MINISTRY OF EDUCATION AND TRAINING

HO CHI MINH NATIONAL ACADEMY OF POLITICS

ACADEMY OF JOURNALISM AND COMMUNICATION

LE MINH NGOC

MANAGEMENT OF CYBERSECURITY COMMUNICATION ACTIVITIES IN THE STATE BANKING SYSTEM IN VIETNAM TODAY

DOCTORAL DISSERTATION SUMMARY IN PUBLIC RELATIONS

Scientific Supervisors: Assoc. Prof., Dr. Pham Huy Ky

Dr. Dinh Thi Thanh Tam

HA NOI - 2026

THE RESEARCH HAS BEEB COMPLETED AT
ACADEMY OF JOURNALISM AND COMMUNICATION

***Scientific Supervisors*: Assoc. Prof., Dr. Pham Huy Ky**
Dr. Dinh Thi Thanh Tam

Reviewer 1: .....

Reviewer 2: .....

Reviewer 3: .....

The thesis is defended at the Academy-level Thesis Examining Council
Academy of Journalism and Communication

OPENING

1. Rationale for selecting the topic

Digital transformation is “a comprehensive and fundamental process of change in individuals and organizations regarding lifestyle, working methods, and production modes based on digital technologies.” It is not merely the digitization of data but also a shift in mindset and operational methods to adapt to the rapidly changing business and social environment. In this context, stability in banking operations is a prerequisite for financial stability, contributing to the sustainable growth of the national economy, as banks are the lifeblood of the economy and play a crucial role in Vietnam’s financial system.

Cybersecurity communication aims to protect personal information, ensure safety and security in online transactions and other digital banking activities, in an environment where communication activities take place through digital means such as the internet, social media, mobile applications, and other online platforms. Recognizing the importance of cybersecurity communication in banking, the Government issued Decree No. 59/2022/ND-CP, which stipulates electronic identification and authentication; electronic authentication services; the rights and obligations of service users; and the responsibilities of relevant agencies, organizations, and individuals. The State Bank of Vietnam (SBV) and the Ministry of Public Security signed a coordination plan to implement the Project on Developing Applications of Population Data, Identification, and Electronic Authentication for National Digital Transformation in the 2022–2025 period, with a vision to 2030, to effectively utilize data, ensure accuracy and security of banking-related information.

The management of cybersecurity communication activities in banks, including the state banking system (SBV system), is the process of planning, organizing, directing, coordinating, and controlling to identify appropriate methods that help banks perform effectively in a constantly changing environment. The reality of managing cybersecurity communication activities in the SBV system has been initially implemented with certain effectiveness; however, the strong and diverse impacts of digital transformation have brought many challenges, affecting the effectiveness of such management in Vietnam’s SBV system.

Research on managing cybersecurity communication activities in the state banking system in Vietnam today has both theoretical and practical significance, contributing to stabilizing operations and protecting the system’s information, while providing a multidimensional perspective to enhance operational capacity and stable development of the SBV system, in line with the criteria of the digital economy in the current digital transformation environment.

2. Research Objectives and Tasks

2.1. Research Objectives: Based on clarifying certain theoretical issues and analyzing, evaluating the current situation of managing cybersecurity communication activities in the SBV system, the dissertation proposes orientations and solutions to strengthen such management in the SBV system in Vietnam in the coming period, meeting practical requirements.

2.2. Research Tasks:

Provide an overview of research works related to the management of cybersecurity communication activities in the SBV system in Vietnam, and propose a theoretical research model.

Systematize, analyze the theoretical and practical foundations of the research issue.

Analyze and evaluate the current situation of managing cybersecurity communication activities in the SBV system; identify emerging issues that need to be addressed.

Propose orientations and solutions to strengthen the management of cybersecurity communication activities in the SBV system in Vietnam in the coming period.

