Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 6, No. 1, 2024

China's Universities Network Security Current Situation and Solutions

Jianhua Shan

Information Construction Management Office, Nanjing University of Finance & economics, Nanjing, Jiangsu, China

Abstract: With the development of new technologies such as the Internet, artificial intelligence and big data, more convenience has been brought to Chinese colleges and universities, but it is followed by threats in network security. Due to the maturity of big data algorithms, it is easy to leak personal information and cause campus network security accidents while bringing convenience to college students. China's university network has experienced great development, but the current situation is not optimistic. There are many problems such as not paying attention to the ideology, heavy construction and light application. This paper focuses on the system construction, safety education and professional construction of these problems.

Keywords: Universities; Network Security; Solutions.

1. Introduction

After more than 30 years of rapid development, the network construction of Chinese universities has reached the international leading level in terms of basic hardware construction, software intelligent early warning management and user scale. The scientific, standardized and modern network has boosted the speed of colleges and universities in their own development process, and provided efficient, fast, sharing and forward-looking services for colleges and students to achieve the expected goals. At present, Chinese universities have fully realized the full coverage of network teaching, and established an internal campus network information management system. With the increase of user scale, data storage and access, colleges and universities rely more and more on the network. As a necessary way in the development of colleges and universities, colleges and universities can share resources and exchange information internally on the basis of network, and realize academic exchange and subject database construction externally. A potential threat is also becoming more and more concerned by university network administrators and operation maintainers. There are problems in the network operation of colleges and universities, such as malicious attacks, virus attacks, network extortion and other problems, resulting in paralysis of the university network or information leakage and hijacking, which will greatly affect the normal academic activities of colleges and teachers and students, and bring immeasurable losses. In 2016, the ransomware viruses WannaCry and Nopetya broke out worldwide, which spread freely in medical, transportation, energy and other network operation modules, causing system paralysis and user data lock, and bringing hundreds of millions of losses to network users. This problem is the need for high alert network operators. In the new era, it is very necessary to discuss how to carry out network security construction and deal with various network problems in daily operation and maintenance.

2. What is University Network Security

Network security is a dynamic process, not a static product, and network security is a big system, not just some equipment and management regulations. While on the surface these do play an important role in cyber security, the concept of cyber security is much broader and far-reaching. All network security starts with security policies, and network security also covers the users who must follow these security policies, and the implementors who are mainly responsible for enforcing these policies. Therefore, network security is broadly defined as a collection of all network equipment, technologies and best practices that provide security for information and data resources through mutual cooperation. Including access control technology, firewall technology, flow control technology, anti-virus software and so on. Through the establishment of data middle platform, the data of campus professional systems and business systems are fused to form a subject library. Build an information base including basic data. Third party partners such as functional departments and social forces can authorize the use of specific data in a limited scope, and at the same time reduce the risk of data leakage. Attention should be paid to improving data security protection capabilities for new technologies. Facing the challenges brought by new technologies such as cloud computing, big data analysis and artificial intelligence, it is necessary to strengthen security management to ensure their compliant use and healthy development. For example, measures such as data backup, data encryption, data desensitization and fine-grained access control are taken to strengthen data security and privacy protection capabilities. And deepen the construction of data security technology platform, and use big data analysis and AI technology to intelligently predict and discover potential data security problems and risks, prevent them before they happen, and change passive defense into active attack.

The network construction of colleges and universities is very mature. Based on the framework of on-campus student learning and exchange and off-campus academic exchange and sharing, great progress has been made in the hardware of network construction. From the physical level, the university network server can withstand high-energy, centralized access; Network security management through the authority management, virus early warning, information monitoring and other means, to a certain extent, can resist the risk of network operation; After a long time of network security education, teachers and students have a high awareness of using network security in colleges and universities, but some

students still do not understand the source and transmission mode of potential threats enough. However, limited by professional Settings and talent compilation, the network skills of background management personnel in network operation in colleges and universities and the effective treatment of unexpected problems need to be further improved. Attaching importance to network security and strengthening the construction of talent team in network security construction in colleges and universities will be the focus of network security work in colleges and universities.

