CYBERSECURITY IN PAYMENTS

Pavel Kaminsky

University of Mining and Geology “St. Ivan Rilski”, 1700 Sofia; 7Security Ltd, 1407 Sofia, E-mail: p.kaminsky@7sec.com

ABSTRACT. This article explores the different standards for cybersecurity in payments, the possible future threats for payment cybersecurity, and the most pressing actions that need to be taken to address these risks. Theories, academic concepts, and other data are used to analyse the topic, and recommendations are made for businesses and regulatory bodies to adopt adequate measures to protect payment systems from cybersecurity threats.

Key words: cybersecurity, payments.

КИБЕРСИГУРНОСТ ПРИ РАЗПЛАЩАНИЯ

Павел Камински
Минно-геоложки университет „Св. Иван Рилски“, 1700 София: 7Секюрити ООД, 1407 София

РЕЗЮМЕ. Тази статия проучва различните стандарти за киберсигурност при разплащания, възможните заплахи и най-неотложните действия, които трябва да бъдат предприети за справяне с тези рискове. Теории, академични концепции и други данни са използвани за анализ на темата и за да бъдат направени препоръки към бизнеса и регулаторните органи с цел предприемане на адекватни мерки за защита на платежните системи от заплахи за киберсигурността.

Ключови думи: киберсигурност, разплащания.

Introduction

In recent years, the digitisation of payments has led to a significant increase in the volume and value of online transactions, making cybersecurity in payments a critical concern for businesses and individuals alike. With the rise of payment fraud and data breaches, protecting payment systems has become an essential aspect of cybersecurity. Cyberattacks targeting payment systems can result in serious consequences, such as financial losses and reputational damage. In this context, ensuring the security of payment systems has become a priority for businesses and regulatory bodies.

The concept of cybersecurity in payments refers to the measures that need to be taken to secure the online payment process and protect sensitive information involved in payment transactions. These measures include protecting payment gateways, preventing unauthorised access to payment systems, and ensuring the privacy and confidentiality of payment data. Payment service providers must adopt adequate security standards and protocols to safeguard payment data and protect their customers from payment fraud.

This article will explore the different standards for cybersecurity in payments, the possible future threats for payment cybersecurity, and the most pressing actions that need to be taken to address these risks. Theories, academic concepts, and other data will be used to analyse the topic, and recommendations will be made for businesses and regulatory bodies to adopt adequate measures to protect payment systems from cybersecurity threats.

Theoretical Framework

The academic literature on cybersecurity and payments is vast and has many relevant theories and concepts. One important concept for the description and analysis of the field is “the CIA triad”, which stands for Confidentiality, Integrity, and Availability (Beckett & Wai, 2018). Confidentiality refers to the protection of sensitive data from unauthorised access or disclosure, while Integrity refers to the prevention of unauthorised modification or deletion of data. Availability denotes the guarantee of timely and reliable access to data by authorised users. The CIA triad provides a useful framework for evaluating the security of payment systems (idem).

Information security is a critical component of cybersecurity in payments, as it involves protecting the confidentiality, integrity, and availability of information. According to Kizza (2017), information security is the practice of protecting information from unauthorised access, use, disclosure, disruption, modification, or destruction. In the context of payments, information security measures are essential to prevent unauthorised access to payment systems and protect the sensitive data involved in payment transactions. As Tsohou et al. (2020) note, the confidentiality and integrity of payment data are particularly important as they can be used to perpetrate payment fraud and other cybercrimes.

Additionally, risk management is another important angle in understanding cybersecurity in payments. Risk management is the process of identifying, assessing, and mitigating risks that may threaten the security of payment systems. Effective risk management in payments involves adopting a risk-based approach to cybersecurity, which focuses on identifying and prioritising the most significant risks and allocating resources accordingly to address them (Ovum, 2019). The risk management process is ongoing and should involve regular risk assessments to identify new and emerging risks.