3. Research Object and Scope

3.1. Research Object: The banks within the SBV system: Vietcombank (Joint Stock Commercial Bank for Foreign Trade of Vietnam), Vietinbank (Vietnam Joint Stock Commercial Bank for Industry and Trade), and BIDV (Bank for Investment and Development of Vietnam). These banks are multidisciplinary financial service providers, hold significant market shares in the stock market, have the largest customer bases in Vietnam, and wield decisive influence over business activities. They ensure competitiveness in the financial activities of the socialist-oriented market economy and in digital transformation. Therefore, they provide objectivity and representativeness for surveys on the management of cybersecurity communication activities in the SBV system.

3.2. Research Scope

Content scope: Management of cybersecurity communication activities in the SBV system in Vietnam. Specifically, the management of cybersecurity communication through cybersecurity content and protection measures; electronic identification and authentication activities, biometric authentication based on the national database, and sectoral databases using digital means.

Spatial scope: The dissertation studies the management of cybersecurity communication activities in the SBV system in Vietnam on digital platforms and

social networks, focusing on BIDV, Vietcombank, and Vietinbank, specifically their headquarters and branches in Hanoi.

Temporal scope: The dissertation examines the management of cybersecurity communication activities in the SBV system in Vietnam from 2022 to the present. This marks the period when the Government issued Decree No. 102/2022/ND-CP (December 12, 2022) defining the functions, tasks, powers, and organizational structure of the State Bank of Vietnam (Clause 32, Article 2). It is also the period when Decree No. 59/2022/ND-CP on electronic identification and authentication was promulgated, alongside the cooperation plan between the SBV and the Ministry of Public Security to develop applications of population data, identification, and electronic authentication for the national digital transformation program in 2022–2025, with a vision to 2030.

4. Methodology and Research Methods

4.1. Methodology: The dissertation is based on dialectical materialism and historical materialism; Ho Chi Minh's ideology on economic development; the Party's guidelines and the State's policies and laws. It also draws on communication theory, management theory, stakeholder theory, and inherits as well as develops research results related to the management of cybersecurity communication activities in the SBV system in Vietnam.

4.2. Research Methods: The dissertation employs specific research methods such as: Analysis and synthesis method; Statistical and comparative method; Case study method; Sociological survey method

5. Research Questions and Hypotheses

5.1. Research Questions:

Firstly, what issues have been thoroughly investigated in previous studies on the governance of financial instruments related to security within the State Bank of Vietnam's banking system, and what research gaps does this thesis need to address? Secondly, what are the theoretical and practical foundations of governance of financial instruments related to security within the State Bank of Vietnam's banking system in the current context? Thirdly, what are the successes and limitations in the current state of governance of financial instruments related to security within the State Bank of Vietnam's banking system, and what are the causes? Fourthly, what are the key issues that need to be addressed, and what solutions can be implemented to enhance governance of financial instruments related to security within the State Bank of Vietnam's banking system in the future?

5.2. Research Hypotheses*:* The field of communication and information security management has a rich content and numerous research studies. However, scientific

works have not yet conducted in-depth research on information security management in the State Bank of Vietnam's banking system. Analyzing the current state of management helps banks identify strengths and weaknesses, discover opportunities and understand the fundamentals from internal and external factors to overcome weaknesses and strengthen information security management. The research results of this thesis will improve the efficiency of bank management, enhance user acceptance and trust; and contribute to the successful implementation of the banking industry development strategy until 2025, with a vision to 2030, as approved in Decision 986.

6. Theoretical and Practical Significance of the Study

6.1. Theoretical Significance: The dissertation contributes to clarifying the importance of managing cybersecurity communication activities in the SBV system in Vietnam. It provides a theoretical foundation on the relationship between cybersecurity communication, the management of cybersecurity communication activities, and user acceptance and trust in such management.

The dissertation proposes a model for managing cybersecurity communication activities in the SBV system, which can be applied to banks and other financial institutions with similar cybersecurity communication environments. This contributes to modernizing the banking system toward a rational organizational model and a synchronous, effective, and efficient operational mechanism, consistent with the socialist-oriented market economy, ensuring macroeconomic stability, and promoting sustainable growth.

