GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Journal of Computer, Signal, and System Research

Article

Research on the Design of Corporate Office Data Security Protection Systems

Yu Pan [1,*]

[1] Matthews Real Estate Investment Services, El Segundo, California, 90245, USA
* Correspondence: Yu Pan, Matthews Real Estate Investment Services, El Segundo, California, 90245, USA

Abstract: With the rapid development of information technology, the security of enterprise office data has become particularly important. Frequent data security incidents, such as data leaks, network attacks, internal threats, etc., pose a huge threat to enterprise business operations and reputation. In response to these challenges, it has become particularly urgent to build a comprehensive enterprise office data security protection system. This article analyzes the current status of enterprise data security protection systems, conducts in-depth research on the security challenges faced by enterprises, and proposes a design concept that integrates multi-layer protection strategies and technological innovations to enhance the security of enterprise data. The research results aim to provide a theoretical basis and practical guidance for security construction during enterprise informatization. They also seek to help enterprises effectively resist various security risks and ensure the integrity of data and information.

Keywords: enterprise office data; data security; protection system; protective measures; information safety

Received: 05 March 2025
Revised: 11 March 2025
Accepted: 14 April 2025
Published: 18 April 2025

1. Introduction

Under the promotion of digital reform and information construction, office data of enterprises is gradually transformed into critical resource wealth, but with it comes the increasingly prominent challenge of data security. External threats, such as data breaches, cyber-attacks, and malicious software, pose unprecedented risks to enterprise data. Data leakage and exploitation may not only result in financial losses, but also have a negative impact on the company's image and market position. Therefore, building an efficient and reliable data security protection system has become an important issue that enterprises must immediately face [1]. Although many enterprises have deployed various data security management strategies and technical measures, the current data protection system still struggles to fully resist rapidly developing technologies, increasingly complex network attack methods, and insufficient employee awareness of security.

2. Types of Enterprise Office Data Security Protection Systems

Enterprise office data security protection systems cover four main areas: physical security, network security, application security, and data security [2]. Physical security focuses on the protection of devices and their storage media to prevent the loss or theft of data. Network security relies on strategies such as firewalls and intrusion detection technologies to resist external attacks and unauthorized access. Application security is committed to ensuring the stability of enterprise software during runtime, preventing interference from security vulnerabilities and malicious behavior. Data security focuses on data encryption, data backup, and access control to ensure that data is not leaked, tampered with, or lost [3]. With the continuous advancement of information technology, enterprises are developing multi-level and all-round strategies for data security protection,

https://doi.org/10.71222/xfbxfw97

aiming to comprehensively defend against various security risks and ensure the security, integrity, and availability of office data [4].

3. Current Status of Enterprise Data Security Protection Systems

3.1. Data Security Protection Measures Lag Behind

Although many enterprises have recognized the urgency of data confidentiality, the security measures currently adopted often cannot keep up with the increasing security risks [5]. A large number of enterprises still adhere to traditional security barriers, such as firewalls and antivirus software, without timely introduction of cutting-edge protection technologies and tools [6]. Faced with complex network attacks and internal security risks, traditional protection strategies often fail to provide effective defense. In addition, some small and medium-sized enterprises have not been able to establish a comprehensive multi-level security protection network due to budget constraints, and often lack sufficient response and recovery measures when encountering data breaches and network attacks. Meanwhile, some enterprises are slow to respond in system upgrades and vulnerability fixes, making them highly vulnerable to hacker attacks. With the continuous advancement of network attack technology and the growing complexity of data security threats, current protection measures are insufficient to meet enterprises' data security needs. There is an urgent need for further improvement [7].

3.2. Insufficient Safety Awareness among Employees

Many companies have failed to provide security education and awareness enhancement to their employees on a regular basis, resulting in employees lacking sufficient attention to the necessity of data confidentiality in their daily work processes. For example, employees often habitually use simple passwords, frequently use the same password, or record passwords in easily accessible locations, which invisibly increases the risk of data leakage. Meanwhile, employees lack the ability to identify network security threats such as phishing emails and harmful programs, making them vulnerable to hacker attacks. Some employees have leaked critical data without permission or stored enterprise data on unencrypted external storage media. Overall, companies overly focus on technical measures in security protection, while neglecting the cultivation and awareness building of employee safety behavior, which leads to significant risks in data security for the company.

