ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

Construction of Enterprise Information Security Guarantee System in the Digitalization Background

Hongjiang Pan

Taizhou Water Treatment Development Co., Ltd, Taizhou City, 318000, Zhejiang Province, China
839192017@qq.com

Abstract: *With the continuous improvement of enterprise informatization in the digital background, the problem of enterprise information security has become more and more prominent. The construction of information security assurance system has become an inevitable trend of enterprise informatization development. In this paper, we discuss the thinking points of constructing the enterprise information security system under the digital background from the aspects of security strategy, security policy, security monitoring and emergency response, and puts forward corresponding suggestions.*

Keywords: *Digitalization, enterprise information security, security assurance system*

1. Introduction

With the continuous improvement of enterprise informatization in the digital background, the problem of enterprise information security has become more and more prominent, and information leakage, network attacks, malware and other security incidents have occurred repeatedly, bringing huge economic and reputation losses to enterprises. Therefore, the construction of enterprise information security protection system has become an inevitable trend of enterprise information development. The construction of enterprise information security assurance system not only involves many aspects such as technology, management and organization, but also requires comprehensive consideration of the actual situation and needs of enterprises. This paper will discuss the idea of constructing enterprise information security system in the digital background from the aspects of security strategy, security policy, security monitoring and emergency response, and put forward corresponding suggestions.

2. Enterprise Information Security Issues

2.1. Information leakage

Information leakage is a serious security issue that can lead to the disclosure of privacy, property damage, reputation damage, and other consequences for businesses and individuals. The problem of information leakage involves multiple aspects, including technology, management, and personnel. Therefore, in order to effectively prevent and address information leakage, various factors need to be comprehensively considered. Firstly, technical issues are one of the main causes of information leakage. Technical issues include network security, system vulnerabilities, software defects, password cracking, and more. Businesses and individuals should take a series of technical measures to mitigate the risk of information leakage, such as encryption technology, firewalls, antivirus software, intrusion detection systems, etc. Additionally, timely updates and upgrades of security software and devices, patching system vulnerabilities, and preventing hacker attacks and malicious software intrusion are crucial. Secondly, management issues are also significant causes of information leakage [1]. Management issues include inadequate information management systems, improper access control, insufficient security training, and more. Businesses should establish sound information management systems, standardize the collection, storage, processing, and transmission of information, and strengthen the management and monitoring of internal employees and external service providers. Enhancing security training and awareness among employees is essential. Thirdly, personnel issues are important contributors to information leakage. Personnel issues include negligence, improper operations, malicious behavior by internal employees, and more. Businesses should strengthen employee management and monitoring, establish sound security management mechanisms, provide comprehensive security training and education, and enhance employees' awareness and prevention

ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

capabilities. Controlling and limiting employee permissions appropriately can help avoid situations of excessive authorization or misuse of privileges. Finally, the social environment includes policies and regulations, industry standards, and third-party security service providers. The government should strengthen legislation and regulation of information security, enhance security education and awareness among businesses and individuals, and promote the development of information security. Businesses should choose reliable third-party security service providers, enhance cooperation and communication with the government and industry organizations, and jointly promote the development of information security [2]. Overall, preventing and addressing information leakage requires a comprehensive approach that involves technological measures, sound management systems, employee training and awareness, as well as support from the social environment in terms of policies and collaborations.

2.2. Cyber attack

Cyber attacks refer to the means of hackers, viruses, Trojan horses, phishing and other methods to attack computer networks, with the aim of obtaining sensitive information, damaging network systems, and gaining economic benefits. The problem of cyber attacks involves various aspects such as technology, management, and personnel. Therefore, in order to effectively prevent and respond to cyber attacks, it is necessary to consider various factors comprehensively. Technical issues are one of the main causes of cyber attacks. Technical issues include network security, system vulnerabilities, software defects, password cracking, etc. Enterprises and individuals should adopt a series of technical measures to mitigate the risks of cyber attacks, such as encryption technology, firewalls, antivirus software, intrusion detection systems, etc. At the same time, enterprises and individuals should update and upgrade security software and devices in a timely manner, patch system vulnerabilities, and prevent hacker attacks and malicious software intrusion. Secondly, management issues are also important causes of cyber attacks. Management issues include inadequate information management systems, improper permission controls, and insufficient security training [3]. Enterprises should establish sound information management systems to standardize the collection, storage, processing, and transmission of information, and strengthen the management and monitoring of internal employees and external service providers. Strengthening security training and promoting employee awareness of security are crucial. Furthermore, personnel issues are a significant cause of information leakage. Personnel issues include negligence, improper operations, and malicious behavior by internal employees. Enterprises should strengthen the management and monitoring of employees, establish sound security management mechanisms, and provide comprehensive security training and education to enhance employee awareness and prevention capabilities. Controlling and limiting employee permissions appropriately can help avoid excessive authorization or abuse of permissions. Finally, the social environment includes policies and regulations, industry standards, and third-party security service providers. Governments should strengthen legislation and supervision of information security, enhance security education and awareness for enterprises and individuals, and promote the development of information security. Enterprises should choose reliable third-party security service providers, strengthen cooperation and communication with governments and industry organizations to promote the development of information security. In summary, preventing and responding to cyber attacks requires a comprehensive approach, including technical measures, sound management systems, employee training and awareness, as well as support from the social environment in terms of policies and cooperation [4].

