Financial Engineering and Risk Management (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/ferm.2024.070322
ISSN 2523-2576 Vol. 7 Num. 3

Identification of Factors Influencing Enterprise Data Security Risks under the Background of Digital Transformation

Cong Wang

State Grid Shandong Electric Power Company Information and Communication Company, Jinan, Shandong, 250000, China

Keywords: Digital Transformation; Enterprise Data Security; Risk Influencing Factors

Abstract: The advancement of digital transformation has led enterprises to face an increasing number of data security risks. This paper aims to identify the influencing factors of enterprise data security risks under the context of digital transformation. First, it classifies the factors affecting enterprise data security risks into technological and organizational categories. Next, it introduces methods for assessing and identifying these risk factors, which include both quantitative and qualitative evaluation methods. Finally, it proposes data security risk management strategies, including preventive measures, monitoring and detection, and emergency response and recovery strategies. By thoroughly researching these aspects, enterprises can better cope with the data security risks brought about by digital transformation.

1. Introduction

With the continuous advancement of digital transformation, enterprise data has become increasingly crucial, while also facing growing data security risks. Threats such as data breaches, cyber-attacks, and internal errors can lead to financial losses and damage to corporate reputation. Therefore, identifying and understanding the factors influencing enterprise data security risks in the context of digital transformation is crucial. This paper will conduct an in-depth study to explore the technological and organizational factors, introduce methods for assessing and identifying these risk factors, and propose a series of data security risk management strategies to help enterprises better protect their data assets.

2. Classification of Factors Influencing Enterprise Data Security Risks

2.1. Technological Factors

2.1.1. Cloud Computing and Virtualization

In recent years, enterprises have widely adopted cloud computing and virtualization technologies for data storage and processing. Cloud computing offers flexibility, scalability, and cost-effectiveness, but it also introduces certain security risks. Firstly, storing data on the servers of cloud service

providers can lead to data breaches or unauthorized access. Therefore, ensuring that cloud service providers have robust security measures and compliance is crucial. Secondly, the shared resources in a virtualized environment may cause data confusion between different users or cross-VM attacks. For enterprises, implementing strict access controls, isolation, and encryption measures is key to ensuring data security and privacy protection[1].

2.1.2. Internet of Things (IoT) and Edge Computing

The rapid development of the Internet of Things has brought more data sources and connected devices to enterprises. However, the security issues of devices and communication in IoT make enterprises vulnerable to attacks. IoT devices often have vulnerabilities such as firmware flaws, default credentials, and insecure communication protocols, which hackers can exploit to invade enterprise networks or steal sensitive data. Additionally, the use of edge computing increases the risks during data transmission and processing. Edge devices often process data locally and then send the results to the cloud or central servers. During this process, data may be exposed to attacks and tampering risks during transmission. Therefore, ensuring the secure configuration of IoT devices, strengthening communication encryption, and implementing strict access controls are crucial for protecting data security.

2.1.3. Big Data and Artificial Intelligence

The application of big data and artificial intelligence brings more opportunities to enterprises, as well as new security challenges. The storage and processing of big data involve a large amount of sensitive information, such as personal identification information and transaction records. If this data is not adequately protected, it may lead to privacy breaches and identity theft. Moreover, data merging and sharing in the process of big data analysis may lead to an aggregation effect, further revealing sensitive information. For artificial intelligence algorithms, their black-box nature makes it difficult to understand and assess their impact on data security. Hackers can manipulate input data to deceive or even sabotage AI systems. Therefore, ensuring data privacy protection, implementing data anonymization, and adopting transparent and interpretable AI algorithms are key in the application of big data and artificial intelligence[2].

2.2. Organizational Factors

2.2.1. Security Culture and Awareness

The internal security culture and the awareness of employees are crucial to data security. Establishing a positive security culture can encourage employees to take personal responsibility for data security and ensure they take necessary security measures in their daily operations. Employees should receive regular training to understand the latest security threats and protection measures, as well as how to identify and respond to potential security risks. A lack of security awareness and training may lead to employees committing security breaches or becoming targets of social engineering attacks.

2.2.2. Internal Management Systems and Processes

Robust internal management systems and processes form the foundation of data security. This includes access control, permission management, data classification and labeling, and security auditing. By defining and implementing these systems and processes, enterprises can limit access to and usage of data, reducing the risks of data leaks and misuse. Access control and permission

management ensure that only authorized personnel can access sensitive data. Data classification and labeling help enterprises determine appropriate security measures and protection levels based on the sensitivity and confidentiality of the data. Security audits can track and monitor data access and usage activities, promptly identifying abnormal behavior and potential security threats.

