and enterprises. In addition, emergency plans should be refined and international cooperation strengthened; participation in the formulation of international data security standards should be actively pursued; advanced technologies and management models should be learned from; social forces should be guided to participate; a governance ecosystem featuring multi-party collaboration should be formed; and the improvement of data practitioners' data security literacy should be promoted.

4 Conclusion

This paper uses literature analysis, grounded theory, and structural equation modeling to explore the factors influencing the data security literacy of data practitioners in Internet enterprises, and proposes corresponding strategies for cultivating data security literacy. However, this study still has certain limitations. Follow-up research may incorporate the types of employers of data prac-

titioners in Internet enterprises into the scope of consideration, and conduct classified studies on the factors influencing the data security literacy of data practitioners in different types of enterprises, such as state-owned enterprises, listed companies, and small, medium, and micro enterprises. By analyzing differences among different types of enterprises, future studies can further investigate the mechanisms by which factors such as enterprise scale, industry status, and management mechanisms affect data practitioners' data security literacy, thereby providing theoretical basis and practical reference for formulating more targeted strategies to improve the data security literacy of data practitioners in Internet enterprises.

References

[1] Ma Feicheng, Lu Huizhi, Wu Yimei. Development and operation of the data-element market [J]. *Journal of Information Resources Management*, 2022(5): 4-13.

[2] Zhan Yuqi. A preliminary study on data security risks and countermeasures in cloud computing [J]. *Network Security Technology & Application*, 2024(4): 80-82.

[3] Meng Yuxiao, Zhou Xiping. A public security intelligence data governance method based on the data lifecycle [J]. *Information Research*, 2021(10): 33-40.

[4] McClelland D C. Testing for competence rather than for "intelligence." [J]. *American Psychologist*, 1973(1): 1-14.

[5] Zhu Shiqin, Lü Jialin, Zhang Yanqi. Research on pathways for improving college students' data security literacy based on grounded theory [J]. *Journal of Academic Library and Information Science*, 2025(6): 50-59.

[6] Cao Zhenxiang, Chu Jiewang. Research on the influence of mobile-device users' digital literacy on information security protection intentions and behaviors: estimation based on an Ordered Probit model [J]. *Journal of Intelligence*, 2023(11): 199-207.

[7] Ayuyang D M. Data security awareness and proper handling of ICT equipment of employees: an assessment [C]// *Science and Information Conference*. Cham: Springer, 2022: 682-692.

[8] Fang Shengqiang, Zhao Jun. Research on the correlation between resource endowment and data literacy among new primary and secondary school teachers: an investigation based on a heterogeneous-choice ordered Logit model [J]. *Education Academic Monthly*, 2023(3): 71-76.

[9] Wang Fang, Xu Lijie. Survey research on the current state of cybersecurity literacy among higher vocational students in the era of big data [J]. *Times Youth*, 2025(34): 111-113.

[10] Zhong Manping. Measurement of the digital literacy level of economics undergraduates and cultivation strategies [J]. *Journal of Yichun University*, 2025(2): 114–119.

[11] Wu Shikai. Differences in cybersecurity literacy between urban and rural minors and their influencing factors: based on data from the 11th Survey on the Internet Use of Chinese Minors [J]. *Southeast Communication*, 2024(4): 107–111.

[12] Guo Qian, Li Jianxia. An empirical study on the data literacy capabilities of college students focusing on security ethics education [J]. *New Century Library*, 2019(5): 14–19.

[13] Lei Yu, Wu Chao. Research on the mechanism and promotion of security data literacy [J]. *Journal of Intelligence*, 2019(9): 192–197, 207.

[14] Qin Dianqi, Zhang Yuwei. Intelligence literacy: A core element of information security theory [J]. *Information Studies: Theory & Application*, 2015(4): 30–33.

[15] Revision Committee of the *Occupational Classification Dictionary of the People's Republic of China. Occupational Classification Dictionary of the People's Republic of China: 2022 Edition* [M]. Beijing: China Labor and Social Security Publishing House, 2022: 208–211.

[16] Jia Ruonan, Wang Xiwei, Fan Xiaochun. Research on influencing factors of social network users' personal information security and privacy protection behavior [J]. *Modern Information*, 2021(9): 105–114, 143.

[17] Huo Mingxing, Zhu Jiaqi, Tan Jingping. Analysis of influencing factors and safeguard countermeasures for civil servants' information security behavior based on grounded theory [J]. *Information Science*, 2019(3): 49–54.

[18] He Jianping, Qi Runmei. Information security awareness and behavior of urban elderly people and their influencing factors [J]. *Journal of Southwest University of Political Science and Law*, 2021(6): 72–87.

