On Enhancing Information Security Awareness of Corporate Employees in the Era of Big Data

Jing Sun[1], Youbin Chen[2*]

[1]General Management Department, Aerospace CH UAV Co., Ltd., Beijing 100074, China
[2]School of Foreign Languages, Sichuan University of Science and Engineering, Zigong 643002, China

*Corresponding author: Youbin Chen, youbinchen@suse.edu.cn

Abstract. In the era of big data, protecting information security has become extremely important, especially for corporate employees. Once information security problems occur, it will cause considerable losses to individuals, the enterprise and even the country. This paper first addresses the importance of information security and the significance of ensuring information security. Then a questionnaire survey was conducted among different people especially corporate employees. The survey shows that most corporate employees have moderate concern over the information security of the organization which they serve, and some even show no concern. Compared with government employees, their information security awareness is insufficient, so it is necessary for us to enhance their awareness. On this basis, we propose eight recommendations for enhancing the information security awareness of corporate employees in aspects such as training and education, privacy, publicity, competitions, tools and resources, culture, audits and drills, and confidentiality systems.

Keywords: Information security; Corporate employees; Era of big data; Information security awareness

1 Era of Big Data and Information Security

1.1 Overview

Recently, information security in the era of big data has aroused wide concern among scholars. Tian Qiu has explored the network security issue in the era of big data, and proposed some solutions for these issues[1]. Zhang Yuxia has reviewed the status quo of network information security, and explored some countermeasures for the current problems[2]. Ma Yaping and Fan Jingyan has conducted a questionnaire survey of personal information security awareness among college students[3]. Nevertheless, only a few scholars have researched into information security in enterprises. Gao Jiameng has researched into corporate information security capability building and its key influencing factors[4], and Bi Xingyuan has analyzed relevant risks in the era of big data, and

S. M. Chung et al. (eds.), *Proceedings of 2024 4th International Conference on Public Management and Big Data Analysis (PMBDA 2024)*, Advances in Economics, Business and Management Research 318,
https://doi.org/10.2991/978-94-6463-656-7_37

proposed corresponding information security protection strategies[5]. To date, none has discussed how to enhance the information security awareness of corporate employees, so it is of great significance to address the issue of corporate employees' information security awareness.

1.2 The Era of Big Data

Big data refers to data sets that are huge in scale, complex in structure, and difficult to process with traditional data processing methods and tools. It features large data volume, diverse data types, fast data processing speed, and low value density. Big data has wide applications in various industries, such as finance, healthcare, retail, manufacturing, and transportation. It can be used for market forecasting, customer relationship management, risk management, product optimization, and other aspects. According to the forecast of the market research company Marketsand Markets, the global big data market size will reach $103 billion by 2026[6][7].

Based on the data from the research institution IDC, the global big data market size has maintained a high growth rate in the past few years and is expected to reach hundreds of billions of dollars by 2025. Meanwhile, the generation and storage of data are also growing rapidly. It is expected that by 2025, the global data volume will reach hundreds of zettabytes (ZB). This means that a large amount of data will be generated every day, and they include structured data, unstructured data, and semi-structured data[8][9][10].

1.3 Information Security

Information security refers to the state in which an information system (including hardware, software, data, people, physical environment, and infrastructure) is protected from being damaged, altered, or disclosed due to intentional or accidental reasons, enabling the system to operate continuously, reliably, and normally, and ensuring that information services are not interrupted and business continuity is achieved[11].

For the protection of information security, the following aspects usually need to be considered:

(1) Data integrity: Data integrity means that the content of the expressed data is complete and can truly reflect all the ideas of the publisher without being tampered with or edited.
(2) Data confidentiality: That is, all ideas are known only within the scope of information permitted by the publisher.
(3) Information availability: That is, when information needs to be queried, complete information content can be obtained.
(4) Non-repudiation: That is, there is sufficient evidence to prove when and where the information publisher released certain information.
(5) Controllability: That is, to ensure that the processes such as the use, release, storage, and query of information and information systems are all in a controllable state[12][13].