2.2.3. Enterprise Data Security Risk Management and Compliance Measures

In the context of digital transformation, enterprises face diverse data security risks, making effective risk management and compliance measures crucial. Key factors include comprehensive risk assessments and vulnerability identification covering technological, organizational, and regulatory aspects, providing a basis for developing risk mitigation measures. Establishing clear security strategies, policies, and standards is crucial for regulating the behavior of employees and systems, ensuring data is adequately secured during access, processing, and storage. Additionally, enterprises must ensure that their security strategies and operations comply with relevant laws and regulatory requirements. Establishing compliance requirements with third-party partners ensures that external partners also adhere to best practices and industry standards in data processing and storage. These measures collectively form the core elements for protecting data security in digital transformation, considering multiple factors such as technology, organization, and regulations, enabling enterprises to more effectively address potential data security risks[3].

3. Technical Factors of Enterprise Data Security Risks in Digital Transformation

In the wave of digital transformation, enterprises extensively use advanced technologies such as cloud computing, virtualization, the Internet of Things, edge computing, big data, and artificial intelligence, which bring tremendous business opportunities and benefits. However, these technologies also introduce a series of potential data security risks, requiring enterprises to be highly vigilant and cautious in adopting these technologies.

3.1. Cloud Computing and Virtualization Technologies

3.1.1. Cloud Computing Security Challenges

In the wave of digital transformation, cloud computing, as a flexible mode of data storage and processing, provides enterprises with outstanding scalability and cost-effectiveness. However, this convenience also comes with potential security challenges, especially when storing data on servers of cloud service providers. To effectively manage cloud computing security challenges, enterprises need to pay close attention to the security measures of cloud service providers, ensuring they can provide adequate data privacy protection, robust access control mechanisms, and compliance with regulatory standards. Through these measures, enterprises can more securely enjoy the flexibility and economic benefits of cloud computing, ensuring the security and integrity of data during the digital transformation process.

3.1.2. Data Disarray and Attacks in Virtualized Environments

The widespread application of virtualization technology allows different users to share the same physical resources, but it also brings the potential risks of lateral attacks and data disarray. To ensure the security and privacy of data in virtualized environments, enterprises should adopt multilayered security measures. By implementing strict access control, refined isolation, and enhanced encryption measures, enterprises can effectively mitigate the security risks in virtualized environments and ensure the comprehensive protection of sensitive data. This includes controlling access to virtual

machines, encrypting network communications, and securing the virtualization management platform. This series of security measures collectively builds a solid defense, helping to ensure the security and privacy of data during the enterprise's digital transformation process.

3.2. Internet of Things and Edge Computing

3.2.1. Security Issues with IoT Devices

The rapid development of the Internet of Things (IoT) provides enterprises with more data sources and connected devices, but the security issues associated with IoT devices also make enterprises vulnerable to attacks. Problems such as device firmware vulnerabilities, default credentials, and insecure communication protocols require enterprises to take measures such as secure device configuration, communication encryption, and enhanced identity authentication to guard against potential attacks[4].

3.2.2. Data Transmission Risks in Edge Computing

Edge computing pushes data processing to the network edge, increasing the risks associated with data transmission and processing. The use of secure protocols such as SSL/TLS, along with implementing device authentication and data encryption, becomes an essential way for enterprises to reduce the risks associated with edge computing.

3.3. Big Data and Artificial Intelligence

3.3.1. Big Data Storage and Privacy Protection

The storage and processing of big data involve a significant amount of sensitive information, such as personal identification information and transaction records. To ensure privacy protection, enterprises need to adopt encryption measures to effectively protect sensitive data stored in databases, file systems, and cloud services, and implement access control and data classification strategies.

3.3.2. Black Box Risks of Artificial Intelligence Algorithms

The black box nature of artificial intelligence (AI) algorithms makes it difficult to understand and assess their impact on data security. By adopting transparent and explainable AI algorithms, enterprises can reduce the risks associated with the use of AI, guarding against the possibility of hackers manipulating input data to deceive systems.

By thoroughly understanding and effectively managing the technical aspects of data security risks associated with cloud computing, virtualization, IoT, edge computing, big data, and artificial intelligence, enterprises can better address the challenges of digital transformation and protect critical data resources.