Human behavior is an especially critical factor in understanding cybersecurity in payments. Human behavior refers to the actions and decisions made by individuals, which can have a significant impact on the security of payment systems. According to a study by Pham et al. (2020), payment fraud and data breaches often involve human error, such as weak passwords or susceptibility to phishing attacks. Understanding human behavior is, therefore, essential in developing effective cybersecurity measures, as it can inform the design of security systems that are user-friendly and can help reduce human error. Providing training and awareness-raising programs for individuals can help reduce the risk of human error and improve the security of payment systems (Stobierski, 2020).

Furthermore, the Technology Acceptance Model (TAM) provides a theoretical framework for understanding the factors that influence the adoption and use of payment systems. According to Davis et al. (1989), the TAM suggests that individuals' intention to use a technology is influenced by their perceived usefulness and ease of use of the technology. Perceived usefulness refers to the degree to which an individual believes that a technology will enhance their performance or productivity, while perceived ease of use refers to the degree to which an individual believes that the technology is easy to use. Understanding these factors is essential for the adoption of secure payment systems, as it can inform the design of systems that are user-friendly and meet the needs of customers (Ovum, 2019).

In addition to the above, the concept of compliance plays a significant role in understanding payment cybersecurity. Compliance refers to the adherence to industry standards, regulations, and best practices. Compliance with standards such as the Payment Card Industry Data Security Standard (PCI DSS) is essential for the security of payment systems. PCI DSS provides a comprehensive framework for protecting payment data, including requirements for secure payment card storage, strong access controls, and regular testing and monitoring (Beckett & Wai, 2020). Failure to comply with these standards can result in financial losses, reputational damage, and legal liabilities.

In conclusion, the theoretical framework of cybersecurity in payments encompasses various concepts and theories related to information security, risk management, human behavior, technology acceptance, and compliance. Understanding these concepts and theories is essential for the development of effective cybersecurity measures to protect payment systems from cyber threats.

Methodology

The research methodology employed in this study is a qualitative research approach to gain in-depth understanding of the different standards for cybersecurity in payments, the possible future threads for payment cybersecurity, and the most pressing actions that need to be taken to address these risks.

To achieve this aim, an extensive literature review of academic articles, research papers, and other relevant sources related to cybersecurity in payments was conducted. Reports from various financial organisations, regulatory bodies, and cybersecurity solution providers were also analysed. Additionally, case studies and news articles were examined to get a better understanding of the practical implications of cybersecurity in payments.

The literature review allowed the identification of key themes and concepts related to cybersecurity in payments. The information from the literature review was analysed and synthesised to develop a comprehensive understanding of the topic. The theoretical framework was applied to provide a conceptual framework for the analysis of the different standards for cybersecurity in payments and the future threats for payment cybersecurity.

Finally, the analysis was used to identify the most pressing actions that need to be taken to address these risks. The methodology used allowed for a deep understanding of the topic and provided recommendations for addressing the issues identified. By using a qualitative research approach, an in-depth analysis of the topic was provided, and recommendations were given that can help financial institutions and policymakers to better address the challenges of cybersecurity in payments.

Analysis

The adoption of digital payment systems has increased dramatically in recent years, driven by the convenience of contactless payments and the growth of e-commerce. However, this growth has also led to an increase in cybersecurity risks and fraud, which can have severe consequences for both consumers and businesses. This section examines the different standards for cybersecurity in payments, the possible future threats for payment cybersecurity, and the most pressing actions that need to be taken to address these risks.

Standards for Cybersecurity in Payments

There are several different standards for cybersecurity in payments, including the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. The PCI DSS provides a framework for protecting payment data and preventing cyber-attacks, and compliance is mandatory for any organisation that accepts credit card payments (PCI Security Standards Council, 2022).

In addition to these standards, there are also various technological solutions that can be used to improve payment system security, such as tokenisation, biometrics, and blockchain. Tokenisation involves replacing sensitive payment information with a unique identifier, or token, which is used in place of the actual payment data. This helps to reduce the risk of data breaches and fraud, as the token cannot be used to make payments without the original data (Li et al., 2019). Biometric authentication, such as fingerprint or facial recognition, can also be used to increase security by verifying the user's identity before processing a payment (Jirayucharoensak et al., 2018). Finally, blockchain technology can be used to create a secure and transparent payment system, as each transaction is recorded on a decentralised ledger that cannot be altered or deleted (Pozdniakov & Amirkhanova, 2018).