6.2. Practical Significance: The dissertation supports bank managers and cybersecurity experts in developing strategies for managing cybersecurity communication activities in the SBV system. It enhances the SBV system’s role, increases autonomy and accountability, and improves governance capacity according to international standards and practices.

It provides useful information for investment and technology development decisions, helping banks improve performance and ensure system safety, create breakthroughs in administrative reform, strengthen cooperation among departments within banks, promote effective cybersecurity measures, and develop the credit institution system in line with the digital economy and digital transformation conditions. The dissertation helps banks enhance the effectiveness of managing cybersecurity communication activities.

7. New Contributions of the Dissertation: The dissertation focuses on the management of cybersecurity communication activities in the SBV system in Vietnam, offering a new perspective compared to previous studies which often concentrated on technical or legal aspects. It provides a specific, detailed view of the actual

cybersecurity environment in the SBV system, as well as the content and methods of managing cybersecurity communication activities therein.

The dissertation applies principles of communication management to the field of cybersecurity within the SBV system, particularly through electronic authentication activities. This remains an uncommon practice in the banking system and has not been deeply studied by academia. From this, the dissertation proposes feasible solutions to strengthen the management of cybersecurity communication activities, meeting the practical requirements of digital transformation and international integration..

8. Structure of the Dissertation: The dissertation consists of 4 chapters with 11 sections:

Chapter 1: Overview of research works related to the management of cybersecurity communication activities in the state banking system in Vietnam.

Chapter 2: Theoretical and practical foundations of managing cybersecurity communication activities in the state banking system in Vietnam.

Chapter 3: Current situation of managing cybersecurity communication activities in the state banking system in Vietnam and emerging issues.

Chapter 4: Orientations and solutions to strengthen the management of cybersecurity communication activities in the state banking system in Vietnam in the coming period.

Chapter 1
OVERVIEW OF RESEARCH WORKS RELATED TO THE MANAGEMENT OF CYBERSECURITY COMMUNICATION ACTIVITIES IN THE STATE BANKING SYSTEM IN VIETNAM

1.1. Research on Communication and Communication Management

1.1.1. Research on Communication and Communication Activities

1.1.1.1. Worldwide: First, global scholars have paid attention to the history of communication formation and development. Accordingly, communication studies can be divided into four stages based on criteria such as emerging communication technologies, cultural environments, methodologies, perspectives, and ideologies employed by researchers. *Second*, scholars have thoroughly studied the nature and role of communication, analyzing human communication theories and affirming the interactive and decisive relationship between communication and social context. Their strength lies in analyzing communication from multiple angles. However, a gap remains as the management of communication activities has not been deeply addressed. *Third*, scholars have studied various forms of communication. Communication theories have been mentioned, but works have not fully addressed

theories such as the “magic bullet theory,” two-step flow theory, agenda-setting theory, framing theory, and uses and gratifications theory.

1.1.2. In Vietnam: *First*, communication and communication activities have been studied by scholars from multiple perspectives. *Second*, they have studied various forms of communication such as mass communication, multimedia communication, and public relations. *Third*, many works have examined communication activities from both theoretical and practical perspectives. The strong development of social networks today brings enormous potential but also raises governance issues that need resolution. These issues have not been deeply analyzed by scholars and have mostly been studied in specific contexts—for example, mass communication and public opinion regarding parliamentary activities, communication activities of state administrative agencies, or economic policy communication.

1.1.2. Research on Communication Management

1.1.2.1. Worldwide: Scholars have addressed communication management as a means of building and developing brands or marketing products/services of enterprises. Studies have explored communication management on television and internet communication. Their strength lies in analyzing the concept of communication management as including planning, organizing, implementing, evaluating, and controlling the communication activities of an organization or business to achieve set objectives. These studies also mention how managers use tools and methods to ensure information reaches the right audiences and objectives. However, scholars have not generalized issues related to communication management, often focusing on specific activities or fields.

