Information Systems and Economics (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/infse.2023.040701
ISSN 2523-6407 Vol. 4 Num. 7

Construction of enterprise network information security technology system under the background of big data

Li Ke*

Shandong Rongyue Financial Holdings Co., Ltd, Jinan, Shandong, China
**Corresponding author: like@royojr.com*

Keywords: Big data; Enterprise; Network information; Safety technical system

Abstract: This paper aims to explore the construction of enterprise network information security technology system under the background of big data. With the advent of the era of big data, enterprises are facing the growing threat of network information security. In order to deal with these threats, enterprises need to establish a perfect network information security technology system. Firstly, this paper analyzes the network information security challenges faced by enterprises under the background of big data. The rapid development of big data has brought more risks such as data leakage and cyberattacks to enterprises. Secondly, this paper puts forward the key elements of constructing the technical system of network information security. By establishing these elements, enterprises can form a comprehensive network information security technology system and improve their ability to cope with network security threats. Finally, this paper summarizes the significance and challenges of building a network information security technology system. By building a perfect network information security technology system, enterprises can effectively deal with network security threats under the background of big data and protect their core information assets. However, the construction of network information security technology system also faces challenges in technology, management and personnel training, which requires the joint efforts of enterprises and relevant departments.

1. Introduction

In today's digital age, the rapid development of big data has brought great influence on the operation and management of enterprises. However, it is followed by more and more network information security threats. Enterprises are faced with security risks such as data leakage, network attacks and malicious software, which may lead to significant economic losses and reputation damage. Therefore, it is very important for enterprises to build a strong network information security technology system.

First of all, the construction of enterprise network information security technology system under the background of big data has important theoretical significance. With the continuous development of big data technology, enterprises are facing more complex and diverse network security threats. Constructing a perfect network information security technology system can provide effective protection measures for enterprises and improve their ability to cope with network security threats.

Secondly, the construction of enterprise network information security technology system has important practical significance. Network information security has become an important support for the development and operation of enterprises. By constructing a perfect network information security technology system, enterprises can better protect their core information assets and prevent data leakage, network attacks and other security incidents. At the same time, enterprises can also improve the trust of customers and partners in their information security capabilities and enhance their competitiveness and sustainable development capabilities.

In addition, the construction of enterprise network information security technology system is also of great significance to the country and society. In the digital age, network security has become an important part of national security. As an important force of national economic and social development, the network security of enterprises is directly related to the security and stability of the country and society. Therefore, by constructing a powerful network information security technology system, the network security level of the whole country and society can be improved, and the stability and development of the country and society can be maintained.[1]

2. The challenge of enterprise network information security under the background of big data

2.1 The threat of network information security in the era of big data

In the era of big data, enterprises are facing increasing threats to network information security. With the continuous growth of enterprise data scale, the risk of data leakage also increases. Hackers, internal employees or external attackers may obtain sensitive data through various means, such as customer information and financial data. These leaks may lead to corporate reputation damage, legal liability and economic losses. The storage and processing of big data need to rely on the network, so network attacks have become one of the main threats faced by enterprises. Network attacks include DDoS attacks, malware, phishing, etc. These attacks may lead to the interruption of enterprise network services and the tampering or destruction of data. In the era of big data, the data collected and analyzed by enterprises involves a large amount of personal information. If this information is not properly protected, it may lead to personal privacy disclosure. In addition, when using big data analysis, enterprises also need to abide by laws and regulations to ensure the legality and compliance of data use. Social engineering and phishing attacks are a way to obtain sensitive information by deception. Attackers may impersonate legal institutions or individuals, and entice users to click on malicious links or provide personal information through e-mail, text messages, etc., so as to obtain sensitive data. In the era of big data, enterprises often share and exchange data with many suppliers and partners. This cooperative relationship increases the risk of supply chain security, and attackers may invade the enterprise network through supply chain links, obtain sensitive data or engage in other malicious activities.

In order to deal with these network information security threats, enterprises need to take a series of measures. These measures include establishing a strong network security infrastructure, formulating perfect security strategies and management measures, strengthening security monitoring and early warning, and improving employees' security awareness and skills. Only through the construction of a comprehensive network information security technology system can enterprises better protect their core information assets and meet the network security challenges brought by the era of big data.

