American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 05 2025
PAGE NO. 21-25
DOI 10.37547/ajast/Volume05Issue05-06

Cybersecurity in Financial Technologies: Current Threats, Methods of Protecting User Data, And Ensuring Business Security

Aigerim Sydykova
PhD student, South Korea

Received: 09 March 2025; **Accepted:** 05 April 2025; **Published:** 08 May 2025

Abstract: The first decades of the energy-information era are marked as a period of digital transformation, accompanied by the large-scale digitalization of key sectors. The financial sector stands at the forefront of this global movement. The rapid development and implementation of modern digital financial technologies present great opportunities for business growth and expansion. At the same time, advanced technologies and innovations adopted in the industry are not always fully protected from various threats. This article explores the current cyber threats typical for the fintech sector, methods of protecting users' personal data, and strategies for ensuring business cybersecurity. It analyzes modern cybersecurity tools and best practices. Special attention is paid to the scientific novelty in the application of artificial intelligence and machine learning. The article concludes that a comprehensive approach to cybersecurity is essential as a strategic element in the development of fintech businesses. The purpose of this article is to examine current threats, analyze data protection methods in the fintech sector, and develop recommendations for ensuring business resilience in cyberspace.

Keywords: Financial technologies, cybersecurity, data protection, digital threats, business security, artificial intelligence, cryptography, machine learning.

Introduction:

The introduction of modern digital financial technologies has radically transformed the way financial services are delivered, enabling faster and more efficient processes in payments, lending, insurance, and investment. This has significantly improved customer service quality and operational efficiency across businesses. However, large-scale and accelerated digitalization is also accompanied by an increase in cyber threat risks. Fintech companies, which process vast amounts of confidential data, have become prime targets for cybercriminals. The illegal activities of individual hackers and organized hacker groups directed at companies and their clients result in substantial financial losses, reputational damage, and legal consequences. The growing popularity of fintech applications has been accompanied by a rise in cyber threats, including attacks on payment systems such as transaction data interception, credential theft via malware, and phishing attacks. Among the widely used malicious software (malware) by criminals are spyware and ransomware targeting mobile apps and digital wallets to extort money.

One of the most notorious cases was the large-scale WannaCry ransomware attack, which exploited vulnerabilities in the Windows operating system to infiltrate computer systems, encrypt all data, and demand ransom for decryption. This attack paralyzed the operations of banks, government agencies, and airports. The virus was stopped by researcher Marcus Hutchins, also known as Malwaretechblog, who noticed that before encrypting files, the program attempted to contact a non-existent domain. Hutchins registered this domain, causing WannaCry to cease its malicious activity.

Another example includes Man-in-the-Middle (MITM) attacks, which occur due to insufficient protection of communication channels, allowing attackers to intercept data exchanged between users and servers. Social engineering methods, where cybercriminals deceive users to gain access to their credentials, are also among the most common threats.

Internal threats also pose significant risks—these are actions by dishonest employees or accidental staff errors that result in data leaks.

It resembles an ongoing race between fintech companies and the criminal world: while one side constantly upgrades its systems and protection methods, the other relentlessly searches for vulnerabilities in their targets' infrastructure and software. According to research, the global cybersecurity market is expected to reach $195 billion over the next four years, with an average annual growth rate of 22.4%.

As a result, the need for a systematic approach to continuously improve and apply comprehensive methods to protect users and businesses becomes increasingly relevant in the face of ever-growing cyber threats.

Cybersecurity in Financial Organizations

Ensuring the reliable protection of information and infrastructure is an integral part of any financial organization's strategy. Every company generates large volumes of information that require protection. Confidentiality requirements may be defined by legislation—such as banking secrecy or personal data protection—or by the company's internal policies, especially regarding trade secrets. Developing effective cybersecurity measures not only safeguards sensitive data but also prevents financial losses, maintains customer trust, and ensures compliance with regulations.

In this regard, the protection of confidential data is a top priority for financial institutions. The problem is exacerbated by the fact that the volume of stored and transmitted sensitive information increases significantly with the growth of digital technologies and the transition to online platforms. In such conditions, it is crucial to guarantee that clients' personal data, bank account details, and other sensitive information are reliably protected from unauthorized access, theft, or leaks.