1.1.2.2. In Vietnam: First, communication management has been studied in connection with brand management, considered a component of social governance, involving the mobilization and exercise of power to achieve social and human development goals. Works have not expanded to compare with communication management in other fields, such as cybersecurity communication or policy communication. *Second*, the role of communication management has attracted much attention, emphasized as a management tool for internal and external organizational activities. *Third*, in academic works, communication management has been approached from two perspectives: From a specific perspective, communication management is studied as the integration of communication tools to achieve message consistency. From a broader perspective, works refer to integrated marketing communication activities as a modern approach. *Fourth*, elements of communication management have been identified based on information integration and interaction theories. *Fifth*, scholars have studied factors affecting communication management, paying attention to internal and external factors of enterprises. *Sixth*, research has

examined communication management in specific sectors. However, gaps remain, such as communication skills and managerial capacity of actors, coordination mechanisms in communication management, criteria for evaluating effectiveness, and solutions to improve efficiency.

1.2. Research on Cybersecurity, Cybersecurity Communication Activities, and the Management of Cybersecurity Communication Activities in Banking

1.2.1. Research on Cybersecurity and Cybersecurity Communication Activities

1.2.1.1. Worldwide: Scholars have studied cybersecurity and pointed out that cybersecurity involves protecting electronic systems, networks, computers, mobile devices, programs, and data from malicious, deliberate cyberattacks by criminals. It is considered a matter of survival for nations. While the content and role of cybersecurity have been analyzed extensively, many issues remain absent from these works, particularly the link between cybersecurity and financial security in banking operations—an urgent, vital matter. Research has not yet deeply examined the digital banking business environment and solutions for ensuring cybersecurity in the banking system....

1.2.1.2. In Vietnam: Many academic works have studied cybersecurity from multiple perspectives. Scholars recognize cybersecurity as a top priority, reflected in Vietnam's viewpoints, strategies, and concrete actions. Cybersecurity communication activities have been discussed in scientific topics, conferences, dissertations, and journal articles. Overall, these studies offer valuable insights for the author when researching the management of cybersecurity communication activities in the SBV system in Vietnam.

1.2.2. Research on the Management of Cybersecurity Communication Activities in the Banking System

1.2.2.1. Worldwide: Numerous academic works have studied banking. Many foreign books on banking have been translated into Vietnamese, exploring the early stages of the technological revolution and fundamental changes taking place with trends in banking payments and credit services.

1.2.2.2. In Vietnam: First, there are many books on banking, its origins, characteristics, materials, and socio-economic significance. *Second*, numerous articles have addressed issues related to the management of cybersecurity communication activities in banks, analyzing the state of cybersecurity in banks and the necessity of ensuring cybersecurity through communication management. *Third*, many scientific projects, conferences, and dissertations have researched the management of cybersecurity communication activities in banks. However, these works have not

analyzed the roles, content, and methods of managing cybersecurity communication activities in the SBV system in Vietnam.

1.3. Evaluation of Achievements of Previous Studies and Identification of Issues Requiring Further Research

1.3.1. Evaluation of achievements of previous studies

1.3.1.1. Communication and communication management have been approached from multiple perspectives and studied extensively. First, scholars have examined communication in depth, addressing many aspects of communication theory with convincing analyses. *Second*, basic elements of communication activities have been analyzed: source, message content, communication channels or methods, audience, feedback, and noise in the communication process. *Third*, academic works have studied management and management models, predicting trends in communication management as digital communication becomes an integral part of modern communication.

1.3.1.2. Cybersecurity and cybersecurity communication have been extensively analyzed. First, studies have examined concepts such as cybersecurity, cybersecurity safety, cybersecurity protection principles, and protection measures. *Second*, cybersecurity communication has attracted scholarly attention. *Third*, research has shown that cybersecurity communication activities occur in diverse forms and methods, through both traditional and modern media, in both direct and online formats....