3. The Necessity of University Network Security

3.1. The Need to Ensure the Information Security of College Students

College students are the direct beneficiaries and influencers of the Internet era. The promotion of network security education in colleges and universities is conducive to the protection of college students 'information security and development rights and interests in cyberspace. The Internet era is also the era of big data. The ability of big data to acquire, store, manage and analyze data has gone beyond traditional database software tools, with massive data scale, rapid data flow and diverse data types. Big data includes both structured data and unstructured data such as images, texts and videos, which are characterized by diverse content sources and diverse values. Under the background of Internet big data, the chaotic applications such as "information cocoon room", big data killing and algorithm discrimination emerge in an endless stream, which brings security risks and risks to colleges and universities, such as network payment security, network privacy security, network fraud, network psychological security and network violence. Colleges and universities strengthen network security education, improve college students' network risk awareness, safety awareness and responsibility awareness, make good use of the characteristics of big data immediacy, universality, unbounded and interconnection, and deeply mine and integrate the inherent advantages of it, which plays a very important role in promoting the construction of campus network security. Traditional education is mainly indoctrinated in a simple and rigid way, but in the big data environment, colleges and universities use big data to obtain and store data information, and carry out in-depth analysis and mining of the collected data information, and carefully arrange students 'needs for network security education, so that network security education is closer to college students 'study and life, and more prominent the subjective role of college students. Improving college students 'identification with network security education is conducive to ensuring the needs of college students 'information security and personal development under the background of big data.

3.2. The University's Own Information Security and Development Needs

The information security of colleges and universities is inseparable from the safe network environment. Conforming to the trend of educational informationization, technology and digitalization in the new era is the inevitable choice for the majority of colleges and universities. The integration of big data technology represented by the Internet, big data, cloud computing, artificial intelligence and university network security has brought new ideas and new directions to university network security. In the context of the Internet era, access to information in colleges and universities is no longer a small number of representative samples, but the use of frontier technologies such as big data, cloud computing, block chain, artificial intelligence and other technologies, through the application of collection, mining and storage technology, the current situation of campus network security is displayed graphically and in lists, so that complex data information can be integrated and presented. So as to effectively assess and reasonably predict the security risk of college students and colleges. In addition, in order to improve the pertinence and efficiency of network security construction in colleges and universities, big data technology can be used. Big data provides the possibility for the early warning mechanism of network security in colleges and universities, and reduces the negative impact of uncertain security risks in time. When the data information is abnormal, colleges and universities can realize the dynamic tracking and control of different management modules, flexibly adjust the education objectives, content and methods, and make network security education more timely, efficient and accurate. We will effectively improve colleges and universities' ability to prevent and resolve risks.

4. The Current Situation of Network Security in Colleges and Universities

China pays more and more attention to information industry, information technology is also developing continuously, and colleges and universities are also increasing the promotion of information education. The application of information technology achievements in colleges and universities is mainly manifested as: multimedia teaching, information query, paperless office, etc. Nowadays, the information dissemination of colleges and universities mainly depends on the network. The network has become the guarantee of the construction of the information platform of colleges and universities, and an important way for colleges and universities to sustainable development. China's Network Security Law was officially promulgated on June 1, 2017. This law stipulates that any technical or other schemes used in the construction, operation of networks or the provision of network services must comply with relevant laws and regulations as well as national mandatory standards to provide a safe, stable and effective operation of networks. It can reasonably respond to network security events, have scientific prevention countermeasures for network illegal crimes, and maintain the integrity, privacy and reliability of network data. Colleges and universities are the main body of the creation, operation and service of the campus network system, should refer to the relevant national policies and standards, and can not have any shirking behavior for social responsibility and legal responsibility. They should actively assume the corresponding responsibility to improve the security of the campus network and ensure its normal and stable operation. At present, a series of advanced cutting-edge technologies such as artificial intelligence, neural network and deep learning continue to develop and progress, and the education management mode has also been continuously improved. The information construction of colleges and universities has gradually developed from digital to intelligent. However, the resulting network security problems are also gradually increasing, such as increasing security equipment, improving the difficulty of management, the increase of users and their

behavior is gradually uncontrollable, and the continuous emergence of such as denial of service attacks (DDoS), system vulnerabilities are attacked, tampering with web pages and other security problems. As a result, the network teaching and scientific research work in colleges and universities have been affected and destroyed in different degrees. Network security management in colleges and universities is limited by factors such as staffing, operation and maintenance costs, and lacks smooth management mechanisms, fine control services, and standardized operation and maintenance processes. It is urgent to form a unified security protection system and establish a corresponding emergency early warning mechanism.

4.1. The Network Security Management System is not Sound

Through the online research method, browsing the websites of some university informatization related departments, it is found that there are the following problems in the network security management system: First, some colleges and universities do not have their own network security management system, and more rely on the national level of the Network security Law and the Data Protection Law, etc., without understanding and transforming according to the actual situation of the school, and issuing more detailed implementation methods or rules; Second, some universities have introduced network security responsibility system management methods, but the content is not comprehensive, the network security work is not detailed enough; Third, the network security management system of some colleges and universities has been issued for a long time, and the introduction time is not a minority around 2001. More than 20 years ago, with the development of society and the progress of information technology, the system has been unable to adapt to the current situation and characteristics, and the network security protection ability needs to be further enhanced, and the network security management system mechanism needs to be further improved.