Clients of financial institutions expect their money and personal information to be securely protected. Maintaining a high level of cybersecurity helps preserve customer trust and increase satisfaction with financial services. Clients are more likely to choose organizations that offer the highest level of security and data protection.

Today, cybersecurity is an integral part of national security. Financial companies are subject to strict regulatory and legislative requirements in the field of cybersecurity. Compliance with laws and standards not only protects customer data but also helps avoid fines and legal issues related to improper processing and storage of confidential information.

There are numerous cyber threats and types of attacks in the financial sector that can have serious consequences for companies and their clients. Understanding these threats is a crucial step toward developing effective cybersecurity strategies. Let us look at the most common techniques used by hackers:

- Phishing attacks rank at the top of this list. These are fraudulent attempts by cybercriminals to obtain confidential information such as logins, passwords, and banking details by disguising themselves as trusted sources—emails or websites of financial institutions. This type of attack is one of the most common and continues to gain popularity among attackers.
- Social engineering refers to manipulative tactics used by attackers to deceive individuals and gain access to sensitive information or systems. In the financial sector, this may involve accessing bank accounts, financial records, or other critical data.
- Malware is one of the most serious threats in the financial sector. These are software programs designed to harm computer systems, networks, and data. Malware can be used for information theft, financial fraud, or to disrupt normal company operations.
- DDoS attacks (Distributed Denial of Service) aim to overload servers and network infrastructure, causing online services to become temporarily unavailable and potentially resulting in significant losses for both companies and clients.
- API attacks: In modern banking, APIs (Application Programming Interfaces) are widely used for data exchange and system integration. However, APIs also introduce new vulnerabilities that can be exploited by attackers. These include bypassing authentication mechanisms or injecting malicious data to disrupt banking systems.
- AI-related crimes: Recent advances in artificial intelligence have brought new threats. The outcome of AI models depends on input data, which opens the possibility for attackers to manipulate this data and disrupt AI functioning.

Such vulnerabilities have been experimentally confirmed—for example, adding noise to an input image caused a neural network to misclassify it. Humans could hardly distinguish the modified image from the original, but in practice, such an attack would still require access to the internal AI system.

Moreover, the development of generative AI introduces a new danger. Criminals can use publicly available photos and voice recordings to generate realistic images and audio messages, making scams more convincing. In one experiment, a researcher successfully passed voice authentication at Lloyds Bank using an AI-generated voice recording. According to research by Signicat, 6.5% of fraud attempts now involve deepfakes.

A recent incident saw attackers gain access to the popular YouTube channel LinusTechTips through a phishing email, despite two-factor authentication. At the time, the channel had over 15 million subscribers. The hackers renamed it to resemble Tesla's official channel and launched a livestream where Elon Musk allegedly promoted a crypto giveaway. A QR code was displayed, encouraging viewers to send cryptocurrency and receive double the amount in return. The billionaire's voice was, of course, AI-generated. Due to the channel's popularity, the livestream quickly trended on the platform, amplifying the scam. The attackers reportedly earned around $14,000 in Bitcoin and Ethereum.

Cybersecurity Framework and Strategy

Implementing effective cybersecurity measures is essential for minimizing risks and protecting clients' confidential data. Each threat described above can be countered with appropriate solutions. Company leadership must develop and implement a cybersecurity framework. This document forms the foundation for internal regulations and protective systems. Often, external information security experts are engaged to audit the company's IT infrastructure, organizational structure, and business processes and develop a tailored protection plan.

A company's information security concept should include:

- Identification of data assets that require protection, including legal or business-based justifications. This involves cataloging software tools, physical and electronic data carriers, assessing their value and sensitivity, and determining employee access levels.
- Core information protection principles, typically confidentiality, business feasibility, and legal compliance. These guide the development of security policies and infrastructure.
- A threat model tailored to the company and its units, and a hypothetical adversary model (e.g., competitors, hackers, or internal insiders).
- Security requirements for the system and its components, based on business process analysis, system architecture, and risk models.
- Specific methods and tools for information protection.