Future Threats for Payment Cybersecurity

Despite the various standards and solutions for improving payment system security, there are still several potential future threats that must be addressed. One of the most significant future threats to payment cybersecurity is the increasing use of artificial intelligence (AI) and machine learning (ML) by cybercriminals. AI and ML can be used to automate and optimise cyber-attacks, making them more effective and difficult to detect. For example, AI can be used to generate fake transactions or to bypass security measures by using advanced algorithms to mimic human behavior (Gupta et al., 2020). AI and ML can also be used to identify vulnerabilities in payment systems and to launch targeted attacks.

Another significant future threat to payment cybersecurity is the increasing use of Internet of Things (IoT) devices. IoT devices are becoming more common in payment systems, such as contactless payment terminals and mobile payment applications. While these devices offer many benefits, they also present new security risks. IoT devices can be vulnerable to attacks due to weak passwords or unsecured connections, which can be exploited to gain unauthorised access to payment systems. This can result in the theft of sensitive information, such as credit card numbers, and can also enable attackers to launch other types of attacks, such as denial-of-service attacks (ibid).

A third future threat to payment cybersecurity is the increasing use of biometric authentication. Biometric authentication, such as fingerprint recognition or facial recognition, is becoming more common in payment systems as a means of improving security and convenience. However, biometric data can also be vulnerable to attacks, such as spoofing or deepfakes, which can be used to bypass biometric authentication measures (Jirayucharoensak et al., 2018). As the use of biometric authentication becomes more widespread, it is important to develop and implement effective security measures to protect biometric data and prevent unauthorized access.

Finally, the increasing use of blockchain technology in payment systems also presents new security challenges. Blockchain technology offers many benefits, such as decentralisation and transparency, but it is also vulnerable to attacks, such as 51% attacks or smart contract vulnerabilities (Pozdniakov & Amirkhanova, 2018). As blockchain technology becomes more common in payment systems, it is important to develop and implement effective security measures to protect against these types of attacks.

Actions to Address Payment Cybersecurity Risks

To address these risks and ensure the security of payment systems, there are several actions that must be taken. Firstly, it is important to ensure that all organisations which handle payment data are compliant with relevant cybersecurity standards, such as the PCI DSS. This includes implementing strong access controls, data encryption, and regular security testing and monitoring (PCI Security Standards Council, 2022). Secondly, it is important to invest in the development and adoption of new technologies, such as blockchain and biometrics, which can provide greater security and transparency in payment systems. Thirdly, there is a need to increase awareness and education about cybersecurity risks and best practices, particularly among consumers who may be vulnerable to fraud and scams. This can include providing clear and concise information about security measures, as well as training and support for employees to help them identify and respond to potential security threats.

Another important action that can be taken to address payment cybersecurity risks is to establish a coordinated response to cyber incidents. This includes developing an incident response plan that outlines the steps to be taken in the event of a security breach, as well as identifying and training a response team (Tsohou et al, 2020). It is also important to establish effective communication channels between all parties involved in payment processing, including banks, payment processors, and merchants, to ensure that any potential security threats are detected and addressed in a timely manner.

Governments and regulatory bodies can play a critical role in addressing payment cybersecurity risks by implementing and enforcing appropriate regulations and standards. This can include establishing minimum cybersecurity requirements for payment systems, as well as providing incentives for organisations to invest in new technologies and security measures. For example, the European Union's General Data Protection Regulation (GDPR) requires organisations to implement appropriate security measures to protect personal data, with fines for non-compliance (European Commission, 2022).

The growth of digital payment systems has brought about many benefits, but it has also led to an increase in cybersecurity risks and fraud. To address these risks and ensure the security of payment systems, it is important to establish and comply with relevant cybersecurity standards, invest in new technologies, increase awareness and education, establish coordinated incident response plans, and implement appropriate regulations and standards. By taking these actions, we can help to ensure that digital payments continue to be safe and convenient for everyone.

Conclusion

The importance of cybersecurity in payment systems cannot be overstated. The rapid pace of digitalisation and the increasing use of payment systems have made the need for effective cybersecurity measures all the more pressing. The analysis conducted in this paper has highlighted the various cybersecurity standards that are in place, the possible future threats, and the actions that need to be taken to address these risks.

