# Cyber Security in Commercial Transactions

M. Buvaneswari

*Assistant Professor, Morning Star Arts and Science College for Women, Pasumpon, Kamudhi (Affiliated to Alagappa University, Karaikudi), Tamil Nadu, India.*

*Corresponding Author Email: buvanabuvana569@gmail.com*

**Abstract**

*The adoption of digital platforms, electronic payment methods, cloud-based infrastructures, and data-driven decision-making models by businesses has resulted in a fundamental redefining of managerial practices and commercial operations. Organizational vulnerability to cyber hazards has increased even as these advancements have greatly increased market reach, consumer engagement, and operational efficiency. When it comes to digital business transactions, cyber security has become a crucial factor in determining trust, resilience, and sustainability. The function of cyber security within the larger context of digital transformation in management and commerce is critically examined in this article. It examines the main online dangers that impact business dealings, such as financial fraud, phishing, malware attacks, identity theft, and data breaches. Additionally, the research assesses modern cyber security tactics such organizational governance models, encryption technology, authentication methods, secure payment systems, and regulatory compliance frameworks. The article makes the case that, from a managerial standpoint, cyber security is now a strategic management requirement that has a direct impact on risk management, competitive advantage, customer trust, and company reputation. According to the study's findings, a strong cyber security infrastructure is necessary to successfully execute digital transformation projects because it guarantees the privacy, availability, and integrity of business data and transactions. As a result, cyber security serves as a fundamental tenet of both long-term organizational performance in the digital economy and safe digital commerce.*

***Keywords***: *Commercial transactions, e-commerce, cyber security, digital transformation, risk management, information systems, and business management.*

## Introduction

The integration of digital technologies into every aspect of business is known as "digital transformation," and it radically alters how companies function and provide value to their clients. Traditional business transactions have been altered in the fields of management and commerce by digital tools like cloud systems, digital wallets, mobile banking, and e-commerce platforms. For financial reporting, supply chain management, customer relationship management, and payments, businesses increasingly mostly rely on digital infrastructure. Cyber security risks have increased, meanwhile, as a result of our growing reliance on digital systems. Online transactions are the focus of cybercriminals who aim to steal confidential data, interfere with business operations, and perpetrate financial fraud. Because of this, cyber security is now a top priority for businesses involved in online sales. The importance of cyber security from a technological and managerial standpoint is examined in this study, along with its role in safeguarding business transactions.

## Review of Literature

The swift expansion of internet banking, electronic payment systems, and digital commerce has made cyber security in business transactions more crucial. To safeguard online financial operations, researchers have looked at a variety of security issues, threats, and technology solutions. The significance of cryptographic methods including digital signatures, encryption, and authentication in guaranteeing safe online transactions was emphasized by Stallings (2019). In order to reduce vulnerabilities, Whitman and Mattord (2020) underlined the significance of information security management, risk assessment, and security policy.

Kshetri (2018) noted that phishing, malware, identity theft, and online fraud are among the main cyber threats that mostly impact poor nations. According to Gupta and Shukla (2021), robust cyber security procedures improve user satisfaction and trust in digital payment systems. Block chain-based security models were suggested by Alzahrani et al. (2020) to enhance transparency and data integrity, and Verma and Singh (2022) showed how well artificial intelligence works in real-time fraud detection. Sharma and Kumar (2021) identified issues such growing cyber fraud and data privacy threats in the Indian setting and suggested stricter laws and education initiatives. The body of research generally affirms that strong cyber security protocols are necessary to provide secure and trustworthy business dealings.

**Objectives of the Study:**

1. To identify major cyber threats and risks affecting online commercial activities.
2. To analyze existing cyber security technologies and protection mechanisms used in digital transactions.
3. To evaluate challenges in implementing effective cyber security frameworks in commercial systems.

**Research Methodology**

Cyber security in business transactions is examined in this study using a descriptive and analytical research design. Secondary sources including books, journals, research papers, and industry reports are used to gather data, whereas surveys and questionnaires are used to gather primary data. Using a straightforward random sample procedure, descriptive statistics and percentage analysis are utilized to examine the data. The study focuses on recognizing security technologies, cyber threats, and obstacles to putting in place efficient cyber security measures.

**Cyber Security as A Concept for Business Transactions**

The practice of defending networks, data, and systems against online threats is known as cyber security. Cyber security makes it possible for buyers, sellers, and middlemen to securely share financial and corporate information during commercial transactions. It entails protecting online platforms, digital contracts, payment systems, and client records. Digital invoicing, electronic fund transfers, online payments, and e-commerce purchases are examples of commercial transactions. In order to prevent unwanted access and guarantee data security, these transactions need to take place in secure digital environments. Commonly employed cyber security techniques to safeguard these procedures include multi-factor authentication, intrusion detection systems, firewalls, and encryption.

**Cyber Security Threats in Digital Commerce**

The volume of online business transactions, including digital contracts, online purchasing, mobile banking, electronic payments, and cloud-based corporate operations, has expanded dramatically due to the quick development of digital commerce. Convenience, efficiency, and worldwide connectivity are provided by these digital systems, but they also expose businesses and consumers to a variety of cyber security risks. The confidentiality,

availability, and integrity of business data and systems are seriously threatened by these dangers.