2.3. Human negligence

Another important reason for enterprise information security problems is human negligence. Employees' low security awareness and lack of attention to information security make them prone to using weak passwords, downloading software at will and visiting insecure websites, which increase the risk of enterprise information security.

2.4. Mobile devices and cloud computing

With the widespread use of mobile devices and cloud computing technology, the storage and processing of enterprise information has become more convenient and efficient. However, at the same time, mobile devices and cloud computing also bring new security risks. The volatility and loss of mobile devices increase the risk of information leakage, and the security and compliance of cloud computing is also an important issue for enterprise information security assurance.

ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

2.5. Regulatory compliance requirements

With the increase of informationization, enterprises are facing increasing regulatory compliance requirements. Regulations require enterprises to strictly protect customer privacy and sensitive information, and enterprises need to establish a perfect security system to meet regulatory compliance requirements.

3. How to Build Enterprise Information Security Protection System

3.1. Security strategy development

This is an important aspect of enterprise information security. It refers to a series of security measures and management methods formulated to protect the security of enterprise information systems and data resources [5]. The development of security strategies requires comprehensive consideration of the specific situation, business requirements, and security risks of the enterprise in order to ensure the security, integrity, and availability of enterprise information. In the digital age, the increasing level of enterprise informatization exposes businesses to more and more information security risks. In order to safeguard the security, integrity, and availability of enterprise information, it is necessary for enterprises to establish scientifically reasonable security strategies. Security strategies can assist enterprises in determining information security goals and standards, clarifying security responsibilities and obligations, standardizing security behaviors and operations, strengthening security management and emergency response capabilities, thus effectively preventing and reducing information security incidents [6].

The steps for developing a security strategy are as follows:

(1) Risk Assessment: The enterprise should conduct a risk assessment of its information systems and data resources. This involves analyzing and evaluating security risks, identifying security threats and vulnerabilities, and providing foundational data and evidence for developing the security strategy.

(2) Goal Setting: The enterprise should determine the goals and standards for information security, clearly define the focus and importance of security measures, and develop strategies and plans for information security. This step provides guidance and support for subsequent security measures and management.

(3) Security Measures Development: Based on the results of the risk assessment and goal setting, the enterprise should formulate a series of security measures and management methods. These may include security policies and regulations, security technologies and tools, security training and awareness, etc. The aim is to ensure the security, integrity, and availability of the enterprise's information systems and data resources.

(4) Implementation and Monitoring: The enterprise should implement the security measures and management methods outlined in the security strategy. Regular security checks and assessments should be conducted, and monitoring of employees' security behaviors and operations should be carried out to ensure the security and reliability of the enterprise's information.

(5) Training and Awareness Raising: The organization conducts employee training and awareness-raising activities to enable employees to understand the content and importance of safety strategies and to have the appropriate safety skills and behavioral awareness.

(6) Security control and monitoring: The organization establishes appropriate security controls, including access control, authentication, encryption, etc., to protect critical assets and sensitive information. It also establishes security monitoring mechanisms to detect and respond to security events in a timely manner and make necessary fixes and improvements.

(7) Regular evaluation and improvement: The organization regularly evaluates the effectiveness and compliance of security policies and makes adjustments and improvements according to the actual situation. It responds to new threats and risks in a timely manner and maintains the continuous adaptability of the security policy.