1.4 Hazards of Information Security Breaches and Significance of Protection

Information security breaches may bring the following hazards to individuals:

(1) Personal privacy leakage: Hackers, cyber criminals, or other malicious entities may obtain personal information (such as names, addresses, phone numbers, email addresses, and ID numbers), resulting in the leakage of personal privacy.
(2) Economic losses: Information security breaches may lead to the theft of personal financial information (such as credit card numbers, and bank account information), thus causing economic losses.
(3) Reputation damage: Personal information may be maliciously misused or tampered, resulting in damage to reputation or a negative impact on personal image.

According to the statistics of China Anti-Fraud Center, as shown in Table 1, in 2022, a total of 1.55 billion fraud calls and 1.76 billion fraud messages were intercepted, and 210,000 fraud-related websites were blocked, helping the public avoid economic losses of more than 200 billion RMB yuan.

Table 1. Statistics of telecommunication frauds found in 2022

Categories	Fraud calls	Fraud messages	Fraud-related websites	Economic losses avoided
Data	1.55 billion	1.76 billion	210,000	200 billion RMB yuan

Source: *China Anti-Fraud Center*

A report jointly released by Apple and researchers from the Massachusetts Institute of Technology (shown in Fig. 1) says that over 2.6 billion personal records were breached in 2021 and 2022, and the number of data breaches more than tripled between 2013 and 2022. In the first nine months of 2023, the number of data breaches in the US increased by nearly 20% compared to all of 2022; over 80% of data breaches involved data stored in the cloud, and in the first three quarters of 2023, the number of ransomware attacks increased by almost 70% compared to the first three quarters of 2022. in the first eight months of 2023 alone, over 360 million people were victims of corporate and institutional data breaches, and in the first three quarters of 2023, one in four people in the US had their health data exposed in a data breach[14].

The destruction of information security can also bring huge harm to enterprises, mainly in the following aspects:

1) Economic losses: The destruction of information security may lead to the theft, alteration or deletion of important data of an enterprise, thus resulting in economic losses. This includes the leakage of commercial secrets, the infringement of intellectual property rights, and the loss of customer data, which may lead to a decline in competitiveness, a reduction in market share and damage to economic interests.
2) Reputation damage: Information security incidents may cause serious damage to an enterprise's reputation. Once the information of customers or partners is leaked,

the enterprise will lose their trust, resulting in the loss of customers and the breakdown of cooperative relationships, which will have a negative impact on the long-term development of the enterprise.

3) Legal liability and compliance risks: According to relevant laws and regulations, enterprises are responsible for protecting the data security of users. If an information security destruction event occurs, the enterprise may face legal proceedings, fines or penalties from regulatory authorities, bringing legal liability and compliance risks to the enterprise.

4) Operational disruption: The destruction of information security may cause the breakdown of an enterprise's IT system and affect its normal operations. This may include cyber attacks, malware infections, and system failures, resulting in the enterprise's inability to provide products or services, bringing economic losses and business interruptions to the enterprise.

5) Competitive disadvantage: The destruction of information security may put an enterprise at a disadvantage in competition. Competitors may use stolen commercial secrets or sensitive information to gain a competitive advantage, thus threatening the enterprise's market position and development prospects.