1.3.1.3. Communication activities and their management in banks have been studied. First, scholars have deeply researched banking, identifying its nature, characteristics, and functions in Vietnam. *Second*, they have begun researching cybersecurity issues in banks, emphasizing the critical importance of ensuring cybersecurity amid rising online threats. *Third,* research has confirmed that the SBV has recognized the importance of cybersecurity communication activities in the SBV system in Vietnam, and that such activities have been implemented. *Fourth*, scholars have forecast cybersecurity threats in banking and recommended that the SBV's Communication Department develop communication regulations with clear enforcement mechanisms regarding cybersecurity communication..

1.3.2. Issues requiring further research

First, there has been limited research on communication management and specifically on managing cybersecurity communication activities in the SBV system in Vietnam. *Second,* the current state of managing cybersecurity communication activities in the SBV system in Vietnam has not been studied deeply in academic works, appearing only in some journal articles. *Third*, no academic work has

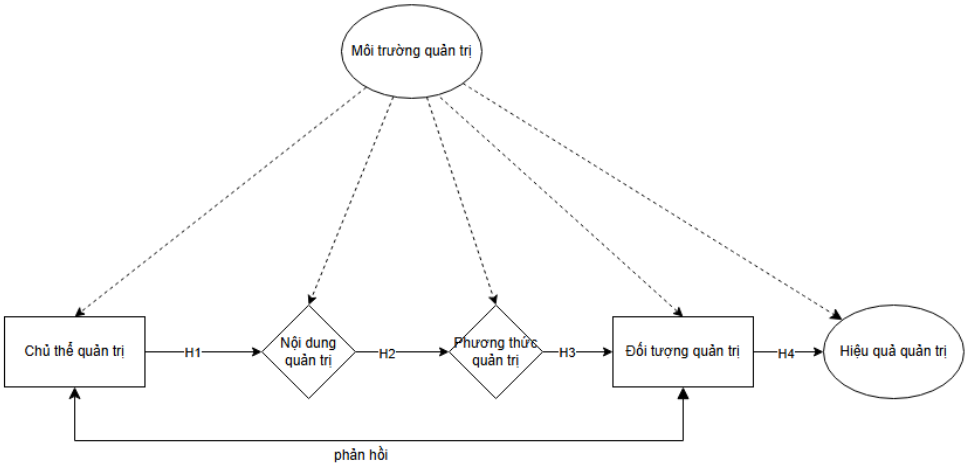
researched solutions to improve the effectiveness of managing cybersecurity communication activities in the SBV system in Vietnam. Such issues have only been mentioned as suggestions for enhancing governance effectiveness or preventing risks in banking operations. These gaps need to be addressed.

1.3.3. Theoretical Frameworks and Proposed Research Model

1.3.3.1. Theoretical Frameworks: A review of scientific works shows that:

Communication theory studies how media affects society and individuals in communication activities. Shannon's communication model describes two-way interactions. *Management theory* helps the dissertation define communication management as a system of methods, processes, and tools used to plan, organize, implement, and control communication activities to achieve set goals. *Stakeholder theory* helps banks better understand their social responsibilities in managing cybersecurity communication activities, building sustainable relationships with stakeholders to share responsibilities and benefits.

1.3.3.2. The proposed thesis framework: Based on the above analysis, the thesis proposes a model of cybersecurity governance composed of six basic elements: governance subjects, governance objects, governance content and methods, governance effectiveness; these elements are influenced by the governance environment. The proposed cybersecurity governance model for cybersecurity is based on the following theories:



Summary of Chapter 1: The overview shows that communication, cybersecurity, cybersecurity communication, banking operations, and communication management have been researched in depth. However, many issues still require further study, particularly the theoretical and practical foundations of managing cybersecurity communication activities in the SBV system, as well as the current situation and solutions to enhance effectiveness in the context of digital transformation. These will be addressed in the following chapters.

Chapter 2

THEORETICAL AND PRACTICAL FOUNDATIONS OF CYBER SECURITY COMMUNICATION MANAGEMENT IN THE STATE BANK SYSTEM OF VIETNAM

2.1. Theoretical basis for managing cybersecurity communication activities in state-owned banking systems in Vietnam.

2.1.1. Some basic concepts

2.1.1.1. Communication and Communication activities

Communication is the process of multidirectional and equal exchange of messages among individuals or groups in society in order to achieve mutual understanding, raise awareness, change attitudes, and adjust behaviors according to the purposes of the communicator within a specific environment.