Developing a security strategy can help enhance an enterprise's information security capabilities, protect its business secrets and customer privacy, and improve its reputation and credibility. An effective security strategy can help prevent information leaks, network attacks, and other security incidents, minimize information security risks and losses, and improve the enterprise's security

ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

defenses and emergency response capabilities.

3.2. Security policy development

The formulation of a security strategy is an important step in ensuring the information security of an enterprise. When developing a security strategy, the enterprise should consider its specific situation, business requirements, and security risks to ensure the security, integrity, and availability of its information. The specific content of a security strategy includes the following aspects: Firstly, the enterprise should establish clear security policies and regulations. Security policies and regulations are the foundation for safeguarding the information security of an enterprise. The enterprise should define the security responsibilities and obligations of employees, restrict employees' access privileges, and prevent unauthorized access to the enterprise's information systems and data resources. In addition, the enterprise should develop password and access control regulations to specify password strength and expiration dates, preventing password leaks and cracking. Furthermore, the enterprise should establish data backup and recovery regulations to ensure the backup and recovery capabilities of important data, preventing data loss and damage. Additionally, the enterprise should develop security audit and logging regulations to monitor the security status of its information systems and data resources, promptly identifying and addressing security vulnerabilities and anomalies. Secondly, the enterprise should adopt scientifically reasonable security technologies and tools to strengthen the security protection and management of its information systems and data resources. The enterprise should deploy security technologies and tools such as firewalls, intrusion detection systems, and encryption techniques to guard against network attacks and malicious software. Moreover, the enterprise should utilize a unified security management platform to centrally manage the security status and management measures of its information systems and data resources. Thirdly, the enterprise should regularly conduct security training and awareness programs to enhance employees' security awareness and skills and strengthen security prevention and emergency response capabilities. The enterprise should establish a security training plan to provide information security education and training for employees, enhancing their awareness and prevention capabilities regarding security issues. Simultaneously, the enterprise should regularly conduct security awareness campaigns to raise employees' security awareness and sense of responsibility, fostering a strong security culture. Lastly, the enterprise should conduct regular security checks and evaluations to identify and address security vulnerabilities, improving the security and reliability of its information systems and data resources. The enterprise should establish a sound security inspection system to conduct regular security checks and evaluations of its information systems and data resources, promptly identifying and addressing security risks and vulnerabilities [8]. Additionally, the enterprise should establish an emergency response mechanism, develop emergency plans and procedures, and respond to unforeseen security incidents. When formulating a security strategy, the enterprise should select appropriate security measures and management methods based on its own situation and practical needs, ensuring the security, integrity, and availability of its information. The enterprise should view information security as an important strategic aspect of its development, strengthen security prevention and management, enhance information security capabilities, and ensure the business operations and growth of the enterprise.

3.3. Security management and monitoring

Security management and monitoring are critical components of enterprise information security. They help organizations identify and address security threats, as well as mitigate risks to information systems and data resources. When implementing security management and monitoring, enterprises should adopt comprehensive security measures and management methods to ensure the confidentiality, integrity, and availability of their information systems and data resources. Firstly, enterprises should establish sound security management systems and implement comprehensive security measures. The security management system should include security responsibility mechanisms, security management standards, security training and awareness programs, and security inspections and evaluations. Enterprises should establish clearly defined security responsibility mechanisms that specify the individuals and their roles in security management. Additionally, they should develop security management standards to regulate employees' security behaviors and operations, thereby preventing security risks. Regular security training and awareness activities should be conducted to enhance employees' awareness and preventive capabilities. Lastly, enterprises should conduct regular security inspections and evaluations to identify and resolve security vulnerabilities and risks. Secondly, enterprises should employ scientifically sound security monitoring technologies and tools to comprehensively monitor and manage their information systems and data resources. This includes

ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

deploying firewalls, intrusion detection systems, encryption technologies, and other security measures to ensure the security and integrity of information systems and data resources. Furthermore, enterprises should adopt a unified security management platform to centrally manage the security status and measures of their information systems and data resources. They should establish a robust security event monitoring and management mechanism to promptly detect and handle security incidents. Thirdly, enterprises should establish a sound security audit and log management mechanism to monitor the usage of their information systems and data resources. Enterprises should develop security audit standards and log management specifications to record the usage and security incidents of their information systems and data resources. Additionally, they should implement security information and event management systems to achieve real-time monitoring and management of security events. Lastly, enterprises should establish an effective emergency response mechanism to timely respond to security incidents and threats. They should develop emergency response plans and procedures that outline specific steps and responsible personnel. Enterprises should conduct emergency drills and training to enhance employees' emergency response capabilities. Simultaneously, they should establish an emergency response team composed of professional technical and managerial personnel to coordinate responses to security incidents. During the implementation of security management and monitoring, enterprises should strengthen security awareness and culture, enhance employees' security awareness and preventive capabilities, and establish a comprehensive security safeguard system with the participation of all staff members. Enterprises should also collaborate with third-party security service providers to jointly enhance their security management and monitoring capabilities and improve their information security defenses. Additionally, enterprises should continuously learn and explore the latest security technologies and methods, continually enhancing their own security management and monitoring capabilities to ensure the security, integrity, and availability of their information.

3.4. Technical protection and emergency response

Technical protection and emergency response are important components of enterprise information security. They help businesses to prevent and respond to security threats, ensuring the security and integrity of information systems and data resources. When implementing technical protection and emergency response, enterprises should adopt comprehensive measures and methods to enhance their security capabilities. Firstly, enterprises should establish a robust security protection system and utilize scientifically sound security technologies and tools to comprehensively protect their information systems and data resources. This can involve deploying technologies such as firewalls, intrusion detection systems, and encryption techniques to ensure the security and integrity of information systems and data resources. Additionally, regular vulnerability scanning and security testing should be conducted to identify and address security vulnerabilities and risks. Secondly, enterprises should employ data backup and recovery technologies to ensure the security and reliability of important data. Regular backups should be performed, and multi-layered backup and recovery mechanisms should be established to safeguard the security and availability of data. Furthermore, data encryption techniques can be employed to protect the confidentiality and integrity of critical data. Thirdly, enterprises should establish a robust security monitoring and early warning mechanism to promptly detect and handle security threats. Deploying security event management systems enables real-time monitoring and management of security events. Establishing an early warning mechanism allows for swift response and mitigation of security incidents. It is also important to analyze and trace security events to identify their root causes. Lastly, enterprises should establish a comprehensive emergency response mechanism to effectively address security incidents and threats. This involves developing emergency plans and procedures, clearly defining specific steps and responsible personnel for emergency response. Regular emergency drills and training should be conducted to enhance employees' emergency response capabilities. Additionally, establishing an emergency response team consisting of professional technical and managerial personnel facilitates coordinated responses to security incidents. During the implementation of technical protection and emergency response, enterprises should strengthen security awareness and cultivate a security culture to enhance employees' awareness and prevention capabilities, forming a comprehensive security assurance system involving all staff members. Collaboration with third-party security service providers can also promote enterprise security management and monitoring, thereby enhancing information security capabilities. Furthermore, continuous learning and research on the latest security technologies and methods are essential to continually improve security capabilities and ensure the security, integrity, and availability of enterprise information [9].

ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

3.5. Multi-partnership and sharing

Multilateral cooperation and sharing are important means for ensuring the security of enterprise information. They can help enterprises make full use of external resources and information, and enhance their capabilities in information security. When implementing multilateral cooperation and sharing, enterprises should strengthen the selection and management of partners to ensure the improvement of security capabilities. Firstly, enterprises should cooperate with third-party security service providers to jointly promote security management and monitoring. Enterprises can entrust third-party security service providers to conduct security consultation, assessment, monitoring, and other work to enhance their security capabilities. In addition, enterprises can also collaborate with security technology and product suppliers to jointly advance the research and application of security technologies, thereby improving their security capabilities. Secondly, enterprises should strengthen cooperation with industry organizations and government departments to jointly promote information security. Enterprises can participate in the formulation of security standards and reporting of security vulnerabilities in industry organizations, thus promoting industry-wide information security. Furthermore, enterprises can collaborate with government departments to participate in the formulation and implementation of government policies on information security, working together to promote information security. Thirdly, enterprises should enhance cooperation and sharing among internal departments. Enterprises should establish cross-departmental mechanisms for information sharing and collaboration to achieve shared and coordinated management of information resources. Enterprises should enhance information exchange and communication among internal departments to collectively advance information security. Additionally, enterprises should establish internal security training and awareness mechanisms to enhance employees' security consciousness and preventive capabilities. Lastly, enterprises should strengthen cooperation and sharing with external security partners. Enterprises can establish security cooperation mechanisms with suppliers, customers, and partners to jointly promote information security. By sharing security intelligence and information on security incidents, enterprises can achieve information interoperability and sharing. At the same time, enterprises should enhance security management and monitoring of their partners to ensure that they do not become weak links in enterprise information security. When implementing multilateral cooperation and sharing, enterprises should strengthen security awareness and culture, and enhance employees' awareness and preventive capabilities. Enterprises should establish sound security management and monitoring mechanisms to ensure the security and reliability of security partners. Additionally, enterprises should continuously learn and research the latest security technologies and methods to continuously improve their own security capabilities and ensure the security, integrity, and availability of enterprise information. Multilateral cooperation and sharing are important means for ensuring the security of enterprise information. Enterprises should strengthen cooperation and sharing among all parties, make full use of external resources and information, and enhance their capabilities in information security. Enterprises should also strengthen internal and external security management and monitoring to ensure the security and reliability of security partners, and to safeguard the security, integrity, and availability of enterprise information.