[19] Xuan Changchun, Chen Subai. The influence of privacy-invasion experiences on willingness to protect personal information: Based on the theoretical perspectives of "risk-benefit" and regulatory focus [J]. *Chinese Journal of Journalism & Communication*, 2023(4): 138–156.

[20] Huang Jun, Gong Huaping, Xiong Juan. Influencing factors of college students' perceived information security risks on social media [J]. *Library Tribune*, 2024(7): 120–127, 160.

[21] Li Fengjing, Yuan Xiyi. Research on factors influencing individual subjective well-being under major emergencies: From the perspective of social cognition [J]. *Information Research*, 2024(5): 75–86.

[22] Tao Subai, Wei Juan. The "cost" of self-efficacy: A study on the paradox of privacy protection behavior among intelligent media users [J]. *Modern*

Information, 2024(5): 58–69.

[23] Li Yihui. Research on the influencing factors of data security literacy among property insurance personnel [D]. Wuhan: Hubei University, 2024.

[24] Jiang Bingbing. A brief discussion on the construction of anti-competitive intelligence systems for small and medium-sized enterprises under the wave of "Internet Plus" [J]. *China Management Informationization*, 2018(5): 77–79.

[25] Fang Xing, Lin Zhengjie. An empirical study on the influencing factors of employees' information security behavior: Based on the theory of planned behavior [J]. *Chinese and Foreign Entrepreneurs*, 2013(11): 122–123.

[26] Wu Zhixiang, Zhou Xingyu, Zhu Xiaofeng. Research on an intelligence system for risk early warning of national data security: Cognition, framework, and implementation [J]. *Information Studies: Theory & Application*, 2025(5): 64–72.

[27] Zhou Yi, Guo Mingrui. Construction and implementation of a governance mechanism for implicit data security risks in public data openness [J]. *Information Studies: Theory & Application*, 2024(12): 63–71.

[28] Kan Tianshu, Wang Ziyue. Global data security governance and China' s strategies in the digital economy era [J]. *Journal of International Security Studies*, 2022(1): 130–154, 158.

[29] Deng Lijun, Yang Wenjian. Research progress on individual data literacy evaluation systems and the connotations of related indicators [J]. *Library and Information Service*, 2017(3): 140–147.

[30] Luo Li. On the cultivation of citizens' information security literacy [J]. *Library and Information Service*, 2012(6): 25–28, 37.

[31] Fan Chunzhu, Deng Xiaozhao, Han Yi. Negative use behavior of social media users: A multi-source data fusion perspective [J]. *Library and Information Service*, 2022(15): 76–85.

[32] Lu Miaomiao. Analysis of influencing factors of archival information security based on structural equation modeling [J]. *Archives*, 2023(2): 67–72, 76.

[33] Zhu Lingling, Su Yihong, Zhu Yongfeng, et al. Identification of key influencing factors of government data open readiness: Taking provincial local governments as an example [J]. *Library and Information Service*, 2021(3): 75–83.

[34] Xing Wenming, Liu Wo. Research on factors influencing college students' digital literacy in the context of all-factor digital transformation [J]. *Digital Library Forum*, 2023(10): 79–90.

[35] Liu Chenhui, Huang Haoyuan, Dong Xinyu. The mechanism by which technostress affects civil servants' information security behavior: A mixed method based on SEM and ANN [J]. *Journal of Intelligence*, 2024(5): 201–207.

[36] Lu Kang, Liu Hui, Zhang Jing, et al. Personal data governance in smart libraries in the digital-intelligent era: Trust model and practical application [J]. *Library Work in Colleges and Universities*, 2024(6): 45-50.

Research on the Influencing Factors and Cultivation Strategies of Data Security Literacy Among Data Practitioners in Internet Enterprises

Li Qingwei Liu Yan Zhou Hang

School of History and Culture of Hubei University, Wuhan, 430062

Abstract Exploring the influencing factors of data security literacy among data practitioners in Internet enterprises and their cultivation strategies not only helps improve the data security protection capabilities of Internet enterprises, but also provides important references for the professional development of data practitioners. This study adopts a grounded theory approach to identify the influencing factors of data security literacy among data practitioners in Internet enterprises, and uses structural equation modeling (SEM) to analyze and validate these influencing factors. The study finds that the educational background of data practitioners, negative experiences such as the improper use of data, and corporate data security management norms exert significant influences on the data security literacy of data practitioners in Internet enterprises. Based on these findings, targeted cultivation strategies for enhancing data security literacy among data practitioners in Internet enterprises are proposed, aiming to provide theoretical guidance and practical reference for fostering data security literacy among data practitioners.

Keywords Data security literacy; Internet enterprises; Data practitioners; Influencing factors

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