3.3. Serious Internal Data Leakage Issues

Internal data breaches are particularly severe in many enterprises. According to the 2019 Enterprise Data Breach Report, the proportion of data breaches caused by internal employees is as high as 68%. This situation exposes the shortcomings of enterprises in terms of permission management, employee behavior supervision, and security training. Table 1 provides a detailed breakdown of the proportion of various internal data breach incidents, providing a more intuitive understanding of the specific situation and severity of data breaches.

Table 1. Proportion of Different Types of Internal Data Leakage Cases.

Source of Data Leakage	Proportion (%)
Malicious leakage by internal employees	45
Internal staff negligence in operation	23
Partner or third-party leakage	15
Senior management personnel abuse their authority	10
other	7

According to the detailed data analysis recorded in Table 1, enterprise security breaches are mainly caused by malicious behavior or negligence of internal employees, reflecting that there are still significant security risks in internal management of the enterprise.

3.4. Data Encryption Technology Is Not Widely Used

Data encryption is a key measure for information security, but its application is not widely adopted in the data protection strategies of many enterprises. Especially for small and medium-sized enterprises, the lack of professional security personnel and expensive investment in technology often lead to insufficient attention to the encryption processing of sensitive data. Even in some large enterprises, although critical data and communication information are encrypted, they are often limited to individual regions or departments, resulting in a lack of encryption for the data that many employees come into contact with on a daily basis, making them vulnerable to security attacks. At the same time, enterprises lack consistent standards and regulatory guidance when selecting and implementing encryption technologies, resulting in scattered encryption strategies and increasing the difficulty and risk of security management. Therefore, even data that has been encrypted remains vulnerable to cracking or leakage during transmission and storage, especially when encryption standards are inconsistent.

3.5. Increased External Threats and Security Attacks

In the internet environment, with the advancement of attack techniques and the rise of cybercrime, external threats pose an increasingly serious challenge to enterprise data security. Recently, malicious activities such as ransomware, DDoS attacks, phishing attacks, etc. have emerged one after another, causing significant financial losses and reputational damage to enterprises. Especially in the process of gradually implementing digital work models in enterprises, the possibility of network infringement has significantly increased. Criminals invade the enterprise network by discovering system vulnerabilities, implanting malicious code, and other means, stealing important data or interfering with core business. Faced with frequent and ever-changing external attacks, traditional security measures such as firewalls and intrusion detection that many enterprises rely on often cannot provide sufficient protection. As a result, external security threats are escalating, severely impacting the information resources and business operations of enterprises.

3.6. Increased Legal Compliance Pressure

With the gradual tightening of laws related to data confidentiality and security, the legal compliance pressure faced by enterprises has significantly increased. Recently, legal norms for data protection have been continuously strengthened around the world, especially with the implementation of the EU General Data Protection Regulation (GDPR) and various national cybersecurity laws, which have put forward more stringent conditions for enterprises on how to handle and protect data. If a company fails to meet these legal standards, it may not only face heavy penalties, but also lose public image and consumer trust. In view of this, enterprises need to enhance their level of data security protection, strictly comply with data protection legal requirements, and avoid legal risks in increasingly strict compliance situations. In addition, with the continuous updating of laws and regulations, enterprises also need to constantly refresh policies and strengthen employee education to maintain overall compliance status.

4. Design Ideas for Enterprise Office Data Security Protection System

4.1. Strengthen Multi-Level Defense Mechanisms

In the process of designing data security protection systems, enterprises need to establish multi-level defense mechanisms to resist constantly upgrading security challenges. This level of defense system sets multiple defense levels, each with its own unique protection tasks, and works together to minimize risks and hidden dangers.

At the network layer, enterprises set up firewalls and intrusion detection systems (IDS) to intercept illegal intrusions and irregular data transmissions by continuously monitoring data flows. As for the user terminal layer, enterprises ensure that the computers, mobile phones, and other devices used by employees are updated with the latest security features by equipping them with cutting-edge security applications and implementing device management policies to resist the invasion of malicious programs and viruses. At the application layer, enterprises utilize specialized program vulnerability detection and repair tools to quickly patch security vulnerabilities in systems and software, preventing external attackers from infiltrating through these vulnerabilities.

At the information layer, enterprises implement encryption protection for all critical information and establish strict information access management systems to ensure that only authorized individuals can access and modify sensitive data. In addition, companies strengthen their internal review processes and regularly audit monitoring data access records to identify and contain potential internal data leakage threats in a timely manner. With the help of multi-level security defense mechanisms, enterprises can effectively resist security risks caused by external attacks, internal leaks, and technical defects, thereby ensuring the security of enterprise data throughout its entire lifecycle.