Communication activities are the actions, tasks, and responsibilities performed in the communication process among individuals or groups to achieve understanding, raise awareness, form attitudes, and change behaviors of the audience in line with the communicator's objectives.

2.1.1.2. Management and Communication management

Management is a long-established and widely applied concept, though there is still no universally unified definition. It can be understood as the process of planning, organizing, leading, and managing the operations of an organization/enterprise; utilizing its resources to achieve the objectives set.

Communication management is the process of planning, leading, organizing, and implementing communication activities of an organization/enterprise and using its resources to achieve communication effectiveness aligned with established objectives; it involves directing communication activities through a chain of factors to build good relations with the public and stakeholders for effective communication.

2.1.1.3. Cybersecurity and Cybersecurity management

Cybersecurity, as defined in Vietnam's Cybersecurity Law (2018), is the assurance that activities conducted in cyberspace do not harm national security, social order and safety, or the legitimate rights and interests of agencies, organizations, and individuals.

Cybersecurity management is the process of protecting networks and information from threats, including policy formulation, risk management, staff

training, incident monitoring and response, and maintaining security standards. It focuses on safeguarding computer systems, networks, and data from cyberattacks, viruses, malware, and other forms of intrusion; as well as identifying, assessing, and mitigating potential risks to networks.

2.1.1.4. Cybersecurity Communication Activities and Cybersecurity Communication Management

Cybersecurity communication activities are not yet clearly defined in the literature. From the above concepts, it can be understood as: the use of communication tools to raise awareness, knowledge, and skills on cybersecurity for the community, helping people understand cyber threats, how to protect personal information and digital assets from cyberattacks, and comply with cybersecurity rules and guidelines.

Cybersecurity communication management is the process of planning, implementing, and monitoring communication activities to raise awareness, knowledge, and behavioral change in the community regarding cybersecurity, while also protecting the reputation and image of organizations and enterprises amid growing cyber threats.

2.1.1.5. The State Banking System and Cybersecurity Communication Management in the State Banking System in Vietnam

The State Banking System in Vietnam: According to Article 4 of the Law on Credit Institutions No. 32/2024/QH15, the banking system in Vietnam is structured into two levels. The State Bank of Vietnam (SBV) is the central bank at level one, managing and supervising level-two banks established through contributions of two or more entities, with more than 50% of capital coming from the state budget. The State banking system includes banks wholly or partly owned by the State, operating under state management and supervision, and performing general banking and financial functions.

Cybersecurity communication management in the state banking system in Vietnam is a new issue, not yet addressed in scientific studies. It is the process of intentional planning, directing, and controlling by management entities over targets through communication activities to ensure cybersecurity in the state banking system under dynamic environmental conditions, thereby enabling effective banking operations..

2.1.2. Elements of cybersecurity communication management

2.1.2.1. The governing entity is the individual or organization that exerts the governing function on the subject. The leading and managing entity is the Party and the

State, through guidelines, viewpoints, and legal documents. The advisory entity is the Propaganda Department at all levels and agencies within the State government system. The entities directly governing the Information Security Activities at the State Bank of Vietnam system are the bank's Board of Directors, the bank's Communication Department/Division, the communication staff, and staff working with partners and customers. Coordinating entities include: the Information Security Department; the Cyber Security and High-Tech Crime Prevention Department (A05); the Research and Application Center for Population Data and Citizen Identification (RAR); the National Cyber Security Association...

2.1.2.2. The main subjects of governance are all communication activities related to cybersecurity, including content and communication methods; these are also the individuals or groups affected by the governing entity, such as the media, those directly involved in cybersecurity communication work, including leaders and managers at all levels within the State Bank of Vietnam and the Communications Department; employees; partners and customers...