4. Data Security Risk Management Strategies

4.1. Preventive Measures

4.1.1. Strengthening Network Security and Identity Authentication

In today's digital environment, enterprises are increasingly exposed to complex and widespread cyber threats. To safeguard enterprise networks from unauthorized access and attacks, strengthening network security is crucial. Key measures include the implementation of firewalls, intrusion detection

systems, and security gateways. Firewalls monitor network traffic and filter potential malicious traffic, intrusion detection systems can detect and alert potential intrusions, while security gateways provide a secure connection point to manage and scrutinize network communications.

Implementing robust identity authentication mechanisms is also an essential step in ensuring network security. Traditional username and password authentication methods are susceptible to hacking and misuse. Multi-factor authentication, which combines several methods of verification such as passwords, fingerprints, tokens, or biometric data, significantly enhances the security of identity verification. Single Sign-On (SSO) allows users to access multiple applications with one set of credentials, reducing the burden of password management and providing stronger authentication protection.

4.1.2. Encryption and Data Protection Measures

Data security during information transmission and storage is critical. Encryption is a common technique used to protect sensitive data. By converting data into an unreadable format using encryption algorithms, data confidentiality and integrity are ensured even if the data is intercepted or leaked. Enterprises should encrypt sensitive data stored in databases, file systems, and cloud services, and use secure protocols such as SSL/TLS during data transmission to protect data from man-in-the-middle attacks.

Additionally, implementing data backup and disaster recovery strategies are important data protection measures. Regularly backing up data and storing backups in secure locations can prevent data loss. Disaster recovery plans help enterprises quickly recover business operations in the event of data breaches, system failures, or other catastrophic events. Restricting access to sensitive data is also key to reducing the risks of data leakage and misuse. By implementing the principle of least privilege and access control policies, authorizing only necessary personnel to access sensitive data can minimize potential internal threats and errors.

4.2. Monitoring and Detection

4.2.1. Security Event Logging and Auditing

Establishing security event logging and auditing mechanisms is an important part of ensuring network security. By recording security events and activities within systems and networks, enterprises can monitor and track potential security threats in real-time. Security event logs include information such as login activities, changes in access permissions, abnormal behaviors, and attempted attacks. This log data can be used for post-event analysis to identify the causes and impacts of security events and to take appropriate defensive measures[5].

Auditing involves reviewing and verifying system and network activities. Through auditing, enterprises can check the compliance of security policies, identify potential vulnerabilities or security risks, and take corrective measures in a timely manner. Additionally, auditing can provide key oversight and compliance evidence to meet regulatory and standard requirements.

4.2.2. Threat Intelligence and Anomaly Detection

Acquiring threat intelligence is crucial for staying informed about attack trends and malicious activities. Enterprises should closely monitor threat intelligence from security vendors, communities, and relevant agencies to understand the latest attack techniques and malware information. This helps enterprises adjust their security strategies and strengthen protective measures to address emerging threats.

In addition to threat intelligence, anomaly detection is a vital security measure. By monitoring

system and user behaviors in real time, enterprises can identify potential threats and risks. Anomalies may include unauthorized access, unusual data transmissions, or abnormal login activities. Using behavior analysis and machine learning techniques, enterprises can develop models to detect these anomalies and promptly discover potential attacks and intrusion attempts.

4.2.3. Establishing and Operating a Security Operations Center (SOC)

Establishing a Security Operations Center (SOC) is a key initiative to enhance enterprise network security. The SOC provides real-time threat monitoring, incident response, and security management through centralized monitoring and response to security events. It integrates security tools, technologies, and processes and is staffed by a professional security team. The SOC can rapidly identify and respond to threats by monitoring and analyzing security event logs, threat intelligence, and abnormal behaviors in real time.

The Security Operations Center is responsible for monitoring the security status of networks and systems, promptly detecting and responding to potential security events. It helps enterprises quickly address security threats and limit potential losses through the implementation of security policies, vulnerability management, and emergency response plans. The SOC can also provide security training and awareness activities to help employees improve their understanding of security risks and response capabilities.

In summary, establishing security event logging and auditing mechanisms, acquiring threat intelligence, using anomaly detection technologies, and establishing a Security Operations Center are key measures for strengthening enterprise network security. These measures help monitor and respond to potential security threats in real time and stay updated with the latest attack trends and malicious activities. By comprehensively applying these measures, enterprises can enhance their network security level, ensuring the integrity and reliability of sensitive data and business operations.