4. Conclusion

With the advent of the digital age, the level of enterprise informatization is constantly improving, and information security issues have become increasingly complex and severe. The construction of an information security assurance system has become an inevitable requirement for the development of enterprise informatization and an important guarantee for sustainable development. In the digital context, enterprises should strengthen multi-party cooperation and sharing, based on technical protection and emergency response, to build an information security assurance system that involves all employees and is jointly maintained. Enterprises should strengthen security awareness and culture and enhance employees' awareness and preventive capabilities. Continuous learning and research on the latest security technologies and methods are necessary to continuously improve their own security capabilities and ensure the security, integrity, and availability of enterprise information. At the same time, enterprises should strengthen cooperation and sharing with third-party security service providers, industry organizations, government departments, and security partners, making full use of external resources and information to enhance their information security assurance capabilities. Enterprises should strengthen internal and external security management and monitoring to ensure the security and reliability of security partners and safeguard the security, integrity, and availability of enterprise information. The construction of an information security assurance system is a long-term and dynamic process that requires continuous adaptation and response to new security challenges and threats.

ISSN 2616-5775 Vol. 6, Issue 7: 138-144, DOI: 10.25236/AJCIS.2023.060718

Enterprises should remain vigilant, strengthen security management and monitoring, and continuously improve their own security assurance capabilities to provide strong guarantees for the development and operation of the enterprise. Overall, enterprises need to establish a comprehensive and systematic information security assurance system, which includes technical measures, employee awareness and training, cooperation and sharing with external parties, and continuous improvement and adaptation to new challenges. By doing so, enterprises can effectively protect their information assets, maintain business continuity, and ensure sustainable growth in the digital era.

References

[1] Di Zhenpeng,Liu Yun,Li Shimei. Networked Organizational Structure of Enterprise Information Security Management Based on Digital Transformation and Genetic Algorithm [J]. Frontiers in Public Health, 2022,10.

[2] Liu S.,Qiao L.,Liu Y.,Ran R. Enterprise information security evaluation system based on big data[J]. IPPTA: Quarterly Journal of Indian Pulp and Paper Technical Association,2018,30(8).

[3] Dharmalingam Ramalingam,Shivasankarappa Arun,Neelamegam Anbazhagan. A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM[J]. Procedia Computer Science,2018,134.

[4] Paul John Steinbart,Robyn L Raschke,Graham Gal,William N Dilla. SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs[J]. Journal of Information Systems, 2016,30(1).

[5] Ramalingam D, Arun S, Anbazhagan N. A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM[J]. Procedia Computer Science,2018,134.

[6] Nina Evans,James Price. Development of a holistic model for the management of an enterprise's information assets[J]. International Journal of Information Management,2020,54.

[7] Kai Li, Guihong Zhang, Nan Li, Hua Yang. A Novel Public Information System for Mobile Geriatric Medical Services[J]. Revue d'Intelligence Artificielle,2019,33(3).

[8] Lv X,Zheng S,Li Z, et al. Application of graph databases in the communication and information asset management in power grid[C]//Wuhan Zhicheng Times Cultural Development Co., Ltd. Proceedings of 2016 International Conference on Automotive Engineering,Mechanical and Electrical Engineering(AEMEE 2016).CRC Press/Balkema,2016:374-379.

[9] Nina Evans,James Price. Enterprise information asset management: the roles and responsibilities of executive boards[J]. Knowledge Management Research & Practice,2016,14(3).