**Data breaches:** One of the biggest threats to online shopping's cyber security is data breaches. Data breaches occur when sensitive information, such as bank records, credit card numbers, customer information, and company databases, is accessed without authorization. These violations often result in financial losses, legal repercussions, reputational damage, and a drop in consumer trust. High-profile data breach cases demonstrate that even large organizations with complex systems are vulnerable to cyber attacks.

**Phishing**: Another major worry is phishing assaults, which involve dishonest attempts to fool people into divulging financial or personal information via phoney emails, websites, or texts. In digital business, phishing is widely used to get login passwords, bank information, and payment details.

**Attacks using malware and ransom ware** pose serious hazards in digital business settings. Software intended to cause system disruptions, data theft, or illegal network access is referred to as malware. A particular kind of malware known as ransom ware encrypts company data and requests payment to unlock it. Such attacks have the potential to disrupt company operations, jeopardize client data, and result in significant financial losses.

Another major risk is **identity theft**, in which cybercriminals use stolen personal information to fraudulently impersonate people or businesses. Identity theft makes it possible for financial fraud, phony account creation, and illegal transactions in digital commerce. Identity protection has become a top priority for companies and authorities due to the growing usage of digital identities and online verification systems.

In business transactions, **financial fraud and attacks on payment systems** are two of the most harmful cyber security risks. Attacks on point-of-sale systems, digital wallet manipulation, credit card fraud, and unauthorized fund transfers are a few examples. Payment gateways, authentication systems, and transaction systems are all vulnerable to cybercriminals who use these flaws to commit fraud.

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)** attacks also pose a threat to digital commerce platforms by flooding servers and networks with too much traffic. By interfering with internet services, these attacks prevent authorized users from accessing payment systems and e-commerce websites. As a result, companies face operational disruption, consumer discontent, and revenue loss.

**Digital commerce** is also seriously threatened by insider threats. These risks occur when workers, subcontractors, or business associates abuse their permitted access to steal information, alter systems, or divulge private information. Insider attacks are especially risky since they target those who already have authorized access to the system.

**Cyber security risks in digital commerce** are, all things considered, intricate, ever-changing, and dynamic. These risks jeopardize long-term company viability, consumer trust, and regulatory compliance in addition to causing immediate financial harm. As a result, firms looking to accomplish safe and robust digital business operations must comprehend and control cyber security risks.

**Resulting**

1. Safe and dependable business transactions are mostly dependent on cyber security.
2. Techniques for authentication and encryption greatly lower the risk of cyber attacks.
3. Safe payment channels reduce the likelihood of financial fraud.
4. Digital transactions are safer overall when robust security measures are in place.
5. A greater understanding of cyber security builds consumer confidence.

**Recommended**

1. Businesses should use cutting-edge authentication and encryption methods.
2. System updates and security audits should be carried out on a regular basis.
3. To stop cyber fraud, customer awareness campaigns must to be put into place.
4. For increased security, block chain technology and AI-based fraud detection are advised.

**Conclusion**

Protecting business transactions in the digital world requires cyber security. Because digital banking and e-commerce are expanding so quickly, companies need to put strong security measures in place to protect customer information and stop online attacks. Systems

for safe, reliable, and effective business transactions require constant technological development, regulatory support, and user awareness.

**References**


1. *In 2019, Stallings, W. Network security and cryptography. Pearson Schooling.*
2. *Mattord, H. J., and Whitman, M. E. (2020). Information security principles. Cengage Education.*
3. *N. Kshetri (2018). E-commerce cyber security and cybercrime. Global Information Technology Management Journal.*
4. *Shukla, S., and R. Gupta (2021). Cyber security's effect on customer confidence. International Journal of Cyber Security Studies.*
5. *S. Alzahrani and associates (2020). IEEE Access, "Block chain-based security framework."*
6. *Verma, A., & Singh, R. (2022). Cyber threat detection using artificial intelligence. Information Security and Applications Journal.*
7. *Bishop, M. (2019). Security of Computers: Art and Science. Wesley & Addison.*
8. *(2020) Anderson, R. Building Reliable Distributed Systems using Security Engineering. Wiley.*
9. *ISO/IEC 27001 (2022). Requirements for Information Security Management Systems. International Standardization Organization.*
10. *S. Kumar and R. Kumar (2021). issues with digital payment systems' cyber security. Journal of Computer Applications International, 174(15), 12–18.*
11. *Patel, A., & Mehta, S. (2020). E-commerce security challenges and solutions. Information Security Journal, 11(3), 145–156.*
12. *OECD (2021). Risk management for digital security for social and economic well-being. OECD Publications.*
13. *NIST (2020). Version 1.1 of the Cyber security Framework, National Institute of Standards and Technology, USA.*
14. *Zhao, H., Gai, K., and Qiu, M. (2018). Cloud computing data offloading with security considerations. IEEE Cloud Computing Transactions, 6(3), 1–12.*