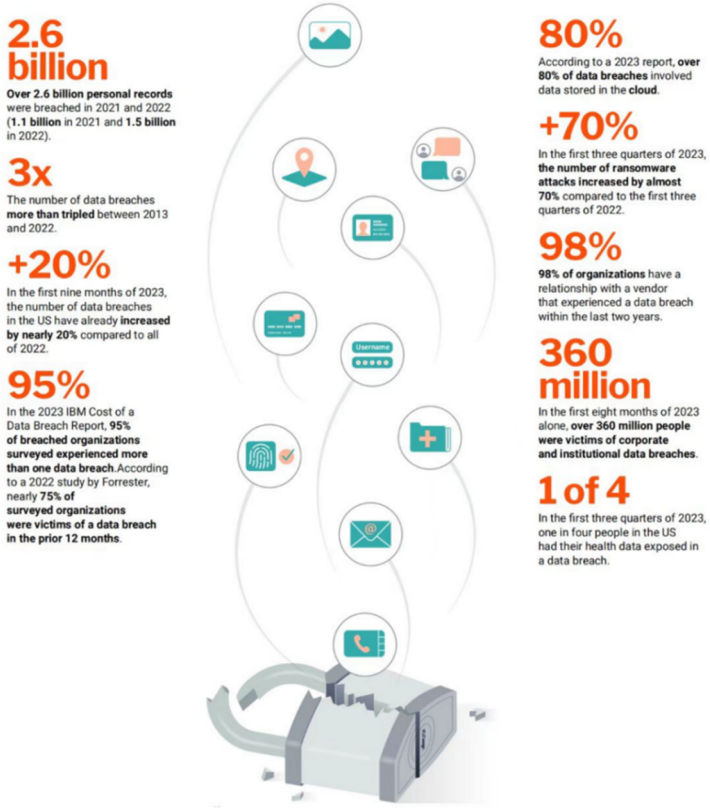

Fig. 1. Overview of Key Factors of the Continued Threat to Personal Data in 2022 and 2023. Source: *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase*

According to data released by Venusense Zhibai Lecture Hall, the average total cost of data leakage reached $4.45 million in 2023, hitting a record high. Compared with $4.35 million in the previous year, this figure increased by 2.3%. The German Digital Association Bitkom stated on September 1, 2023 that by 2023, the theft of IT equipment and data, as well as digital and industrial espionage and sabotage activities, had costed Germany 206 billion euros ($223.55 billion).

To sum up, protecting information security is of great significance for both individuals and enterprises. It can protect personal privacy, prevent identity theft and fraud, and protect financial security. Meanwhile, for enterprises, protecting information security is an important measure to maintain business reputation, protect intellectual property rights, comply with laws and regulations, and ensure business and operation continuity[15] [16].

2 Surveying the Status Quo of Information Security Awareness of Corporate Employees

2.1 Survey Overview

To know the status quo of information security awareness of people, esp. corporate employees (employees in enterprises), a survey was conducted among different people. A questionnaire was prepared on www.wjx.cn, and a survey was launched via WeChat and QQ groups from December 13, 2024 to December 14, 2024. 69 people of different background participated in the survey. They were expected to give their opinions (Strongly agree; Agree; No comment; Disagree; Strong disagree) on five statements concerning information security awareness as shown in the first column of Table 2.

The participants are aged from less than 18 years old to more than 60 years old: mostly young professionals (30 people: 25~44 years old), and next students (18 people: 18~24 years old) and middle-aged professionals (17 people: 45~59 years old). More than 60% (42 people) are female. More than 70% (49 people) have received college education, and 24.6% (17 people) are postgraduates. Nearly 70% (47 people) are literal arts majors, and slightly above 30% (22 people) are science and engineering majors. They are mostly management personnel (21 people) and clerks (20 people), and students, engineers and teachers are all about 10 people. Nearly half of them (34 people) come from enterprises, and nearly the same number of people come from the government (11 people) and public institutions (10 people).

2.2 Survey Results

This study is mostly concerned with information security awareness of people in different organizations, so we conducted cross-over (chi-square) analysis of information security awareness of people in different organizations. The results are shown in Table 2 below:

Table 2. A survey of information security awareness of people from different organizations: Cross-over (chi-square) analysis