4.2. Strengthen Employee Data Security Awareness and Behavior Management

Strengthening employees' awareness and behavior management of data security is a core step in ensuring enterprise data security. Despite the continuous improvement of technological defense measures, employee misconduct remains the main cause of data breaches and security incidents. Faced with this challenge, enterprises must start from various aspects such as employee education and training, code of conduct, and supervision mechanisms to create a sound data security culture.

In the process of designing data security protection, emphasis should be placed on deepening the training of employees' security awareness, focusing on practical security risks and preventive measures. Enterprises regularly conduct data security education courses to ensure that all employees are aware of various security risks (such as phishing attacks, malicious software, internal data leaks, etc.) and corresponding preventive measures. After the training, employees must complete a network test to verify whether they have mastered the necessary security protection knowledge. At the same time, the company has established clear guidelines for employee behavior. Employees are required to follow strict security operating procedures when processing company data, such as using complex passwords, avoiding clicking on links from unknown sources, and not storing critical data on unauthorized devices.

In addition, the enterprise is building a regulatory system based on behavior analysis to monitor employee actions in real-time during data processing. If abnormal behavior is detected, such as repeated copying of critical data or illegal login to the system, the system will automatically trigger an alert and submit it for professional review to identify potential security risks. This type of monitoring system not only enhances employees' awareness of security issues, but also enables companies to promptly identify and address internal security risks. With the help of this comprehensive employee security management system, enterprises not only enhance employees' awareness of security precautions, but also effectively ensure data security and reduce risks.

4.3. Implementation of Data Encryption and Protection

Data encryption is a key means of ensuring that critical information of enterprises is not leaked during storage and transmission. Enterprises need to integrate encryption methods and data protection strategies to create comprehensive data security protection. Encryption measures need to be applied to all core data, such as employee personal information, consumer data, financial reports, etc., to ensure that data can be properly protected in any form (whether stored, transmitted, or processed).

When encrypting sensitive customer data stored in the cloud, a strategy combining symmetric encryption and public key encryption is adopted. All data to be stored will undergo a symmetric encryption operation using a specific key before being sent to the cloud. During the data transmission phase, SSL/TLS encryption transmission protocol is used to enhance data protection and prevent data from being intercepted and stolen during transmission. In addition, a two-factor authentication system is implemented to ensure that only authorized personnel can decrypt and query sensitive data.

In the specific process of performing encryption and decryption, this process can be represented by the following formula: $C = E(K, P)$.

Among them: C represents ciphertext (encrypted data); E representing encryption algorithms; K representing the encryption key; P represents plaintext data (raw data). By using encryption methods, enterprises not only ensure the security of data, but also avoid the serious losses that may be caused to the enterprise in the event of data leakage.

4.4. Improve Data Backup and Disaster Recovery Mechanisms

In the process of enterprise office data security protection system, data backup and disaster recovery mechanism are key parts to deal with emergencies and ensure data persistence and availability. Whether it is natural disasters, system failures, or operational errors, data loss or damage can have a significant negative impact on the normal operation of enterprises. In view of this, enterprises need to develop efficient backup and recovery plans so that they can recover data in real time in the event of disasters, shorten business downtime, and reduce financial losses.

Design a comprehensive data backup and disaster recovery mechanism in the data protection system. Enterprises need to implement regular backup operations on core data (such as financial statements, consumer information, contact information, etc.) and store these data in multiple geographically different backup centers through a distributed backup strategy.

In daily work, data is automatically backed up to local servers and cloud storage. Perform a full back up once a week and implement incremental backups daily to reduce potential data loss during the recovery process. In the face of system failures or data loss emergencies, the information technology department of the enterprise prioritizes restoring data from local backups according to a pre-established recovery plan, and then compares it with cloud backups to ensure data integrity and consistency. After verified data recovery, it can be reintroduced into the production environment to ensure the continuity of enterprise business. This design ensures that even in extreme cases of data damage or equipment failure, enterprises can quickly resume operations, prevent long-term business shutdowns, and significantly reduce the risks caused by recovery delays. By periodically testing and improving backup and recovery plans, enterprises ensure effective control over data recovery capabilities, thereby ensuring uninterrupted business operations and data security.

4.5. Strengthen Compliance and Legal Risk Management

In response to increasingly stringent data privacy regulations, such as the EU GDPR and various national cybersecurity laws, companies establish compliance management teams whose task is to monitor updates to laws and regulations in real-time and evaluate their data protection measures to confirm their compliance with regulations. To strengthen compliance, the company has implemented periodic data protection and privacy education for all employees and requires each employee to sign a Data Protection Agreement to clarify their responsibilities in data processing. At the same time, the company hires external legal experts to periodically review its data security strategy, ensuring that all processes and technological applications of the company are consistent with the latest legal standards.

