Journal of Electronic Research and Application, 2025, Volume 9, Issue 3
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Research on Cybersecurity Threats and Defenses in the Context of Financial Technology

Sishan Li[1], Wei Li[2]*

[1]China Railway Trust Co., Ltd, Chengdu 610021, Sichuan, China
[2]China Railway Academy Co., Ltd, Chengdu 610032, Sichuan, China

**Author to whom correspondence should be addressed.*

Abstract: With the rapid development of information technology, the deep integration of the financial sector and the internet has become a key driving force for economic growth. However, while this trend brings convenience, it also poses significant cybersecurity challenges to the financial sector. This study comprehensively analyzes the current state, challenges, and protective measures of cybersecurity in the financial sector, aiming to provide important references for financial institutions in formulating cybersecurity strategies and enhancing risk management.

Keywords: Financial sector; Cybersecurity; Protective measures; Data security

Online publication: 29 May, 2025

1. Introduction

The integration of the financial industry and the internet has deepened, bringing significant convenience and new development opportunities to the financial sector. At the same time, cybersecurity risks have gradually emerged, becoming a key factor restricting the further development of the financial industry. The security of financial sector network systems not only concerns the operational stability of financial institutions but also closely relates to the national economic security, social stability, and the safety of the public's assets [1].

Cybersecurity incidents in the financial sector, including cyberattacks, system vulnerabilities, and data breaches, occur frequently. These incidents not only cause significant economic losses to financial institutions but also seriously endanger the property safety of a large number of users. Cybersecurity issues pose a great challenge to the stable operation of the financial industry. Therefore, ensuring the security of network systems in the financial sector and preventing and responding to various cybersecurity threats have become important issues currently facing the financial industry [2].

With the rise of the "Internet + Finance" model, research on information security risk prevention has become particularly important. The information security risks in this model exhibit diversified and complex characteristics, including network risks, technical vulnerabilities, and other practical issues. Therefore, it is necessary to focus on

these issues as entry points, exploring ideas and specific measures for risk prevention, to provide strong guarantees for the healthy development of the financial industry [3].

In-depth research on cybersecurity issues in the financial sector is crucial for maintaining the steady progress of the financial industry. It not only enhances the cybersecurity defense capabilities of financial institutions, reducing potential economic losses, but also ensures a safer and more reliable financial service experience for a wide range of users. At the same time, these research findings can provide decision-making support for the government and relevant regulatory bodies, promoting the sustainable development of the financial industry [4].

2. Financial cybersecurity current situation and challenges

2.1. Analysis of the current situation of financial cybersecurity

The cybersecurity situation in the financial sector is becoming increasingly severe. This current state is attributed both to the acceleration of the online and mobile trends in financial services and to the continuous innovation of hacker attack methods.

With the online and mobile transformation of financial services, the volume of financial transaction data has surged, and the attack surface for cyber threats has expanded accordingly. Today, the vast majority of financial transactions are conducted online, including online banking transfers, mobile payments, stock trading, and more. While this shift provides significant convenience to customers, it also increases the risk of cybersecurity issues. With large amounts of transaction data and customer information being transmitted over networks, if security measures are inadequate, this information is highly vulnerable to theft or tampering by hackers [5].

Hacker attack methods are continuously evolving, ranging from traditional viruses and Trojan attacks to new types of attacks such as advanced persistent threats (APT) and ransomware. These new types of attacks are often more covert and difficult to detect with traditional security measures. For example, advanced persistent threats (APT) can steal sensitive information from financial institutions through long-term infiltration and penetration, posing a significant threat to financial network security [6].

Issues such as weak internal security awareness and inadequate protective measures in financial institutions have also exacerbated cybersecurity risks. Some financial institutions, in their pursuit of business development, have overlooked the importance of cybersecurity, resulting in vulnerabilities in their protective systems and leaving opportunities for hackers. At the same time, the lack of security awareness among some employees, such as casually clicking on unknown links or downloading unknown files, can also lead to the infiltration of viruses or Trojans [7].

The current state of cybersecurity in the financial sector is far from optimistic. In the face of this situation, financial institutions must strengthen security measures and raise employee awareness and vigilance regarding cybersecurity to effectively address the escalating risks and challenges. At the same time, regulatory bodies should increase their oversight of the cybersecurity practices of financial institutions, ensuring that while business development progresses, customer information and transactions are secure and proceed smoothly [8,9].

