Exploration of Factors Influencing Computer Network Information Security and Prevention Strategies in Colleges and Universities

Jing Liu

Library and Information Center, Chongqing Medical and Pharmaceutical College, Chongqing, China

joanna_lj01@163.com

Abstract. With the swift advancement of computer network technology, society is growing more reliant on the network for daily life and operations. As such, computer network security has emerged as an increasingly significant concern. This article embarks by examining four areas - technology, management, laws and regulations, and human-induced factors - shaping the information security landscape in university networks. The discussion further delves into the suitable defensive strategies, concluding with an analysis of the challenges posed by network information security. A tactical utilization of these preventive measures, therefore, can effectively reinforce the information security within university networks, thereby safeguarding the regular academic and administrative proceedings within these institutions.

Keywords: Computer; University Network Security; Influencing Factors; Preventive Measures

1 Introduction

With the rapid development and popularization of Internet technology, computer networks have penetrated into all aspects of people's lives, from work, learning to entertainment, social networking, almost everywhere. However, with the widespread application of the internet, network security issues have become increasingly prominent and have become a global challenge. The network attack against Estonia's Internet infrastructure in 2007, caused the system interruption, rendering the key information infrastructure of many countries unusable. In 2010, the use of the Stuxnet worm virus infected systems in Iran’s uranium enrichment facility at Natanz [1]. The Prism program (PRISM) was exposed in 2013, covering a wide range of countries, organizations, and individuals.

Computer network information security is a crucial issue that strikes the core of national security, national economy, social stability, and the well-being of the public, as it involves multiple levels such as personal privacy protection, enterprise data

Y. Kuang et al. (eds.), *Proceedings of the 2024 5th International Conference on Education, Knowledge and Information Management (ICEKIM 2024)*, Atlantis Highlights in Computer Sciences 22,
https://doi.org/10.2991/978-94-6463-502-7_62

security, national security, and is related to the vital interests of every individual and social stability [2].

Many scholars research on network security from different perspectives. Aslan, Ö. et al. extensively explained the main reasons for cyber attacks in their paper. They reviewed the most recent attacks, attack patterns, and detection techniques. At last, they discussed contemporary technical and nontechnical solutions for recognizing attacks in advance [3]. Kizza, J.M. [4] mentioned that computer network security is made up of three principles: prevention, detection, and response. They focused on discussing the relevance and significance of intrusion detection and prevention. Bayi Xu, Lei Sun et al. also conducted research on intrusion detection and recognition. They presented a novel intrusion detection system consisting of a data preprocessing stage and a deep learning model for accurately identifying network attacks [5]. Kongduo Xing summarized and analyzed the challenges related to computer network information security processing, and proposed some suggestions for the application strategies of big data technology in solving the computer network security problems [6]. By the research on steganography, Shahina Anwarul, Sunil, et al. presented an efficient hybrid security model that provides multifold security assurance [7].

Dany Patrick, Kenfack Bavoua et al. analyzed the importance of enhancing the security of information systems. They set up a hardening procedure in accordance with international security standards for servers, routers and switches and also designed and produced a functional application [8].

Lewis Golightly, Paolo Modesti et al. [9] reviewed the current state-of-the-art Access Control solutions used by organizations as a cybersecurity strategy for user and data authorization. They discussed the business adoption strategies for Access Control and how the technology can be integrated into a cybersecurity and network architecture strategy. Z. S. Younus, M. Alanezi surveyed network security monitoring techniques, encompassing their functionality, contents, and tools like antivirus, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and SIEM. They introduced SIEM as the most common and advanced security tool, highlighting its functionalities and capabilities [10].

AI and blockchain technology are also important areas for current research on network information security. Rajagopal, M., Ramkumar, S. and Sarvesh Kumar, Upasana Gupta et al. recognize the impact of artificial intelligence on network information security. Rajagopal, M., Ramkumar, S. [11] explored the methods of introducing artificial intelligence into IT service management (ITSM) to reduce the impact of information security threats and they also studied how to use artificial intelligence (AI) to improve IT security through prevention, detection, and learning from incidents. In the paper of Sarvesh Kumar, Upasana Gupta et al., they demonstrated the potential of artificial intelligence to effectively predict, identify, and preemptively take a proactive stance on digital security, enabling organizations to take a proactive approach. They also emphasized the need for continuous human supervision and intervention to ensure that cybersecurity measures are proportionate and effective [12].