4.2. The Attention to Network Security is Not Enough and the Network Security Protection Ability of Information Systems in Colleges and Universities is Uneven

The state has limited resources investment in colleges and universities, so colleges and universities pay more attention to investment in education resources. They think that the network security of schools is different from enterprise research and development and government secret departments, which is not so private and has not attracted attention, resulting in the low level of network security protection in colleges and universities. At the same time, colleges and universities generally deal with security problems after the fact, and do not judge the network security situation in time and make a response, and do not formulate a prevention plan. There is not enough understanding of the network security protection of software and hardware facilities in colleges and universities, even if there is relevant equipment, its role can not be maximized, at present, most colleges and universities do not have a mature network security system, there is no full-time professional management personnel, the awareness of network security protection has not kept up with the speed of network upgrading. Some colleges and universities do not have a perfect construction of network security mechanism, which also causes no small security risks.

4.3. College Students and Teachers have Insufficient Understanding of Network Security.

College students' network literacy refers to the ability of college students to collect information in the process of using the network, the ability to reasonably use data, the ability to identify and criticize the acquired data, and the ability to deal with network security. Under the background of big data, college students have poor network security cognition and awareness of security prevention, low network media literacy, weak awareness of personal privacy protection and low vigilance of network information. The massive information of big data makes college students who lack rational judgment at a loss, and it is easy to produce negative psychology such as data anxiety, data fatigue, and data dependence, which leads them to lose themselves in big data. College students' network security education lacks effective methods, and colleges and universities are not practical to improve college students' network literacy. Network security education in colleges and universities needs to guide college students to maintain vigilance of data presented by big data algorithms, cultivate college students 'data thinking ability, enhance college students 'ability to identify and prevent risks brought by data and algorithms, and form a network security education mode of college students 'self-supervision and self-management. In May 2017, a global network security incident, Eternal Blue, broke out all over the world. Many universities in China were not immune, and were extorted a high ransom to decryption files, and key data was lost in a large area. From this incident, we can find that if we have enough common sense of network security and develop good habits when using the network, we will take corresponding preventive measures in advance to avoid or reduce losses. The serious lack of awareness of network security is the biggest hidden danger of network security in colleges and universities. In addition, the majority of teachers and because of the identity of teachers network security awareness is how high. Teachers are only familiar with their own related fields, network security is also a new field for teachers, some teachers always think that their identity and life experience too much disdain network security and then personal information leakage and property damage.

4.4. Network Security Construction Lags Behind Information Application, Attaches Great Importance to Network Construction and Disregards Network Operation and Maintenance.

Quite a few colleges and universities are very enthusiastic about investing in information technology and network security construction, but they do not pay enough attention to specific applications. Application delivery pays attention to function realization, but the operation and maintenance of the system is insufficient after it is put into operation, and the security protection has not been paid due attention. Network application systems and management systems in colleges and universities are mostly built independently by different service providers, which are relatively independent in network security protection. The level of service providers directly determines the level of network security. After the

software and hardware system is running online or the relevant network protection tools are deployed, as long as the system functions normally, the attention to network security issues is not enough, mainly reflected in two aspects: First, the school believes that there is no necessity to do higher level security protection, and that the school's website (information system) is not so important and nothing can be stolen; Second, from the whole network security industry, government agencies and institutions and other organizations are mainly driven by administrative requirements and event-driven, more is to shut down access, after the repair of vulnerabilities, etc., with more websites running with disease, has not yet established a relatively complete overall network security protection system, and can not be prevented.

4.5. The Innovation of Network Security Education in Universities is not Strong

In recent years, network security problems have occurred frequently. Colleges and universities have paid more attention to network security awareness education for college students and achieved certain results. However, in the process of publicity, training and implementation of network security education in colleges and universities, there are still some problems such as scattered educational content and insufficient education guidance. There are still some problems in colleges and universities, such as weak awareness of big data, insufficient research on the technical characteristics of big data, lack of ability to use data and analyze data, and lack of effective judgment and profound grasp of college students 'network behavior under the background of big data, which leads to lagging network security education. In terms of educational content, colleges and universities lack the integration and design of network security education, and mostly focus on policy publicity and interpretation. The educational content is single and fragmented, which cannot meet the diversity needs of college students. In form, network security education in colleges and universities is not strong targeted, limited to instilled education, does not fully mobilize the subjective initiative and consciousness of college students, college students 'participation and interaction are not high; In terms of methods, network security education in colleges and universities lacks pertinence, education focus is not prominent, innovation is not strong, and the effect of network security education is not good. Network security education in colleges and universities is not a simple superposition of big data and education, but according to the general requirements of the country for network security education, under the premise of taking into account the universality and particularity of traditional education and big data network security education, the construction of a complete system with a certain scientific and scientific rationality.