Description: Five statements	Agree or not	Organization which I serve (%)				Total	$\chi 2$	*p*
		Enterprises	Public institutions	Government	Schools			
In the era of big data, there is a problem of information security.	Strongly agree	11(32.35)	2(20.00)	6(54.55)	4(28.57)	23(33.33)		
	Agree	22(64.71)	8(80.00)	5(45.45)	9(64.29)	44(63.77)	4.599	0.596
	No comment	1(2.94)	0(0.00)	0(0.00)	1(7.14)	2(2.90)		
It is important to protect our personal information	Strongly agree	10(29.41)	1(10.00)	6(54.55)	3(21.43)	20(28.99)		
	Agree	23(67.65)	9(90.00)	5(45.45)	10(71.43)	47(68.12)	7.036	0.318
	No comment	1(2.94)	0(0.00)	0(0.00)	1(7.14)	2(2.90)		
It is important to protect the information of the organization which I serve.	Strongly agree	7(20.59)	1(10.00)	6(54.55)	2(14.29)	16(23.19)		
	Agree	24(70.59)	9(90.00)	5(45.45)	11(78.57)	49(71.01)	9.423	0.151
	No comment	3(8.82)	0(0.00)	0(0.00)	1(7.14)	4(5.80)		
We should take measures to protect our personal information.	Strongly agree	11(32.35)	2(20.00)	6(54.55)	3(21.43)	22(31.88)		
	Agree	22(64.71)	8(80.00)	5(45.45)	11(78.57)	46(66.67)	5.053	0.537
	No comment	1(2.94)	0(0.00)	0(0.00)	0(0.00)	1(1.45)		
We should take measures to protect the information of the organization which I serve.	Strongly agree	6(17.65)	0(0.00)	6(54.55)	2(14.29)	14(20.29)		
	Agree	24(70.59)	10(100.00)	5(45.45)	11(78.57)	50(72.46)		
	No comment	4(11.76)	0(0.00)	0(0.00)	1(7.14)	5(7.25)	13.479	0.036*
Total		34	10	11	14	69		

* $p<0.05$ ** $p<0.01$

We made use of chi-square test (cross-over analysis) to find whether people from different organizations strongly agree, agree or disagree on the five statements concerning their awareness of information security. The table shows that people from different organizations have consistent opinions on the first four statements, for they have no remarkable differences (p=0.596, 0.318, 0.151 and 0.537 respectively; all >0.05). This indicates that people from different organizations mostly (more than 60%) agree that "In the era of big data, there is a problem of information security'; "It is important to protect our personal information"; "It is important to protect the information of the organization which I serve"; and "We should take measures to protect our personal information", except for more than half government employees strongly agree on all of the five statements.

Taking a closer look at statement 3 "It is important to protect the information of the organization which I serve", we can find that most corporate employees (more than 70%) have moderate opinion (Agree on statement 3) and three people (8.82%) show no concern (No comment on statement 3). Although their opinions are not remarkably different, but the difference is still clear ($\chi 2$=9.423; p=0.151>0.05). This means that the information security awareness of corporate employees for protecting the information of the organization which we serve is insufficient.

Opinions of people from different organizations on the last statement "We should take measures to protect the information of the organization which I serve", however, are remarkably different (p=0.036 <0.05). Thus, we can have a cross chart of the opinions of people from different organizations on Statement 5: "We should take measures to protect the information of the organization which I serve" as below:

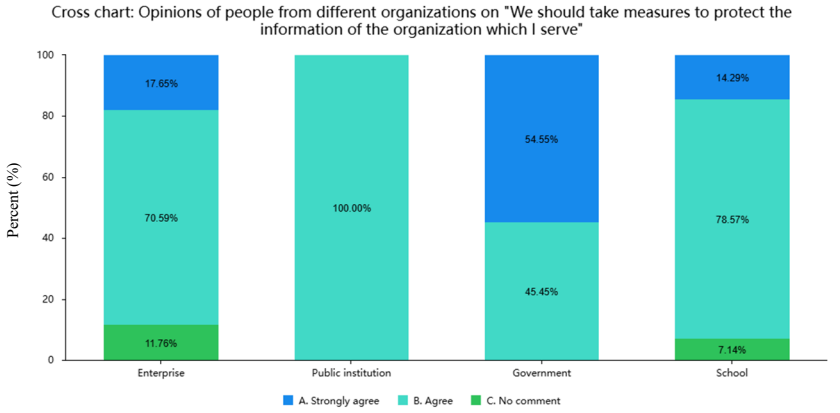

Fig. 2. Cross chart: Opinions of people from different organizations on "We should take measures to protect the information of the organization which I serve"

Fig. 2 indicates that only 17.65% corporate employees strongly agree on statement 5 (i.e.: We should take measures to protect the information of the organization which I serve). This is slightly more than people from schools who strongly agree(14.56%), and much less than government employees (54.55%). Most corporate employees (70.59%) show moderate concern (Agree on statement 5), while less than half (45.45%) government employees have moderate concern. This means that corporate employees do not have strong opinion on enhancing their information security awareness for the organizations which they serve. What's more, there are as many as 11.76% of corporate employees show no concern (No comment of the statement) on statement 5, while there are no government employees expressing no concern. This further indicate their insufficient awareness on protecting the information security for the organizations which they serve[17] [18] [19].