Hephzibah Miriam, D. Doreen et al. and Md.Shohidul Islam Md.Arafatur et al. explored the blockchain technology. Hephzibah Miriam, D. Doreen et al. offered a

Lionized Golden Eagle based Homomorphic Elapid Security (LGE-HES) algorithm for the cybersecurity of blockchain in healthcare networks [13]. Md.Shohidul, Islam, Md.Arafatur et al. conducted a comprehensive survey on cybersecurity enhancement using blockchain in the heterogeneous network and proposed a blockchain based heterogeneous network framework with cybersecurity [14].

Most of the research mainly focuses on technical aspects such as devices, big data, and intrusion detection, and there is relatively little research on the factors and strategies affecting computer network security in universities. This article embarks by examining four areas - technology, management, laws and regulations, and human-induced factors - shaping the information security landscape in university networks. The discussion further delves into the suitable defensive strategies, concluding with an analysis of the challenges posed by network information security, which has certain reference significance for the protection of network information security in universities.

2 Analyzing the Factors that Impact University Computer Network Information Security

The widespread adoption of the Internet coupled with the swift progression of information technology poses new challenges to the preservation of information security within university computer networks. The critical dimension of information security in universities encompasses three key aspects - the integrity, confidentiality, and availability of data. Any compromise in these areas can potentially instigate severe repercussions.

2.1 Technical Factors

The burgeoning development of internet technology has propelled the network information security issues of universities into the limelight. Among all the impacting factors, the technical elements are paramount, encompassing vulnerabilities in network protocols, flaws in encryption technologies, and malicious software attacks.

As the keystone of computer network communication, the security of network protocols directs the stability and safety of the whole network. However, the current ubiquitous vulnerabilities in network protocols, like IP fragmentation attacks and ARP spoofing, offer loopholes for network attackers. This may result in network communications being intercepted, altered or fabricated, which heavily jeopardize network information security. Despite encryption technology being used widely to protect network information security, it has potential downsides. For instance, mismanagement of cryptographic keys and faults in encryption algorithms can lead to data encryption being breached, exposing sensitive information. Therefore, it's critically important to enhance the research and application of encryption techniques, and improve key management mechanisms for safeguarding network security. Malicious software attacks serve as a significant threat to network information security as well. Such malevolent programs can inflict considerable damage to network security by corrupting users’ computers, stealing their private information, or ruining system files. As the methods of malicious software attacks evolve constantly, the difficulty of defense is also escalating, posing great challenges to network information security [15].

2.2 Managerial Factors

A comprehensive security management system is the bedrock of maintaining computer network security. Yet practically, certain universities' security management protocols have apparent defects, such as ambiguous security policies, disorderly distribution of privileges, and inadequate auditing and tracking mechanisms. These issues render the network system more vulnerable to external assaults and internal misuse, thereby increasing the risk of data leakage and system crashes. Additionally, the lack of security awareness among the universities' staff and students is an important factor that can't be brushed over. Their daily conduct and decisions can directly affect the safety of network systems. Unfortunately, many teachers and students have insufficient recognition of the importance of computer network security and lack the needed security knowledge. They might casually click on unknown links, use simple passwords, and share sensitive information with irrelevant individuals. These negligent behaviors could leave loopholes for attackers to exploit, which may lead to the system being assaulted. Lastly, an uneven level of competency among the administrative personnel also poses a challenge to network security. With the high-speed growth of computer network technology, the demand for network security talent is rising rapidly. But a notable issue is the inconsistent competence among the information personnel in various universities. On the one hand, a lack of crucial network security knowledge and skills can leave them floundering against intricate network threats. On the other hand, a lack of proper job opportunities have led to a loss of experienced security experts, further aggravating the talent shortage issue. The uneven competencies of university information personnel not only weaken the security defenses of the network system but also hinder the overall growth of the organization [16].