2.1.2.3. The management content is very rich:

- Managing communication strategies and measuring communication effectiveness
- Managing the content of communication activities on cybersecurity
- Managing the methods and resources for communication activities on cybersecurity

2.1.2.4. The method of managing information and communication activities related to cybersecurity in the State Bank of Vietnam system refers to the methods, forms, and means that the entity managing these activities uses to achieve effective management as defined. There are many management methods depending on the objectives, target audience, budget, and communication environment.

2.1.2.5. The management environment is a factor affecting the management of information and communication activities related to cybersecurity. The external environment includes politics, law, culture, society, economics, science and technology, customers, partners, direct and potential competitors, suppliers, etc. The internal environment includes factors such as finance, human resources, organizational structure, organizational culture, and the norms and values that all members of the organization respect and adhere to.

2.1.2.6. Effective management is the result achieved that aligns with the objectives of the communication entity within the defined environment. The criteria for evaluating the effectiveness of the governance of cybersecurity activities within the State Bank of Vietnam system is that these activities must ensure the achievement of the set objectives, most importantly, a positive change in the awareness, attitudes, and behavior of the governed subjects, in line with the objectives set by the governing body and meeting the requirements of practice.

2.2. Political, Legal Foundations and Influencing Factors in Cybersecurity Communication Management in the State Banking System in Vietnam

2.2.1. Political and Legal Foundations

2.2.1.1. Party viewpoints: Cybersecurity is a special concern of the Communist Party of Vietnam. It serves as the strategic foundation to firmly ensure national security and protect the Fatherland. Responding to cybersecurity threats is considered core and vital for national protection and development. Cybersecurity is regarded as "the fifth space, the fifth battlefield, the fifth domain of the nation, alongside land, air, sea, and outer space.".

2.2.1.2. State policies and laws: The Party's viewpoints are institutionalized through legislation such as the National Security Law (2004), the Electronic Transactions Law (2005), the Law on Information Technology (2006), the High Technology Law (2008), the Telecommunications Law (2009), the Law on Radio Frequencies (2009), the Cipher Law (2011), the Law on Handling Administrative Violations (2012), the Law on National Defense and Security Education (2013), the Law on Network Information Security (2015), the Law on the People's Public Security Forces (2018), the National Defense Law (2018), the Law on Protection of State Secrets (2018), and the Cybersecurity Law (2018), among others....

2.2.2. The Role of Cybersecurity Communication Management

2.2.2.1. Raising awareness and understanding, changing user behavior, helping to protect systems and data from cybersecurity threats

2.2.2.2. Preventing and responding to cybersecurity threats in banks

2.2.2.3. Establishing and maintaining two-way communication, seeking understanding, acceptance, and cooperation between the banking system and partners and customers

2.2.2.4. Contributing to the protection of national security and human security

2.3. Evaluation Criteria and Factors Affecting the Management of Cybersecurity Communication Activities in the State-Owned Banking System in Vietnam

2.3.1. Evaluation Criteria for Management Effectiveness

2.3.1.1. Evaluating Outputs Using Quantitative Indicators: Outputs can be directly measured from communication activities using quantitative indicators, focusing on the level of reach and interaction of the target audience. This is reflected in the level of reach through the number of people exposed to the communication message; the number of people accessing the website; interactions such as likes, comments, and shares, which show the attractiveness of the content; and the mention rate through the number of times cybersecurity communication activities are mentioned on media channels and social networks, showing the coverage of cybersecurity communication activities and their connection with the audience.

2.3.1.2. Evaluating output results using qualitative indicators: Using qualitative indicators as criteria to measure changes in the awareness, attitudes, and behavior of the managed subjects after receiving the subject's influence. Specific manifestations include the interaction rate of the subjects such as likes, shares, and comments on social media; website traffic from various communication channels; and the satisfaction of the subjects with the content and management methods, helping to evaluate the effectiveness of internal communication management for employees and external communication for partners and customers...