2.2 The impact of big data on enterprise information security

In the era of big data, enterprises are facing more risks of data leakage. With the continuous growth and complexity of enterprise data, the risk of data leakage increases accordingly. Hacking attacks, improper behavior of insiders, security loopholes of third-party service providers, etc. may all lead to the disclosure of sensitive data of enterprises and bring huge losses to enterprises.

In the era of big data, enterprises are facing more threats of cyberattacks. Enterprise network in big data environment usually has complex architecture and huge data flow, which provides more targets and opportunities for hackers. Enterprises need to face various types of network attacks, including DDoS attacks, malware, phishing and so on, which may have a serious impact on the business operation and reputation of enterprises.[2]

In the era of big data, enterprises are facing more privacy protection challenges. Big data technology enables enterprises to collect and analyze a large amount of personal data, but it also increases the risk of personal privacy disclosure. Enterprises need to strictly abide by relevant privacy laws and policies to protect users' personal information, otherwise they will face legal risks and reputation losses.

In the era of big data, enterprises are facing more problems of data integrity and credibility. In the big data environment, the amount of data is huge and the sources are complex, which is easily affected by data tampering and false data. Enterprises need to take effective measures to ensure the integrity and credibility of data and ensure the accuracy and reliability of data.

3. Key elements of building enterprise network information security technology system

3.1 Network security infrastructure

Network security infrastructure is an important part of building enterprise network information security technology system. It includes hardware equipment, software system and network architecture, and is used to protect the network and information resources of enterprises from unauthorized access, attack and damage.

Enterprises can configure firewall rules to restrict access to specific IP addresses or ports, and realize network security isolation and access control. Intrusion detection and prevention system (IDS/IPS) can monitor and analyze network traffic in real time, identify potential intrusion behaviors, and take corresponding defense measures. IDS/IPS can improve its ability to identify and respond to network attacks by means of feature detection, behavior analysis and anomaly detection. Virtual Private Network (VPN) provides secure network connection for remote users through encryption and tunneling technology. Enterprises can establish VPN channels to realize the safe access of telecommuters and branches, and prevent sensitive information from being stolen or tampered with during transmission. Identity authentication and access control are important means to protect network security. Enterprises can adopt various authentication methods, such as password, biometric identification, two-factor authentication, etc., to ensure that only authorized users can access sensitive information and system resources.

Data encryption and decryption technology can protect the security of sensitive data during storage and transmission. Enterprises can use symmetric encryption algorithm or asymmetric encryption algorithm to encrypt data, and ensure the security of keys through key management system. Security audit and log management are important components of network security infrastructure. Enterprises can record and analyze the network activity logs through the security audit system, find abnormal behaviors and security incidents in time, and take corresponding response measures.[3]

When building a network security infrastructure, enterprises need to select appropriate hardware devices and software systems according to actual needs and risk assessment results, and conduct effective configuration and management. In addition, regular security vulnerability scanning and vulnerability repair are also important links to ensure the effective operation of network security infrastructure. By establishing a sound network security infrastructure, enterprises can improve their ability to detect and defend against network security threats and protect their core information assets.

3.2 Security Policy and Management

First of all, enterprises need to be clear about their own security goals and needs. This can be determined by risk assessment and security requirements analysis, including the protection of core information assets and the satisfaction of compliance requirements. Secondly, formulate the principles and guidelines of security policy. These principles and guidelines should match the business needs and risk characteristics of enterprises, and at the same time take into account the requirements of laws and regulations. Finally, formulate specific security strategies and control measures. These policies and measures can include access control, identity authentication, data encryption, security audit, etc. to ensure the implementation and enforcement of network security.

Enterprises should set up special security management departments or assign special personnel to take charge of network security affairs, and clarify the security responsibilities and authorities of each department. Enterprises need to formulate specific processes and systems of network security management, including the reporting and handling processes of security incidents and the repair processes of security vulnerabilities, so as to ensure the standardization and efficiency of security management. Enterprises should regularly organize network security training and awareness education activities to improve employees' knowledge and understanding of network security and enhance their safety awareness and skills. Conduct regular safety assessments and drills, find potential safety risks and loopholes, and take timely measures to repair and improve them.