2.3 Factors of Legislation, Regulations, and Policies

In the intricate terrain of computer network information security, the legal, regulatory, and policy elements play an indispensable role. However, these factors are faced with unprecedented challenges due to the ongoing innovation of cyber-attack methods, changes in international political and economic circumstances, and the time lag in adaptation of existing laws and regulations. First off, the continuous evolution of cyber-attack methods causes the existing legislation and regulations to fall behind their development. Cybercriminals utilize sophisticated techniques to launch attacks, such as deep fakes and exploiting zero-day vulnerabilities. These damaging attacks often become known and regulated by the law only after they've dealt significant damage. Hence, laws and regulations require constant updates and enhancements to counter these emergent network threats. Secondly, the alterations in the global political and economic landscapes have a profound impact on computer network information security. With increasing globalization and rising international trade, the internet connections among different countries are tightening, and the transnational nature of cyber-attacks is becoming more apparent. Yet, due to the variations in laws and regulations, cultural backgrounds, and technical standards, collaboration and coordination on international levels in terms of network security are fraught with challenges. Additionally, political tensions on an international scale could potentially cultivate confrontations and conflicts in cyberspace, adding to the gravity of network security risks. Lastly, the delay in legislative amendments and regulatory adjustments poses another significant challenge to the network information security in universities. Although numerous governments are making concerted efforts to introduce and amend relevant laws and regulations, rapid technological advancements and ever-changing network environments often render existing laws ineffective in timely addressing emerging issues and challenges. Also, the sluggish law-making process in some nations regarding cyber security further weakens their capability to tackle network threats efficiently [17].

2.4 Human Factors

Human factors encompass the cognizance, attitudes, and behaviors of users. Many instances of network breaches have been facilitated by the lack of security awareness or operating errors from teachers and students. Phishing emails and malicious software, for instance, typically ensnare users into clicking on links or downloading attachments. If faculty and students were more vigilant in not readily trusting unknown emails or links, such attacks are likely to fail. The internal threats within universities also fall under the human factor category. There could be teachers or students who may compromise critical data or sabotage network security due to dissatisfaction, greed, or other motivations. To avert such circumstances, a holistic internal control mechanism is indispensable in universities, fostering faculty and student education and training as well as elevating their professional ethics and security consciousness. Furthermore, human elements also touch upon the professional integrity and sense of duty of the network security managers. They need to remain equipped with a breadth of professional knowledge and skills to detect and respond timely to any security threats. Synchronously, these administrators should hold themselves accountable and uphold their professional commitment, staying vigilant to network security changes, and ensuring the stability and integrity of the network regime [18].

3 Strategies for Computer Network Information Security Prevention

3.1 Technical Prevention Strategies

In this digital era, the computer network has emerged as a crucial element in the process of information construction in colleges and universities. To shield network resources from harmful attacks and unwarranted data leaks, it is essential to formulate and implement an array of effective information security measures. A firewall, serving as one of the core facilities for network security, plays an instrumental role in controlling and supervising the data flow in the network as well as deterring unauthorized access or attacks. Firewalls can be sorted into two types: hardware and software firewalls, which are respectively installed at the gateways of the network and within the operating system, achieving their security functions through dedicated software. The essence of firewalls lies in the configuration of safety policies which outline the data permitted to enter or exit the network and how the data should be managed. Typical security measures encompass control over the access to particular IP addresses, ports, and protocols; and operations like filtering, monitoring, and logging of network traffic. With appropriately configured security strategies, firewalls can efficaciously obstruct malicious traffic and assaults, thereby securing network resources.

Intrusion Detection and Prevention Systems (IDS/IPS) are security apparatus specifically purposed for monitoring and analyzing network traffic, capable of detecting and blocking malicious behaviors and attacks in real time. IDS primarily oversees the network traffic and log files, identifies unusual behaviors and potential risks, and triggers alarms to administrators. IPS, upon detecting any malevolent activities, automatically initiates steps to counter the attacks, for instance, blocking the malicious traffic or shutting down the affected ports. The crux of IDS/IPS technology rests on its detection algorithm and response mechanism. The detection algorithm, based on predefined rules or machine learning models, analyzes and identifies data to uncover malicious behaviors and attacks. The response mechanism, on the other hand, employs suitable measures based on the detection outcome, aiming to alleviate or prevent the detrimental influence of the attacks. By integrating IDS/IPS technology, network threats can be promptly identified and counteracted, thereby safeguarding the integrity and availability of network resources [19].

3.2 Management Prevention Strategies

In the age of information overload, faculty and students alike are prone to underestimating the significance of network security, falsely believing that robust technology alone is sufficient to tackle all challenges. However, the fact is, many security breaches occur due to human errors or oversight. As a result, it's essential to heighten the safety awareness among all faculty and students through routine safety training, awareness campaigns, and education, thereby familiarising them with the importance of network security and imparting them with skills needed to safeguard their information in daily routines. Moreover, refining the management structure remains a critical step towards ensuring network information security. A robust management system delineates clear administrative duties and permissions for all staff at various levels, which consequently regulates behaviors related to network usage and minimizes security risks. For example, higher education institutions implement rigid password management systems, prompting faculty and students to update their passwords regularly and utilize sophisticated password combinations. Concurrently, an access control system needs to be established, ensuring sensitive information is available only to authorized personnel. Additionally, data backup and recovery systems are to be established to prevent potential data loss or corruption. Lastly, enhancing operation and maintenance standards serves as a safeguard for network information security in universities. Operation and maintenance team members are pivotal to preserving network security, as their expertise and sense of responsibility directly contribute to the network's safety. Therefore, recurrent training and evaluations for these personnel are necessary to elevate their professional competency; meanwhile, establishing comprehensive operation and maintenance procedures and emergency response plans ensure swift and effective response and resolution in the event of security incidents.