To efficiently manage legal risks, the enterprise develops a hierarchical data management plan and enforces strict permission management for all key data (such as consumer privacy, financial records, etc.) to ensure that only authorized personnel have access. During data transmission and storage, enterprises apply encryption methods to enhance data security and prevent potential legal and economic risks associated with data leakage. By maintaining a high level of openness in the field of data security, companies reduce the likelihood of lawsuits and penalties for violating laws and regulations, and enhance consumer and market trust in the company.

4.6. Adopting Intelligent Security Protection Technology

Faced with the continuous evolution of network attack technology, traditional protection strategies seem inadequate, and the application of intelligent protection technology is particularly crucial. When designing an office data security system, an intrusion detection and defense system (IDS/IPS) integrated with artificial intelligence is adopted. This system utilizes advanced machine learning technology to monitor network traffic in real-time, capture abnormal activities and potential attack behaviors in a timely manner, and analyze changes in attack patterns in depth. In the attack simulation test, the system demonstrated its powerful ability to automatically detect unknown malicious IPs and quickly issue warnings to administrators. Thanks to this technology, enterprises can anticipate and warn of upcoming security risks, and automatically implement protective measures such as isolating malicious IPs, controlling abnormal traffic, and effectively avoiding data leaks or system intrusions.

In addition, enterprises use advanced intelligent encryption technology, relying on big data analysis and adaptive encryption strategies to change the level and method of encryption in real time. For example, during the process of sending data through an external network, the system will automatically determine the sensitivity level of the data and use high-strength encryption methods. In the data exchange among internal employees of the enterprise, moderate encryption methods are used to ensure business smoothness while achieving data confidentiality as much as possible. With the help of these intelligent technological means, enterprises can more accurately and efficiently respond to changing security threats, thereby enhancing the overall level of data security protection.

5. Conclusion

With the rapid development of information technology, enterprises are facing unprecedented data security challenges, especially in terms of security measures, employee security awareness, and prevention and control of internal data leaks. Enterprises can establish a more robust security protection mechanism by building multi-level defenses, strengthening employee management, implementing data encryption and disaster recovery strategies. In addition, compliance requirements and the use of intelligent security technologies are particularly crucial. By continuously improving data security management, enterprises can not only effectively resist complex security threats, but also enhance customer trust and ensure the sustainable development of their business. In the future, enterprises need to continuously enhance their data security management capabilities to adapt to the constantly changing security environment and ensure the security and integrity of information assets.

References

1. P. Li and L. Zhang, "Application of big data technology in enterprise information security management," *Sci. Rep.*, vol. 15, no. 1, p. 1022, 2025, doi: 10.1038/s41598-025-85403-6.
2. G. A. P. Rodrigues, A. L. M. Serrano, G. F. Vergara, R. D. O. Albuquerque, and G. D. A. Nze, "Impact, compliance, and countermeasures in relation to data breaches in publicly traded US companies," *Future Internet*, vol. 16, no. 6, p. 201, 2024, doi: 10.3390/fi16060201.

3. M. R. Uddin, S. Akter, and W. J. T. Lee, "Developing a data breach protection capability framework in retailing," *Int. J. Prod. Econ.*, vol. 271, p. 109202, 2024, doi: 10.1016/j.ijpe.2024.109202.
4. A. P. Rodrigues *et al.*, "Understanding data breach from a global perspective: Incident visualization and data protection law review," *Data*, vol. 9, no. 2, p. 27, 2024, doi: 10.3390/data9020027.
5. Y. Xu, G. Xu, Y. Liu, Y. Liu, and M. Shen, "A survey of the fusion of traditional data security technology and blockchain," *Expert Syst. Appl.*, p. 124151, 2024, doi: 10.1016/j.eswa.2024.124151.
6. M. Tahmasebi, "Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises," *J. Inf. Secur.*, vol. 15, no. 2, pp. 106–133, 2024, doi: 10.4236/jis.2024.152008.
7. M. M. Nair, A. Deshmukh, and A. K. Tyagi, "Artificial intelligence for cyber security: Current trends and future challenges," in *Autom. Secure Comput. Next-Gener. Syst.*, pp. 83–114, 2024, doi: 10.1002/9781394213948.ch5.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of GBP and/or the editor(s). GBP and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.