Based on the above analysis of different people's opinions on statement 3 and statement 5, we are in the position to conclude that compared with government employees who mostly hold strong opinion on protecting the information security of the organization which they serve and thus have strong information security awareness, corporate employees hold relatively moderate opinion and insufficient awareness. This means that there is much room for improvement of their awareness of information security for the organization which they serve, so it is of great significance to enhance the information security awareness of corporate employees.

2.3 Significance of Enhancing the Information Security Awareness of Corporate Employees in the Era of Big Data

Apparently, it is very significant to enhance the information security awareness of corporate employees in the era of big data, as is shown in the following aspects:

(1) National security: Industrial enterprises involve the core interests and security of the country. Some employees possess important national secrets and core technologies. Enhancing their information security awareness can effectively reduce the risk of leakage of confidential information and protect the security and interests of the country.
(2) Corporate competitiveness: In the era of big data, information has become an important asset for enterprises. Improving the information security awareness of corporate employees can protect the enterprise's commercial secrets, research and development achievements, and intellectual property rights, prevent theft and attacks by competitors, and enhance the enterprise's competitiveness in the market.
(3) Personal career development: For individual employees, having a relatively high level of information security awareness is a necessary condition for career development. It can enhance employees' sense of responsibility and prudence in their work, protect the security of personal information and work achievements, and avoid career risks caused by information leakage.
(4) Legal compliance: With continuous improvement of laws and regulations related to information security, both enterprises and individuals need to abide by relevant regulations. Enhancing their information security awareness helps corporate employees understand and comply with relevant laws and regulations and avoid illegal acts and legal liabilities.
(5) Social responsibility: Industrial enterprises bear important social responsibilities, and protecting the security of the country and the people is their primary task. Enhancing the information security awareness of corporate employees helps ensure the safe operation of enterprises and maintain social stability and security.

To sum up, enhancing the information security awareness of corporate employees in the era of big data is of great significance for protecting national security, enterprise competitiveness, personal career development, legal compliance, and social responsibility. It is quite urgent to improve corporate employees' information security awareness and prevention capabilities and ensure the security and sustainable development of enterprises in the era of big data.

3 Recommendations for Enhancing Information Security Awareness

Apparently, in the era of big data, it is of great importance to enhance the information security awareness of corporate employees. What should we do to strengthen their information security awareness then? The following are some recommendations for enhancing the information security awareness of corporate employees:

(1) Carry out security training and education

We need to regularly organize online and offline security training courses for corporate employees, covering relevant contents such as network security, data protection, and password security. For example, we can conduct security and confidentiality education and training, network security knowledge training, news publicity confidentiality knowledge training, publicity and implementation training of rules and regulations, and national defense and industry confidentiality knowledge training. In these programs, we can provide an online learning platform to help corporate employees to learn security-related knowledge and skills. We can also hold security seminars or lectures and invite security experts to share experiences and best practices, and provide case analyses to let employees understand actual security incidents and how to avoid similar risks.

(2) Give priority to data privacy and protection

According to security management systems and operating procedures, we determine the person in charge of network security and adopt technical measures to prevent cyber attacks, network intrusions and other behaviors that endanger network security. For example, we can conduct data privacy awareness training to educate corporate employees on how to correctly handle sensitive data. We may classify, back up and encrypt important data, and clearly define the sensitivity and importance of various types of data so as to adopt different protection measures. Data backup can ensure that data can be restored in a timely manner in case of data loss or damage, while data encryption can prevent data from being illegally accessed or tampered with. We need to formulate data classification policies and clearly define the protection requirements for different levels of data, and implement data encryption measures to ensure the security of sensitive data during transmission and storage.