3.3 Legal, Regulatory and Policy Prevention Strategies

Countries should endeavor to devise and refine a comprehensive system of laws and regulations encompassing all facets of network information security, covering aspects like cybercrime, data protection, and individual privacy. Besides legislative measures, the government should also ramp up investments in the domain of network information security, promoting colleges and universities to develop cutting-edge technologies, thereby fostering innovation and upgradation in the industry. Concurrently, a robust policy-support mechanism needs to be constructed, offering policy measures including financial assistance to universities, with the aim of slashing their operational costs. Such initiatives would be instrumental in enticing more universities and corporations to invest in the field of network information security, stimulating the speedy advancement of the industry. Furthermore, the government should reinforce policy directives to encourage universities to shoulder network information security responsibilities. This could be achieved by setting industry standards and conducting safety evaluations, guiding the industry towards establishing a comprehensive security management structure and technical protection measures, thereby increasing their defensive capabilities against security threats. Intensifying surveillance and checks on universities are crucial to secure the effective implementation of security management measures. This combined approach involving the government, universities, and businesses in network information security will help establish a robust security assurance system, contributing significantly towards a healthy growth of cyberspace [20].

3.4 Human Prevention Strategies

In the sphere of network information security, human factors often pose unpredictable and uncontrollable challenges. However, a series of targeted manual prevention strategies can significantly reduce security risks and safeguard critical data of the organization from infringement. On the one hand, it's essential to strengthen the training and management of internal personnel in universities. Regular internal personnel training sessions, aimed at enhancing the safety consciousness of faculty and students, teaching them the skills to recognize and handle various security threats could ensure adherence to the organization's security policies and regulations. On the other hand, the strategy should aim to increase the costs associated with external attacks, as external personnel often constitute one of the primary threats to network information security, potentially infiltrating the university's network system through varied means. Specific measures in this regard may include fortifying identity verification mechanisms, limiting data access rights, deploying intrusion detection systems, providing regular updates to security patches, and establishing security incident response protocols [21].

Through the implementation of the aforementioned prevention strategies, universities can substantially enhance their defensive capabilities against network information security threats, thereby reducing their vulnerability to attacks. Fostering a thorough security culture within the university would ensure that every faculty member and student understands the significance of network information security, thereby collectively contributing to maintaining the organization's stability and security.

4 Case Study

4.1 Prominent Cybersecurity Incidents

In an era marked by rapid technological advancement, computer networks have permeated every aspect of our lives - from social networking and financial transactions, to workspace management and e-learning. The importance of networks is, thus, unquestionable. However, along with its widespread use and convenience, the network brings with it an array of security challenges. Numerous cybersecurity incidents at educational institutions in recent years reflect this. These incidents have led to substantial economic and social repercussions for individuals, institutions, and even at a national level （Figure1 Network threats）.

Ransomware is a kind of malicious software that encrypts a user's files, holding them 'ransom' until a sum is paid for the decryption key. These attacks have become increasingly common in recent years. Perpetrators often utilize system vulnerabilities or phishing emails to spread ransomware, resulting in substantial data and financial loss for victims. The ‘WannaCry’ ransomware attack of 2017 serves as a case in point. The attack affected hundreds of thousands of computers across the world, disrupting online teaching in many institutions.

Data breaches occur when sensitive data is unauthorizedly or inadvertently disclosed to the public or unlawful actors. These incidents often involve sensitive personal information, trade secrets, or classified government data. Causes of data leaks could range from insider leaks, external cyber attacks, to system loopholes. For instance, the Facebook data breach incident of 2018 involved the unauthorized collection and subsequent misuse of personal data of millions of users for targeted advertising.

Phishing, a common form of online fraud involves criminals duping victims into divulging sensitive details like account credentials or credit card numbers by posing as official websites or through misleading emails. The stolen data is then employed for illicit activities such as unauthorized funds transfer and credit card fraud. The 'Emotet' banking Trojan incident in 2019 illustrates this. By resorting to phishing, the Trojan infected thousands of computers globally, leading to a substantial theft of banking information.