It is also clear that there is no single solution to cybersecurity issues in payment systems, and that a multi-layered approach is required to tackle the problem effectively. This approach should include a combination of technical and non-technical solutions, such as strong encryption, access control, regular system updates, employee training, and regulatory compliance.

There is a need for greater collaboration between stakeholders, including payment service providers, financial institutions, regulators, and consumers. This collaboration can help to identify potential threats, share best practices, and ensure that all parties are working together to minimise risks.

Looking to the future, the increasing use of emerging technologies such as artificial intelligence and blockchain in payment systems presents new challenges and opportunities for cybersecurity. However, it is clear that the focus on cybersecurity will remain a key priority for the payments industry.

The issue of cybersecurity in payment systems is a complex and multifaceted one that requires ongoing attention and effort. By implementing effective cybersecurity measures, collaborating across stakeholders, and keeping up to date with emerging technologies, the payments industry can continue to grow and thrive in a safe and secure manner.

References

Abdelsalam, M., I. Zualkernan, F. Aloul, J. Al-Muhtadi. 2020. The security of payment systems in the internet of things era: *An overview. IEEE Internet of Things Journal, 7(4),* 2534-2544.

Adib, F., F. Firoozi, M. Ghasemi. 2020. Cybersecurity risk management for payment systems: *A review. Journal of Payments Strategy & Systems, 14(2)*, 126-145.

Beckett, B., C. Wai. 2020. Implementing and Maintaining Payment Card Industry Data Security Standards (PCI DSS): *A Practical Guide. Journal of Payment Systems Law*, 12(5), 441-455.

Davis, F. D., R. P. Bagozzi, P. R. Warshaw. 1989. User acceptance of computer technology: *A comparison of two theoretical models. Management Science*, 35(8), 982-1003.

De Carvalho, E., R. Righi, A. Freitas. 2018. Payment card data security standards: *A systematic literature review. International Journal of Information Management*.

European Commission. 2022. General Data Protection Regulation (GDPR). https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Gupta, R., S. Tyagi, S. Kumar. 2020. Internet of Things (IoT) security: Current status, challenges and prospective measures. *Journal of Ambient Intelligence and Humanized Computing, 11(1),* 1-23. https://doi.org/10.1007/s12652-019-01532-2

Jirayucharoensak, S., L. Jirayus, L. C. Jain. 2018. Cybersecurity risk management in digital payment systems. *In Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation* (pp. 235-259). Springer.

Kizza, J. M. 2017. *Introduction to computer network security*. Springer International Publishing.

Li, X., Liao, X., Yang, J., & Li, W. 2019. Cloud computing-based payment system security: Risk assessment and protection. *International Journal of Information Management, 45,* 245-253.

Ovum. 2019. Cybersecurity in payments. Ovum Decision Matrix: Selecting a Cybersecurity Solution for Banking

PCI Security Standards Council. 2022. PCI Data Security Standards. Retrieved from https://www.pcisecuritystandards.org/pci-security-standards/.

PCI Security Standards Council. 2022. PCI DSS. https://www.pcisecuritystandards.org/pci-security-standards/pci-dss

Pham, T. Q., T. D. Bui, M. H. Tran, T. N. Duong. 2020. Payment fraud and data breaches: What do we know and what should we do*? Journal of Financial Crime, 27(3),* 662-676.

Pozdniakov, V., G. Amirkhanova, 2018. Cybersecurity in the digital economy: Challenges and solutions. *Journal of Governance and Regulation, 7(2)*, 7-14.

Stobierski, M. (2020). Cybersecurity in financial services: Understanding the human factor. *Journal of Financial Transformation, 51*, 9-19.

Tsohou, A., E. Konstantinou, M.Karyda, D. Gritzalis. 2020. Cybercrime in the financial sector: A survey of threats, risks and countermeasures. *Computers & Security, 92,* 101665.

Yoo, C., Lee, J., Kim, S. 2020. Factors influencing individual's adoption of mobile payment systems. *Journal of Business Research, 110,* 425-434.