(3) Strengthen the publicity of security and confidentiality awareness

There is a lot for us to do to strengthen the publicity of security and confidentiality awareness. For example, we can regularly send security awareness emails or notices to remind corporate employees of common security risks and preventive measures. We can put up security posters or slogans to remind employees of safety. We may hold security awareness publicity activities, set up Security Week or Security Day to strengthen the popularization of security knowledge. For example, June of each year is the National Work Safety Month. Each company and organization can combine its own characteristics, research and formulate activity themes and activity plans, and carry out various safety publicity and education activities with rich activities such as safety quizzes as the carriers, create a strong public opinion atmosphere for safety, build a consensus on safe development, effectively improve everyone's safety awareness, and form a good atmosphere where “everyone is concerned about safety and safety concerns everyone”.

(4) Hold security-related competitions

We can hold various security-related competitions, improving everyone's knowledge reserve and enhancing everyone's understanding of security. For example, we can organize security knowledge competitions to stimulate the enthusiasm of corporate employees to learn security technologies through competitions. We may hold vulnerability

discovery competitions to encourage employees to discover and report security vulnerabilities in the security system. We may carry out activities to collect security micro-videos, comics and aphorisms to create an interesting learning atmosphere. We can also hold security and confidentiality quiz activities to promote everyone to sort out their own security and confidentiality responsibilities in their positions.

(5) Provide security tools and resources

Network security tools are essential for protecting computers, networks and information systems from cyber attacks and malware. To prevent cyber attacks, data leaks and information security threats, the latest security tools such as antivirus software, firewalls, encryption tools, security design tools, vulnerability scanning tools, intrusion detection systems, intrusion prevention systems should be continuously provided for corporate employees, and guide them to use them correctly. Firewalls can not only monitor and block intrusion attempts but also prevent the spread of malware and viruses. Antivirus software can scan and eliminate viruses, malware and spyware in computers. Since it updates the virus database regularly, it can maintain the ability to identify and protect against the latest threats. Encryption tools convert data into encrypted text by using cryptographic algorithms to ensure that only authorized personnel can decrypt and access this data. We can also provide a security resource library, including security documents, guidelines, and standards, to facilitate employees' consultation and learning.

(6) Establish and improve the security culture

The management should lead by example, emphasize the importance of security, encourage corporate employees to actively participate in security work, and regularly study the important statements of superiors on security and confidentiality. For example, we can strengthen security awareness and regularly watch warning education promotional videos on security and confidentiality. We can set up a security reward mechanism to commend and reward employees who perform well in security aspects, improve employees' attention to security, and prompt employees to comply with relevant systems. We may also advocate security sharing and communication among corporate employees to promote the dissemination and popularization of security awareness.

(7) Conduct regular security audits and drills

We may regularly conduct security audits on relevant software and hardware, check and evaluate the security of systems, networks and data, identify risks and insecure factors in work, and look for better solutions. We should continuously improve the security level, organize security drills, simulate the response to emergency incidents, and improve the emergency response ability and security awareness of employees. We can establish a smooth feedback mechanism and communication channels so that corporate employees can report in a timely manner and put forward improvement recommendations after discovering security risks. We can also carry out self-inspection and mutual inspection of security and confidentiality to promote corporate employees to understand the operating procedures of their positions and conduct security and confidentiality entrance examinations for future employees.

(8) Establish and improve the security and confidentiality systems

In accordance with the requirements of laws and regulations and in combination with the actual status quo of each company and organization, we may gradually establish

and improve various security and confidentiality management systems. For example, we can establish the *Corporate Information Security Management Rules for Employees* and it will serve as the criteria and bases for carrying out daily security and confidentiality management. Through the implementation of the systems, we will realize the whole-process security and confidentiality management of personnel, equipment, materials and environment.

Applying the above methods in a comprehensive manner, we can effectively improve the information security awareness of corporate employees, reducing information security risks, and protecting the important information assets of enterprises, so as to better cope with the security challenges in the era of big data. Meanwhile, enterprises should also continuously adapt to the new development of security issues and continuously improve and ensure relevant security measures.

4 Conclusion

This paper analyzes the characteristics of the era of big data and the development of information security, reviews relevant literature and conducts a questionnaire survey to stress the importance of enterprises' efforts to ensure information security. Based on the status quo of information security matter, we put forward some recommendations for improving and enhancing the information security awareness of corporate employees. The following conclusions can be drawn in this paper.