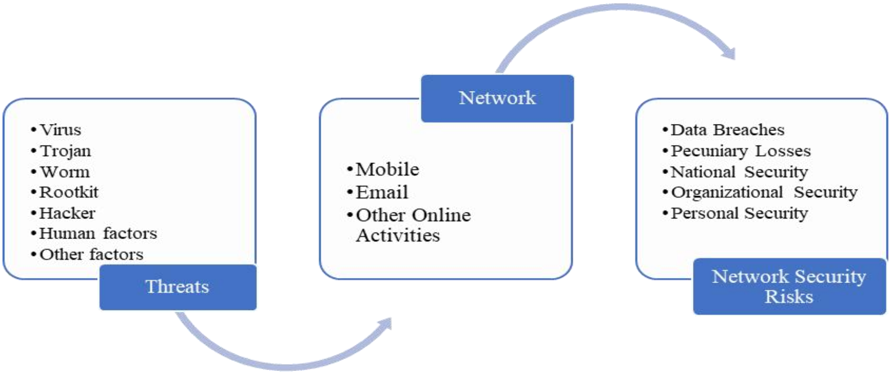

Fig. 1. Network Threats

4.2 Implementation of Countermeasures in Practice

Amid a progressively challenging cybersecurity landscape, it is imperative for educational institutions to adopt varied counterproductive measures to safeguard their information security. Technical remedial strategies form the crux of cybersecurity protection, encompassing common technological means such as firewalls, intrusion detection systems, and antivirus software. For instance, to deter ransomware attacks, safety applications can be used for performing regular comprehensive scans of computer systems. Timely system and software updates help in avoiding known vulnerability exploits. Regular backup of essential files aids quick data recovery in the wake of a ransomware attack.

Management remedial strategies play a crucial role in enhancing network security. Institutions need to introduce and streamline network security management systems and cultivate a culture of cybersecurity awareness through teacher-student training programs. For instance, to thwart phishing attacks, educational institutes may organize regular trainings to equip teachers and students with skills to identify phishing emails, refrain from clicking unfamiliar links, and discourage careless disclosure of personal information.

Legal and policy countermeasures substantially ensure network security. The government has legislated multiple cybersecurity laws and regulations, including the 'Cybersecurity Law' and 'Personal Information Protection Law.' These regulations aim to strengthen cyber surveillance and safeguard citizens’ legitimate rights and interests. In the face of cyber incidents, universities should adhere to these regulations for resolution, promptly report to the relevant authorities, and thereby mitigate damages.

As part of human remedial measures, users themselves need to nurture good security habits while using the network. This includes setting complex passwords, regularly changing passwords, avoiding unsafe network connections in public areas, and not using identical passwords across multiple websites. Furthermore, users should be vigilant in discerning online information and steer clear of deceptive content [22].

5 Anticipated Challenges in Future Developments

Going forwards, the domain of contemporary computation and data processing is set to undergo extraordinary transformations. However, these evolving technologies concurrently present formidable security challenges to university IT systems. Centralized data storage and processing heighten the risk of data breaches and corruption, whereas big data analytics could potentially divulge personal privacy details. The ubiquity of Internet of Things (IoT) devices and mobile technology broadens the scope of potential cyber-attack targets. Vulnerabilities in these devices can be exploited by hackers, thereby enhancing their susceptibility to breaches. The continued progression of AI and blockchain technologies promises innovative applications across various fields, yet they pose inherent challenges associated with data security, model integrity, and counteracting aggressive cyber-attacks.

To mitigate these challenges, universities need to contemporize their cybersecurity protocols and bolster safety provisions across technology and devices. Institutes need to incorporate a gamut of protective measures including identity verification, access control, data encryption, and regular security audits. Periodic firmware and software updates need to be undertaken to mend security gaps, thereby ensuring overall system reliability and protection.

6 Conclusions

In a nutshell, cybersecurity defence is a systematic paradigm. To effectively secure IT systems, universities need to employ a multifaceted approach, amalgamating various technological and administrative means. With network technologies consistently advancing, the face of cybersecurity threats is constantly evolving. Universities need to stay alert, continuously updating and refining their cybersecurity strategies to provide a secure and reliable network environment conducive to teaching and learning.