Enterprises should set up a special security incident response team, which is responsible for monitoring and responding to network security incidents and taking timely measures for emergency treatment. Make a detailed security incident response plan, including the classification and level of the incident, response process and responsible person, etc., to ensure a quick and effective response when a security incident occurs. Through the security monitoring system and log analysis tools, the network security events can be monitored and analyzed in real time to find and deal with potential security threats in time. After the security incident is controlled, the follow-up treatment and summary are carried out, and the causes and lessons of the incident are analyzed to improve the security strategy and management measures.

Through effective security strategy and management, enterprises can establish a perfect network information security technology system. This will help to improve the enterprise's ability to respond to network security threats and protect the core information assets of enterprises. However, security strategy and management are also facing challenges, such as how to balance security and convenience, how to deal with changing security threats, etc., which need to be explored and improved by enterprises in practice.

3.3 Safety Monitoring and Early Warning

Through real-time monitoring and analysis of network traffic, abnormal traffic and attack behavior can be identified. Collect, store and analyze the logs of systems and network devices in order to track and audit security incidents. Using the technology of behavior analysis and machine learning, the abnormal behavior and attack behavior of users are identified. Obtain and analyze threat information from internal and external sources in time to provide support for security early warning. By monitoring network traffic and behavior, we can identify and prevent intrusion. Integrate and analyze information from various security devices and logs to achieve comprehensive security monitoring and event response. Identify potential threats and risks by analyzing the behaviors of users and entities. Obtain and analyze threat information from inside and outside in time, and provide real-time threat information sharing and early warning. According to the enterprise's security requirements and risk assessment results, determine the focus and objectives of monitoring and early warning. According to the requirements, select and deploy appropriate monitoring and early warning systems, including

IDS/IPS, SIEM, etc. According to the actual situation, formulate and configure monitoring rules and strategies in order to find and respond to security incidents in time. Through the monitoring system, the network traffic, logs and behaviors are monitored and analyzed in real time, and potential threats are found. Once abnormal behaviors or potential threats are found, early warning will be issued in time, and corresponding response measures will be taken, including isolation and blocking.

Through effective security monitoring and early warning, enterprises can grasp the network security situation in real time, discover and deal with potential threats in time, and protect the information assets of enterprises. However, security monitoring and early warning is also facing the challenge of data analysis and processing, which requires enterprises to establish a sound monitoring and early warning mechanism and constantly improve and optimize technical means and processes.

3.4 Safety Education and Training

Security education and training is a crucial link in the construction of enterprise network information security technology system. Through effective safety education and training, employees' safety awareness and skills can be improved, and their attention and understanding of network information security can be enhanced.

Conduct regular safety education and training to ensure that employees' knowledge and skills are updated and consolidated. Through continuous safety education and training activities, employees' safety awareness and skill level are continuously improved. Through the above safety education and training measures, employees' awareness of network security can be improved, so that they can actively guard against and respond to network security threats and reduce security loopholes and risks caused by employees' negligence or improper operation. At the same time, security education and training also provide a solid foundation for enterprises to build a sound network information security technology system.[4]

4. The significance and challenges of building enterprise network information security technology system

4.1 Improve the ability to respond to network security threats

The threat of network security is an evolving process, so enterprises need to constantly update and optimize the technical system of network information security to adapt to new threats and attack methods. However, improving the ability to respond to cyber security threats also faces some challenges. First of all, the rapid development and changes of network security technology make enterprises need to keep up with and update the technology. Secondly, the shortage and cultivation of network security talents has become an important factor restricting the improvement of enterprises' coping ability. In addition, the growing network security threats have also brought great pressure to enterprises. Therefore, enterprises need to fully consider these challenges when building a network information security technology system, and work together with relevant departments to improve their ability to cope with network security threats. Only through continuous innovation and improvement can enterprises better protect their core information assets and respond to network security threats.