4.6. Lack of Full-Time Network Security Personnel.

At present, there is a general lack of network security professionals in the relevant departments of informatization in Chinese universities. Compared with the development level of schools and the needs of network security, there are few full-time network security personnel, and the structure of network security full-time team is not perfect. For example, a university in western China has no full-time network security staff, and the network operation and maintenance personnel of the operation and maintenance service department of the information technology center of the school concurrently serve as network security management personnel. The staffing of network security personnel is not scientific. For example, in a university in northeast China, the personnel who undertake network security management study material science, which has a big gap in content with network security work, and there is a mismatch between professional background. Network security staff network security awareness is not strong, network security literacy is not enough, in the usual management work and no initiative to prevent awareness, lack of initiative, easy to implement security measures are not in place, security management operation is not perfect, lack of awareness of emergency treatment and so on.

5. Countermeasures for Improving Network Security Management in Universities

5.1. Strengthen Institutional Construction and Improve the Assessment Mechanism.

To do a good job of network security management in colleges and universities, it is necessary to adhere to the system to implement and standardize the work and personnel management. First, network security management should follow the principle of "who is in charge who is responsible", implement the responsibilities of schools, functional departments and individuals, clarify the responsibilities of the school party committee, information department, various units (departments, directly affiliated units, colleges), and network and information work commissioners, and clarify the responsibilities that need to be taken for violation of duties. Promote the implementation of network security responsibility system and the healthy development of information technology. Second, adhere to the goal and problem orientation, give full play to the guiding and supervising role of assessment and evaluation, formulate the assessment and evaluation standards of network security responsibility system, assessment and evaluation should adhere to the principle of regular, such as once a year, the assessment results can be used as one of the contents of the annual comprehensive assessment and evaluation of relevant personnel. The assessment and evaluation criteria of network security responsibility system need to include the implementation of responsibility system, team construction, work deployment, condition guarantee, publicity and training, system accounting, data management, operation and maintenance management, domain name annual inspection, security measures, data security, terminal management, notification disposal, log preservation, emergency drill and emergency disposal. For example, in January 2023, a university in Nanjing newly formulated the implementation Method of the network Security Work Responsibility System of a certain University. The method clarifies the main responsibility of network security, constructs a network of network security responsibility system, elaborates the responsibilities and content of the work, strengthens the organizational structure and condition guarantee, establishes an evaluation and accountability system, and improves the management level of network security work in the school. At the same time, the system includes network security responsibility system assessment and evaluation standards, which include organizational leadership, information assets,

daily operation and maintenance network security requirements, network security incident handling and other aspects.

5.2. Strengthen the Network Security Awareness Education for Teachers and Students.

University network security is based on the majority of teachers and students network security awareness. Cyber security awareness is not innate, it is acquired through education. Because network security awareness education is not required for everyone, and network security incidents are not necessarily encountered by everyone, so the enthusiasm of teachers and students in network security education is not high, and the study of network security education is ignored. This needs to increase the strength of network security education and guidance. Regularly arrange a network security knowledge science course for the majority of teachers every month. Although this approach will not satisfy every teacher, it is worth the time and money lost. Furthermore, these teachers have mastered the common sense of network security will be popularized to the relatives and friends around, and more and more people will master the common sense of network security, and network security is no longer a big problem. For students, we can put the common sense course of network security as a public required course into the education system, and strive for every student to master the common sense of security. Of course, it is necessary to make breakthroughs in the specific forms of education, and choose cases that occur in reality to carry out education and teaching in a form that is more acceptable to teachers and students, so as to achieve the effect of education.