4.3. Emergency Response and Recovery

4.3.1. Emergency Response Plan and Process

In the context of digital transformation, it is crucial for businesses to have an effective emergency response plan to ensure a swift and orderly response in the event of a security incident. Initial steps include establishing an emergency contact list to ensure timely notification of relevant personnel when an incident occurs. Additionally, setting up a dedicated emergency team or designated individuals who will coordinate and execute emergency measures is vital. After an incident occurs, conduct a rapid investigation and assessment to clarify the nature, scope, and potential impact of the incident. Emergency measures such as isolating affected systems and stopping the spread of the attack are necessary to contain the security incident. Repairing vulnerabilities and quickly restoring system functions are central goals of the emergency response plan, ensuring the business can quickly return to normal operations. These emergency response steps will help minimize potential losses and enhance the business's ability to handle security threats in the context of digital transformation.

4.3.2. Data Backup and Recovery Strategies

During digital transformation, businesses must establish rigorous data backup and recovery strategies to ensure business continuity and effectively counter security threats. Primary measures include regular data backups and verifying the integrity and recoverability of backup data. These backups should be stored in secure and reliable locations and must be encrypted to ensure the confidentiality of the data is not compromised. Establishing a recovery testing plan is crucial; by regularly testing the recovery process of backup data, businesses can ensure that data can be quickly

and effectively restored when necessary. Backup strategies should determine different levels of backup frequency and retention periods based on the importance and sensitivity of the data to better meet business needs. This comprehensive data backup and recovery strategy will effectively enhance the business's data security, ensuring quick and effective business recovery in the face of potential threats.

4.3.3. Risk Response and Business Continuity Plan

To prevent and mitigate the impact of security incidents or disasters on business operations, businesses must develop comprehensive risk response and business continuity plans. Initially, conduct a thorough risk assessment to identify potential threats and vulnerabilities, and develop appropriate control measures based on the prioritization of risks. This includes, but is not limited to, strengthening access control, encrypting sensitive data, and implementing network security measures.

Furthermore, businesses need to establish robust business continuity plans that clearly define critical business functions and processes and develop corresponding measures to ensure that business operations can be quickly and orderly restored in the event of a security incident or disaster. The content of business continuity plans should comprehensively cover aspects such as employee safety, equipment recovery, communication restoration, and supply chain management.

To verify the effectiveness and feasibility of these plans, businesses need to conduct regular drills and tests. By simulating security incidents or disaster scenarios, the performance of business continuity plans in actual emergency situations can be tested, allowing for timely adjustments and enhancements to the plans, enhancing the ability to handle future risks. This comprehensive risk response and business continuity planning will help businesses better cope with potential threats and ensure the stable operation of the business.

5. Conclusion

In the context of digital transformation, businesses face increasing data security risks. By identifying and understanding these risk factors, businesses can implement appropriate management strategies to protect their data assets. This article has discussed technological and organizational factors impacting risk, along with methods for assessing and identifying these risk factors. Additionally, preventive measures, monitoring and detection, and emergency response and recovery strategies have been proposed to help businesses effectively manage data security risks. By comprehensively applying these management strategies, businesses can better withstand various security challenges faced during digital transformation, ensuring the confidentiality, integrity, and availability of data.

References

[1] Lu Ning. Exploration of Digital Financial Models for Port Enterprises Under the Background of Big Data[J]. Today's Wealth (China Intellectual Property), 2023(06):146-148.

[2] Huang Zizun, Zou Kai. Identification of Factors Affecting Enterprise Data Security Risks in the Context of Digital Transformation[J]. Science and Technology Advisory, 2023(04):41-48.

[3] Lin Lu. Research on Data Compliance Marketing Internal Control System for Power Enterprises Under the Background of Digital Transformation[J]. Price Theory and Practice, 2023(01):194-198.

[4] Zhang Hao. Enterprise Digital Transformation Pathways Under the "Dual Carbon"Background[J].Modern Enterprise Culture, 2023(05):40-42.

[5] Yang Mengyuan, Wu Chang. Research on Digital Transformation of Small and Medium-sized Private Manufacturing Enterprises Under the Background of Common Prosperity—A Case Study of Enterprises in Yueqing City[J]. Journal of Wuhan Business University, 2022, 36(05):35-40.