4.2 Protection of enterprise core information assets

First of all, enterprises need to comprehensively identify and classify core information assets. By investigating and analyzing the information assets inside and outside the enterprise, we can determine which information belongs to the core assets and classify them, so as to better formulate corresponding protection strategies and measures. On the basis of identifying and classifying core information assets, enterprises need to formulate corresponding information asset protection strategies. This includes determining the confidentiality, integrity and availability requirements of information, and formulating corresponding security control measures, such as access control, encryption and backup, to ensure the security of core information assets. In order to protect core information assets, enterprises need to strengthen access control and identity authentication mechanisms. By establishing a strict authority management and authentication system, access to core information assets is restricted, and only authorized personnel can access and operate this information.

Data encryption is one of the important means to protect core information assets. By encrypting sensitive data, even in the case of data leakage, attackers cannot obtain useful information. In addition, make regular data backup to prevent data loss or being affected by threats such as ransomware. Enterprises should establish security monitoring and incident response mechanisms to detect and respond to attacks and threats to core information assets in a timely manner. Through the use of security monitoring tools and technologies, the security status of the network and system can be monitored in real time, and the corresponding incident response process can be established, so as to quickly respond to security incidents and investigate and repair them. Employees of an enterprise are an important part of information security, and their security awareness and skills are crucial to protecting core information assets. Therefore, enterprises should strengthen safety education and training, improve employees' knowledge and understanding of network security threats, and conduct regular safety training and drills.

4.3 Challenges in technology, management and personnel training

In the process of constructing enterprise network information security technology system, it faces challenges in technology, management and personnel training. These challenges require the joint efforts of enterprises and relevant departments to effectively deal with them. With the continuous development and evolution of network information security technology, enterprises need to keep up with the latest trend of technology and update and upgrade security technologies and tools in time. Enterprise network environment is complex and diverse, including internal network, external network and cloud service. How to implement security measures in such a complex environment is a technical challenge. In the big data environment, the data is huge and diverse, so how to safely process and protect the data is a technical problem.[5]

Enterprises need to formulate a comprehensive security strategy and ensure its effective implementation. This involves management challenges such as safety policy formulation, compliance management and risk assessment. Network information security is a comprehensive problem involving many departments and teams. How to achieve cross-departmental cooperation and communication and ensure the smooth progress of information security is a management challenge. Network security incidents are hard to avoid, so enterprises need to establish a sound security incident response mechanism and deal with it in a timely and effective manner. This requires management to have emergency response ability and decision-making ability. Professional and technical talents in the field of network information security are relatively scarce, and enterprises are facing difficulties in recruiting and retaining talents. How to train and attract high-quality network security talents is a personnel training challenge. The safety awareness and skills of enterprise employees are very important for network information security. How to carry out effective safety education and training to improve employees' safety awareness and skills is a personnel training challenge. With the continuous development of network information security technology, security threats are also evolving. Enterprises need to establish a learning organization to cultivate employees' continuous learning and adaptability in order to cope with the ever-changing security challenges.

5. Conclusion

First of all, the era of big data has brought more network information security threats to enterprises. The rapid development of big data makes enterprises face increased risks such as data leakage and cyberattacks. Therefore, building a strong network information security technology system is very important for enterprises to protect information assets. Secondly, the key elements of constructing enterprise network information security technology system include network security infrastructure, security strategy and management, security monitoring and early warning, security education and training, etc. These elements are interrelated and together constitute a comprehensive network information security technology system. Finally, by building a perfect network information security technology system, enterprises can effectively deal with network security threats under the background of big data and protect their core information assets. However, the construction of network information security technology system is also facing challenges in technology, management and personnel training. It needs the joint efforts of enterprises and relevant departments to strengthen technological research and innovation, establish a scientific management system and provide professional safety training and education.

References

[1] Du Chuansheng. Construction of network information security technology system under the background of big data [J]. Software, 2022, 43(01):77-79.

[2] Liang Yuan. Research on enterprise network information security technology system under the background of big data [J]. Cyberspace Security, 2018, 9(06):66-69.

[3] Sun Hongmei, Jia Ruisheng. Research on enterprise network information security technology system under the background of big data [J]. Communication Technology, 2017, 50(02):334-339.

[4] Song Li. Explore the construction of campus network information security technology system under the background of big data [J]. Information recording materials, 2023, 24(02):88-90.

[5] Zeng Zhongliang. Enterprise information security in the era of big data [J]. Network security technology and application, 2014, 164(08):137-138.