References

1. Ünal Tatar, Orhan Çalık, Minhac Çelik and Bilge Karabacak， A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. Ünal Tatar et al，211-218.
2. Tianqing He, Factors affecting computer network information security and preventive measures (in Chinese). Science and Information Technology, 2023 (1): 31-33.
3. Aslan, Ö.; Aktu˘ g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. https:// doi.org/10.3390/electronics12061333
4. Kizza, J.M. (2024). System Intrusion Detection and Prevention. In: Guide to Computer Network Security. Texts in Computer Science. Springer, Cham. 295–323. https://doi.org/10.1007/978-3-031-47549-8_13.
5. Bayi Xu, Lei Sun et al. Strengthening Network Security: Deep Learning Models for Intrusion Detection with Optimized Feature Subset and Effective Imbalance Handling. Computers, Materials & Continua, 2024(2):1995-2022.
6. Kongduo Xing, A Practical Study of Big Data Technology in Computer Network Information Security Processing. Journal of Electronic Research and Application, 2023(6):36-41.
7. Shahina Anwarul, Sunil et al. Hybrid Dynamic Optimization for Multilevel Security System in Disseminating Confidential Information. Computer Systems Science & Engineering, 2023(12):3145-3163.
8. Dany Patrick, Kenfack Bavoua et al.Strengthening the Security of Supervised Networks by Automating Hardening Mechanisms. Journal of Computer and Communications, 2023(5):108-136.
9. Lewis Golightly, Paolo Modesti, Rémi Garcia, Victor Chang, Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. Cyber Security and Applications, 2023(1). https://doi.org/10.1016/j.csa.2023.100015.
10. Z. S. Younus, M. Alanezi, A Survey on Network Security Monitoring: Tools and Functionalities. Mustansiriyah Journal of Pure and Applied Sciences, 2023,1(2) :55-86.
11. Rajagopal, M., Ramkumar, S. (2023). Adopting Artificial Intelligence in ITIL for Information Security Management—Way Forward in Industry 4.0. Artificial Intelligence and Cyber Security in Industry 4.0. Advanced Technologies and Societal Change. Springer, Singapore. 113-132. https://doi.org/10.1007/978-981-99-2115-7_5.
12. Sarvesh Kumar, Upasana Gupta et al. Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. Journal of Computers. Mechanical and Management, 2023,2(3):31-24. DOI: 10.57159/gadl.jcmm.2.3.23064.
13. Hephzibah Miriam, D. Doreen et al. Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. Intelligent Automation & Soft Computing, 2023,35(2): 1889
14. Md.Shohidul Islam Md.Arafatur et al. Blockchain-Enabled Cybersecurity Provision for Scalable Heterogeneous Network: A Comprehensive Survey. Computer Modeling in Engineering & Sciences, 2024(1):43-123
15. Yuting Tang, Research on the Factors Influencing Computer Network Information Security and Preventive Measures (in Chinese). Modern Industrial Economy and

Information Technology, 2023,13 (2): 68-70. DOI: 10.16525/j.cnki.14-1362/n.2023.02.025.

16. Song Wang; Ying Zhao, A Brief Analysis of the Factors Influencing Computer Network Information Security and Preventive Strategies (in Chinese). Electronic Components and Information Technology, 2022, 6 (10): 213-216. DOI: 10.19772/j.cnki.2096-4455.2022.10.052.
17. Guoming Cheng, Factors affecting computer network information security and preventive measures (in Chinese). China Science and Technology Information, 2021 (18): 59-60. DOI: 10.3969/j.issn.1001-8972.2021.18.015.
18. Ruiqi Zhang, Factors affecting computer network information security and preventive measures (in Chinese). China Foreign Exchange, 2021, 28 (10): 60].
19. Jingjing Zhang, Factors affecting computer network information security and preventive measures (in Chinese). Shantianxia, 2020 (16): 659-660
20. Xintao Yang, Factors affecting computer network information security and preventive measures (in Chinese). Network Security Technology and Applications, 2022 (5): 169-170. DOI: 10.3969/j.issn.1009-6833.2022.05.100.
21. Shanshan Yuan, Research on Factors Influencing Computer Network Information Security and Preventive Measures (in Chinese). Information recording materials, 2022, 23 (1): 86-88. DOI：10.16009/j.cnki.cn13-1295/tq.2022.01.007.
22. Wenxin He, Research on the Factors Influencing Computer Network Information Security and Preventive Measures (in Chinese). Outdoor equipment, 2023 (10): 460-462. DOI: 10.12277/j.issn.1673-9434.2023.10.154.