The strategy alone does not resolve the issue of employee accountability for mishandling data. To address this, a set of organizational security measures must also be implemented. These include policy awareness training, signed agreements, and inclusion of confidentiality clauses in employment contracts.

Employee training is vital. Regular cybersecurity education increases awareness of potential threats and improves the ability to detect suspicious activity. Teaching employees to identify phishing attempts can prevent serious consequences and is also effective against social engineering.

Reporting suspicious behavior to cybersecurity teams and colleagues ensures that everyone is informed in case of a threat.

Multi-factor authentication (MFA) is a security method that requires multiple forms of identity verification before granting access to a system or resource. Even if one factor is compromised, MFA helps maintain protection. This is especially effective if an employee enters credentials into a phishing site or falls victim to social engineering.

Software updates are essential. New versions often contain patches for vulnerabilities. Timely updates of software and antivirus systems help defend against the latest threats and malware.

Zero Trust security model assumes no user or device should be trusted by default, even within a protected network. Its key principles include:

- Identification: All users and devices must be verified.
- Least privilege access: Access is restricted to only what is necessary for a user's role.
- Monitoring and incident detection: Continuous observation helps detect and respond to threats in real-time.

This model enhances protection against modern threats by preventing data leaks and minimizing security incidents.

A leading innovation in cybersecurity is the intelligent threat management system developed by a major bank. It automatically collects, analyzes, and updates data on potential cyber threats. By integrating with internal and external monitoring systems, the platform enriches threat data and models their potential impact on IT infrastructure. Using analytics and machine learning, it prioritizes threats and uncovers hidden correlations. Automation enables rapid detection and response to cyber threats, and round-the-clock DarkNet monitoring ensures proactive control over malicious actors.

Other financial institutions use Security Information and Event Management (SIEM) systems for full real-time visibility and management of incidents. These systems process up to 16,000 events per second, allowing early detection and response before threats escalate.

Any proposed set of measures must be approved across all relevant departments, as budget constraints often limit the scope of cybersecurity programs and software acquisitions.

CONCLUSION

Cybersecurity in the financial sector plays a vital role in protecting clients' confidential data, ensuring the continuity of banking operations, and maintaining public trust in financial institutions.

Information security measures must be reasonable and proportionate; business processes imply that the cost of protecting assets should not exceed their value. Excessive burdens on business operations or staff are counterproductive.

Major threats such as social engineering, API attacks, and phishing require a comprehensive protection strategy that includes employee training, implementation of multi-factor authentication (MFA), regular software updates, and adoption of the Zero Trust security model.

Implementing such measures helps financial institutions minimize the risks associated with cyberattacks and ensures stable operation of banking systems in a constantly evolving environment.

Protecting users' personal data requires advanced technologies and organizational strategies. One of the fundamental methods is encryption, using modern cryptographic algorithms to secure data storage and transmission. MFA also plays a critical role in reducing the risk of unauthorized account access, as do biometric authentication methods.

Secure software development based on SecDevOps principles is also key, ensuring that cybersecurity is integrated at all stages of product creation, thus minimizing vulnerabilities and errors. To protect APIs, techniques such as strong authentication, encrypted transmission, and injection protection are commonly applied.

Monitoring and incident response have become essential elements of security strategies. The use of Intrusion Detection and Prevention Systems (IDS/IPS), Security Information and Event Management (SIEM) platforms, and User and Entity Behavior Analytics (UEBA) enables real-time detection of anomalies and rapid threat response.

As cyber defenses improve, so too do the complexity and sophistication of cyberattacks. Modern companies must employ both technical and organizational security measures. MFA significantly reduces the likelihood of unauthorized access, even when passwords are compromised. Regular updates of operating systems, antivirus software, and corporate applications close known vulnerabilities that attackers might exploit. Implementing encryption for data transmission and storage prevents compromise even in case of leaks.