2.2. Challenges facing financial cybersecurity

Financial cybersecurity is facing unprecedented challenges in the current digital era. These challenges mainly stem from the rampant external attacks, frequent internal threats, outdated technological updates, and the inadequacy of laws and regulations.

In terms of external attacks, the financial sector is a primary target for hackers, facing various types of cyber threats. Hackers exploit vulnerabilities to launch attacks, steal sensitive data, and compromise system integrity,

resulting in significant economic losses and reputational risks for financial institutions. For example, in recent years, phishing attacks and ransomware attacks targeting banks, securities firms, insurance companies, and other financial institutions have become frequent, highlighting the vulnerabilities of financial cybersecurity in responding to external attacks [10–12].

Internal threats are also a significant concern. Employees within financial institutions may cause security issues such as data breaches and system outages due to operational mistakes or weak security awareness. Additionally, there have been instances where internal personnel collude with external attackers, further complicating the cybersecurity challenges in the financial sector. Therefore, strengthening internal security management and raising employee security awareness have become urgent issues that financial institutions need to address [13].

In terms of technological updates, the insufficient investment in cybersecurity technology and personnel training within financial institutions makes it difficult for them to effectively respond to the constantly evolving cyber threats. As the trend of online and mobile financial services accelerates, traditional cybersecurity measures can no longer meet current demands. Therefore, financial institutions need to continuously adopt new technologies, strengthen technological innovation, and enhance their cybersecurity capabilities. Additionally, increasing the training and recruitment of cybersecurity professionals is key to improving the level of financial cybersecurity [14].

In terms of laws and regulations, although China has continuously improved its legal and regulatory framework for financial cybersecurity in recent years, some challenges and deficiencies remain. For example, the enforcement of relevant laws needs to be strengthened, the division of responsibilities among regulatory bodies is not clear enough, and there is a lack of legal regulation on new security issues such as cross-border data flows. Therefore, further improving financial cybersecurity-related laws and regulations, strengthening regulatory efforts, and increasing the cost of violations are of great significance in safeguarding financial network security [15].

The challenges facing financial cybersecurity are multifaceted and require the joint efforts of financial institutions, regulatory bodies, technology providers, and other stakeholders to form a collective force to effectively respond. In this process, strengthening international cooperation is also an indispensable part. By sharing information and collaborating, we can jointly address global financial cybersecurity challenges.

3. Financial cybersecurity protection measures

3.1. Cybersecurity technology protection

In terms of cybersecurity technology protection, financial institutions need to adopt a series of effective measures to ensure the safe and stable operation of financial systems. In addition to strengthening the application of cybersecurity technologies such as firewalls, intrusion detection, and security auditing, attention should also be given to the implementation of strategies such as data encryption and backup recovery.

Data encryption is a key measure to ensure the security of data during transmission and storage. Financial institutions need to employ high-strength encryption technologies to protect sensitive information, ensuring the security of data during transmission and storage and preventing it from being illegally accessed or tampered with. The application of encryption technologies should also be customized according to specific business scenarios and needs to achieve the best security outcomes.

Additionally, backup and recovery strategies are an important part of cybersecurity protection. Financial institutions should establish a comprehensive backup system, regularly backing up critical data while verifying the completeness and availability of the backup data. In the event of data loss or corruption, the backup should be immediately activated to ensure the continuous, smooth, and reliable operation of business activities.

With the continuous development of technologies such as cloud computing, big data, and artificial intelligence [15], financial institutions can actively explore the application of new technologies in cybersecurity protection. For example, by utilizing the elastic scalability and high availability features of cloud computing, financial institutions can enhance the disaster recovery capabilities and data processing efficiency of financial systems. Additionally, big data analysis and artificial intelligence technologies can be used to achieve precise early warning and intelligent defense against cyberattacks.

Cybersecurity technology protection is not a one-time solution. Financial institutions need to regularly assess and adjust their security strategies to adapt to the constantly changing cybersecurity threat environment. At the same time, strengthening collaboration with technology service providers and security organizations, and quickly acquiring the latest security information and protective measures, is also an important way to improve cybersecurity defense capabilities.