(1) In the era of big data, information security issues involve everyone around us. Once information security is compromised, it will bring huge losses to both enterprises and individuals.

(2) Currently, given that considerable number of corporate employees show moderate concern or no concern of information security for the enterprise which they serve, it is urgent for us to raise the information security awareness of corporate employees. This is of great significance for the country, enterprises, and individual employees.

(3) Eight recommendations for improving the information security awareness of corporate employees are put forward. We can raise the information security awareness of employees from various aspects such as training and education, formulating clear policies and guidelines, and providing regular communication and reminders.

Given that there is only a few researches addressing the issue of information security awareness of corporate employees, we hope more relevant research efforts can be made. It would be of even higher value for them to survey whether corporate employees have taken actions to protect the information security of the enterprise which they serve before addressing how to enhance their awareness.

Acknowledgments

This article has been finished as funded by Ministry of Education Project for Industry-University Cooperation and Collaborative Education: GenAI and CAT-Based Development of Translation Practice Base (241001339144012).

References

1. Tian Qiu. Discussion on the Information Security Issues of Computer Networks in the Era of Big Data [J]. Office Automation, 2024, 29(04): 36-38+8.
2. Zhang Yuxia. Research on the Current Situation and Countermeasures of Network Information Security in the Era of Big Data [J]. Software, 2023, 44(12): 184-186.
3. Ma Yaping, Fan Jingyang. Investigation and Research on the Personal Information Security Awareness of College Students in the Era of Big Data [J]. Science & Technology Information, 2022, 20(05): 238-241.
4. Gao Jiameng. Research on the Construction of Enterprise Information Security Capability and Its Key Influencing Factors in the Industrial Internet Environment [D]. Qingdao University, 2023.
5. Bi Yunxing. Corporate Information Security and Protection Strategies in the Era of Big Data [J]. Information Recording Materials, 2021, 22(07): 45-46.
6. Wu Chen. On the New Characteristics and New Requirements of Information Security in the Era of Big Data [J]. Digital World, 2018.
7. Zhang Yunzhuang, Liu Jifeng. Opportunities and Challenges of Information Security in the Era of Big Data: Taking Open Information Intelligence as an Example [J]. National Defense Science & Technology, 2013(2): 4.
8. Li Jianke. On the New Characteristics and New Requirements of Information Security in the Era of Big Data [J]. Technology and Economic Guide, 2017(27): 1.
9. Liu Jihong, Wang Jiahui, He Yifeng. Analysis of Information Security Risk Prevention in the Era of Big Data [J]. Computer Knowledge and Technology, 2023, 19(21): 79-80.
10. Liu Yahui, Zhang Tieying, Jin Xiaolong, et al. Personal Privacy Protection in the Era of Big Data [J]. Journal of Computer Research and Development, 2015.
11. Shen Changxiang, Zhang Huanguo, Feng Dengguo, et al. An Overview of Information Security [J]. Science in China (Series E: Information Sciences), 2007 (2).
12. Feng Dengguo, Zhang Yang, Zhang Yuqing. An Overview of Information Security Risk Assessment [J]. Journal on Communications, 2004, 25(7): 10-18.
13. Wang Shiwei. On Information Security, Cybersecurity and Cyberspace Security [J]. Social Sciences Academic Press, 2015.
14. Stuart E. Madnick. The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase.2024-12-15.https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf
15. Fan Hong, Feng Dengguo, Wu Yafei. Information Security Risk Assessment Methods and Applications [M]. Tsinghua University Press, 2006.
16. Yang Yixian, Niu Xinxin, Li Mingxuan. Network Information Security and Confidentiality (Second Edition) [M]. Beijing University of Posts and Telecommunications Press, 2001.
17. The SPSSAU project (2024). SPSSAU. (Version 24.0) [Online Application Software]. Retrieved from https://www.spssau.com.
18. Zhou Jun, Ma Shipeng. SPSSAU Research Data Analysis Methods and Application. (First Edition) [M]. Publishing House of Electronics Industry, 2024.
19. Hosmane B S. Improved likelihood ratio tests and pearson chi-square tests for independence in two dimensional contingency tables[J]. Communications in Statistics, 1986, 15(6):1875-1888.