5.3. Strengthen Technical Management.

In order to do well in network security management in colleges and universities, it is necessary to strengthen technical management and improve technical application ability. In today's era, Internet of things, big data, cloud computing and other information technology is promoting the rapid progress of society, network security as a closely related link, its development and changes are becoming more and more complex, showing many new situations and new characteristics, but also exposed a lot of new problems and deficiencies. For example, the development level of some website systems is uneven, the Internet exposure surface is relatively wide, and new risks such as mining and information leakage emerge in an endless stream. Therefore, the urgency and importance of doing a good job in network security are also becoming more and more prominent, and colleges and universities need to have high technical management ability. One is in the firewall technology, encryption technology, anti-hacker technology and other aspects of hard work, in the data room security, data access control, cloud data center security management, situation traffic audit, security operation management and other aspects, do network security into a system, a system, strong operation, can be managed. The second is to continuously improve the network security protection system through a variety of ways, for the campus network basic network, cloud data center, campus wireless, scientific research and teaching data, personal information and other aspects, through the security management, security technology, security operation, security evaluation and other technical management system to achieve full control of the campus network and security support. The third is to upgrade the campus network outlet firewall, realize the automatic switching function of firewall master and backup, deploy the real-time perception platform of network security, comprehensively monitor and analyze the campus network security situation, independently carry out system penetration testing and security vulnerability scanning, and improve the active operation and maintenance ability.

5.4. Build a Full-time Network Security Team.

It is necessary to have a full-time team to do a good job in network security. Strengthening the construction of network security full-time team is an inherent requirement to adapt to the change of situation in the new development stage and help improve the governance ability of colleges and universities, and is an important guarantee to ensure the healthy and safe operation of colleges and universities and promote the overall progress of colleges and universities. First, the full-time team of network security needs to be team, network security work involves network maintenance, system development, operation and maintenance services, administrative management and many other contents, the number of personnel should be determined according to the development level of the school and the scale of the school. Second, the network security full-time team needs to be specialized, network security work is a highly technical work, the staff needs to have professional technical qualifications. Third, the network security full-time team needs to be hierarchical, which requires both management personnel and technical personnel. Management personnel include daily administration, network security personnel, information system administrators, etc., and technical personnel include operation and maintenance services, emergency response, system development, network monitoring and other personnel. Fourth, the full-time team of network security needs to be socialized. Colleges and universities need to strengthen cooperation with companies in the society, make full use of professional strength to complete the work of classified protection evaluation, risk assessment, attack and defense actual combat, and also strengthen communication and contact with the three major operators, network security companies and other units, carry out more exchange of experience, and strengthen win-win cooperation. In addition to the daily staff, some universities also have a full-time network security team composed of six people, including network security engineers, data security engineers, cloud security engineers, and classified equipment operation and maintenance engineers, who are responsible for daily network security management, maintenance and disposal. At the same time, strengthen cooperation with the three major operators, network security companies and other units, establish long-term cooperative relationships, and support the high-quality development of school informatization work.

5.5. Establish a Network Security Information Sharing and Coordination Mechanism in Universities.

At present, the network security information of colleges and universities basically belongs to the fight for themselves, and there is a lack of communication between colleges and universities in network security information. A university network security problem, often is their own or in the third party to solve the help, rarely communicate with other universities. This leads to a problem, network security issues between universities can not do information sharing. When

information is not shared, problem solving is much less effective. Many problems in network security are similar, and some universities have mature solutions. As long as some information is properly shared, it will bring a lot of convenience for other schools to solve the problems. Therefore, it is particularly important for universities in the same region to establish a network security information sharing and coordination mechanism. In this mechanism, colleges and universities can exchange their own experiences and problems in campus network security management. With the coordination and sharing mechanism, it can effectively solve the problems of network security in some colleges and universities, and help to improve the overall security protection ability of colleges and universities.

6. Conclusion

Network security management in colleges and universities requires the participation of all teachers and students. In today's era, teachers and students can not live without the network in the campus, we must face the problem of network security. Only the formation of everyone concerned about network security, everyone involved in network security, in order to maintain the rights and interests of individuals and campus network security. However, the work of network security in colleges and universities is not achieved in one move, but a long-term process of continuous investment and continuous learning. This requires managers to update the concept of university network security work to give enough attention, although the network security work may not be able to bring real benefits, but the security work is not good harm is very big. For individuals, cyber security is closely related to our own interests. Paying attention to cyber security and supporting cyber security-related work is actually helping ourselves. Only all parties give enough attention and cooperate with each other, we can continue to do a good job in campus network security.

References

[1] Information on: https://zhuanlan.zhihu.com/p/527213875.

[2] Information on: https:// www. edu.cn/ xxh/ji_ shu_ ju_le_ bu/ wlaq/201902/t20190227_1646400.shtml.

[3] ShiMing.Wan： Theoretical guide, No2(2017)p.102-104.

[4] Ying Zhang: Information systems engineering ,No8 (2023) , p. 163.

[5] XiaoHong Xu: Network Security Technology and application, No11(2023), p.87-88.

[6] TianBo Liu: Journal of Shanxi University of Finance and Economics, Vol.45(2023), No.S2 p.199-200.