The human factor remains a weak link in cybersecurity. Regular training and phishing simulations help employees recognize threats and avoid errors. Role-based access control and the principle of least privilege reduce risks of data leaks and insider threats. Routine backups ensure data recovery in the event of ransomware attacks.

A comprehensive cybersecurity strategy must include regular staff training, system audits, and penetration testing. Adherence to international standards such as ISO/IEC 27001 and PCI DSS, along with local data protection laws, is essential.

Promising directions include the use of AI and machine learning for real-time identification of attack patterns and anomalies. Intelligent systems enable adaptive protection mechanisms, minimizing the chances of successful attacks.

To improve business resilience, it is necessary to develop automated incident response systems (SOAR), which speed up decision-making when threats are detected. As quantum computing advances, organizations must prepare for the transition to post-quantum cryptography—standards capable of protecting data from future quantum threats.

Blockchain also deserves special attention as it provides transparency and immutability in transactions, making it a valuable tool for cybersecurity in digital payments and lending systems. Automating incident response through orchestration and defense automation helps reduce reaction time and limit the consequences of attacks. Blockchain technologies can ensure the integrity of transaction records and enhance operational authenticity control.

Investments in post-quantum cryptography are vital for long-term data resilience. Companies must proactively prepare for emerging challenges by developing secure architectures and cultivating a strong culture of cybersecurity among employees and users.

Organizational security measures should begin with developing internal policies, regulations, and protocols. Some of these documents are required by law—such as personal data processing policies that every data operator must publish on their website.

Organizational protection efforts also include:

- Documenting and optimizing business processes
- Assigning access levels based on sensitivity of commercial data
- Creating or appointing dedicated information security units
- Educating and retraining staff
- Running drills to test readiness for critical incidents
- Obtaining licenses (e.g., for handling state secrets)
- Implementing physical security and certification of protection classes
- Securing the supply chain by including confidentiality clauses in contracts
- Issuing identification badges and managing access systems
- Complying fully with data protection legislation
- Establishing procedures for responding to government requests for confidential information

A holistic approach combining technical, organizational, and educational measures ensures fintech companies remain competitive and resilient to cyber threats. Only a systematic and proactive approach to cyber risk management will help preserve client trust and enable long-term growth in the digital economy.

REFERENCES

Социально-гуманитарные риски информационного общества и международная информационная безопасность

монография / А. В. Бирюков, М. Б. Алборова ; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Центр международной информационной безопасности и научно-технологической политики. - Москва : Аспект Пресс, 2021. - 94, [1] с. : ил. - Библиогр.: с. 90-95. - Тираж не указ. - ISBN 978-5-7567-1126-4 : 200 р.

https://cat.gpntb.ru/?id=EC/ShowFull&mfn=1531135&irbDb=KATBW

Вопросы обеспечения безопасности в киберпространстве

Материалы Всероссийской научно-технической конференции, 16 декабря 2022 г. / Министерство науки и высшего образования Российской Федерации, Дагестанский государственный технический университет, МИРЭА - Российский технологический университет. - Махачкала : ДГТУ, 2022. - 397 с. : ил. - Библиогр. в конце докл. - 100 экз. - ISBN 978-5-907698-01-7 : 350 р.

https://cat.gpntb.ru/?id=EC/ShowFull&mfn=1753973&irbDb=KATBW

Кибербезопасность в финансовом секторе https://smartgopro.com/novosti2/cybersecurity_financial_sector/

Информационная безопасность в цифровом мире: современные угрозы и защита

https://smartgopro.com/novosti2/information_security/

Безопасность и анализ корпоративных коммуникаций. Вызовы и решения

Валерий Тучинов, Менеджер по развитию бизнеса компании Aurus.

https://smartgopro.com/novosti2/corporate_communications/

Меры по обеспечению информационной безопасности

https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/mery-po-obespecheniyu-informatsionnoj-bezopasnosti/

Информационная безопасность: вчера, сегодня, завтра

Материалы конференций. - Москва : Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Российский государственный гуманитарный университет", 2022. - 191 с. - ISBN 978-5-7281-3105-2 : Б. ц.

https://znanium.ru/cover/1991/1991966.jpg