Financial cybersecurity technology protection requires the comprehensive use of various technological methods and strategies to build a comprehensive and multi-layered security defense system. By continuously strengthening technological innovation and collaboration, financial institutions can better address cybersecurity challenges and ensure the safe and stable operation of financial systems.

3.2. Personnel management and training

Personnel management plays a crucial role in financial cybersecurity. Financial institutions must deeply recognize that employees are not only important assets to the organization but may also pose potential security risks. Therefore, strengthening security awareness training and education for employees is particularly important.

Financial institutions should regularly organize cybersecurity education and training, using methods such as case studies and practical simulations to deepen employees' understanding of cybersecurity and teach them how to prevent potential cyber threats in their daily work. The training content can cover various areas, such as phishing and social engineering, to enhance employees' awareness and ability to respond.

Financial institutions should establish a comprehensive security management system and processes. This includes, but is not limited to, access control for sensitive data, secure configuration of devices, and emergency response mechanisms. By clearly defining security regulations and operational procedures, financial institutions can standardize employee behavior and reduce security risks caused by human errors.

In addition to training and management systems, financial institutions should also strengthen background checks and reviews during the recruitment process. By thoroughly understanding the employee's past experiences, professional ethics, and integrity, financial institutions can select employees who possess a high sense of responsibility and awareness of honesty, thereby further reducing the risk of internal information leakage.

Personnel management is not a one-time task but a long-term process that requires continuous investment and attention from financial institutions. By continuously optimizing training content, updating management systems, and strengthening employee background checks, financial institutions can create a safer and more stable network environment, providing strong support for the smooth operation of financial services.

4. Conclusion

In this study, an all-encompassing analysis of cybersecurity issues in the financial sector has been conducted, deeply exploring the current situation and challenges, and providing a detailed analysis of protective measures.

These efforts aim to reveal the underlying issues in financial cybersecurity and provide effective strategies for financial institutions to address them. It is believed that this paper will help financial institutions strengthen cybersecurity protection, safeguard user information, and promote the healthy and stable development of the financial industry.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Dong B, 2000, Prevention and Guarantee of Financial Network Security. Internet Weekly, (33): 35.

[2] Chen X, Guo Z, Hu Y, et al., 2024, Application Practice of National Data Security Standards in Financial Field. Information Technology & Standardization, (S1): 151–155.

[3] Luo T, 2018, Research on Information Security Risk Prevention under "Internet + finance" Mode. Digital World, (7): 338.

[4] Xie E, Huang X, Zhou Y, 2015, Analysis of Network Security and Information Security Elements in Internet Finance. Journal of Shanghai University (Social Sciences Edition), 32(4): 27–36.

[5] Tang H, 2019, Analysis of Network Security Risks in Financial Information Systems. Tsinghua Financial Review, (1): 42–44.

[6] Jiang C, 2006, Analysis and Reflection on Network Security of Financial System. Water Resources and Electric Power Machinery, 28(6): 69–70.

[7] Tong J, 2023, Analysis and Countermeasures of Network Security Risks in Financial Industry under New Situation. Information Industry Report, (5): 73–75.

[8] Pang E, 2022, Analysis of Current Situation and Countermeasures of Network Financial Security. Security & Informatization, (10): 7–9.

[9] An Q, 2016, Discussion on Current Situation and Countermeasures of Internet Finance. Decision & Information, (33): 1.

[10] Ji H, 2023, Threat Analysis and Response Strategies for Network Security Risks in Financial Services. Information Security and Communications Privacy, (12): 105–113.

[11] Song X, Li P, Zhang L, 2022, Research on Financial Network Security Resilience Regulation in China: Practical Dilemma, British Experience and Institutional Construction. Journal of Intelligence, 41(3): 80–86 + 94.

[12] Yu X, Chen M, 2024, Security Analysis and Optimization of Electronic Payment in Network Financial Environment. Finance, 14(4): 1518–1523.

[13] Yin Q, 2003, Strengthening Network Security to Prevent Financial Risks: On Network Security Management of Grassroots Banks. Financial Computerization, (6): 61–62.

[14] Yin Y, 2016, Research on Risks and Prevention of Internet Finance in China, thesis, Tianjin University of Finance and Economics.

[15] Wu Q, Xu H, Zhao Y, et al., 2018, Intelligent Emergency Rescue System and Application for Mine Water Disaster Based on Cloud Platform. Journal of China Coal Society, 43(10): 2661–2667.