2.3.2. Factors affecting management effectiveness

2.3.2.1. Objective factors: Firstly, the cyberspace with increasingly complex threats, constantly emerging new security vulnerabilities, and increasingly diverse cyberattack trends. Secondly, the development of science and technology in the digital transformation environment creates opportunities and challenges for the management of information security activities. Thirdly, the level of awareness of cybersecurity, internet usage habits, and information sharing behavior of users influence the reception of cybersecurity messages. Fourthly, the State's policy on cybersecurity. Fifthly, digital communication and cybersecurity communication activities of organizations in the financial system, banks, and state agencies.

2.3.2.2. Subjective factors: Firstly, the awareness and capacity of the management entity, leadership ability, coordination, assignment of responsibilities, use of financial resources, human resources, facilities, technology, etc. Secondly, resources that are very important in cybersecurity communication management, including human resources, funding, equipment, technology... to be used as means of communication. Thirdly, the awareness and capacity of communication officers. Fourthly, communication strategy and process. Fifthly, content and communication channels also impact cybersecurity communication management.

Summary of Chapter 2

This chapter clarified several key concepts, including cybersecurity, cybersecurity communication, cybersecurity communication management, the state banking system, and cybersecurity communication management in the SBV system. It also analyzed the roles and key components of cybersecurity communication management in the state banking system of Vietnam. The chapter further examined the political and legal foundations, as well as external and internal factors influencing communication management.

Communication activities play a critical role in building and maintaining the reputation and trust of customers in banks. Banks must develop effective communication strategies to gain these benefits while ensuring proper management of cybersecurity communication activities to mitigate potential negative impacts**..**

Chapter 3

THE CURRENT SITUATION OF CYBERSECURITY COMMUNICATION MANAGEMENT IN THE STATE BANKING SYSTEM IN VIETNAM

3.1. Introduction of the Banks Surveyed in the Dissertation

3.1.1. Vietcombank: Vietcombank is the abbreviation for the Joint Stock Commercial Bank for Foreign Trade of Vietnam. With over 60 years of development, Vietcombank has become a multifunctional bank operating in multiple fields. Equipped with modern infrastructure and having successfully implemented a Core Banking system, Vietcombank enjoys many advantages in applying advanced technology for automated service processing and developing electronic banking products. Its vision is to become one of the world’s top 200 financial groups by 2030.

Vietcombank has more than 600 branches, transaction offices, and representative offices domestically and internationally; 22,599 employees; over 2,500 ATMs and more than 60,000 point-of-sale terminals nationwide; supported by 1,163 correspondent banks in 93 countries and territories.

3.1.2. BIDV: The Bank for Investment and Development of Vietnam (BIDV) was equitized on April 27, 2012, becoming a joint stock commercial bank. On January 24, 2014, BIDV officially listed its shares under the ticker BID on the stock exchange. On April 26, 2022, BIDV launched a new brand identity. Currently, BIDV operates 190 branches across all 63 provinces of Vietnam and in six other countries. Its workforce exceeds 25,700 employees with professional training and high expertise.

3.1.3. Vietinbank: Vietinbank, the Joint Stock Commercial Bank for Industry and Trade of Vietnam, is a multi-ownership, multi-sector bank with the largest charter capital in Vietnam. It was the first Vietnamese bank to establish a branch in Europe, marking a milestone in the country's financial sector. Vietinbank has an extensive network nationwide with one head office, more than 1,000 branches/transaction offices, 9 independent subsidiaries, 5 non-business units, and correspondent relationships with over 1,000 financial institutions in 90+ countries and territories. It is a member of the Vietnam Bankers Association, the Asian Bankers Association, SWIFT, VISA, and MasterCard. Vietinbank has consistently been recognized as one of Vietnam's strongest brands.

3.2. Survey of the current state of communication management

3.2.1. Governing entities

3.2.1.1. Leadership, management, advisory, and coordination entities: The State concretizes the Party's leadership through legal documents for advisory and coordinating entities to implement, such as Decree 04/2019/NĐ-CP on procedures for certain cybersecurity measures; Decision 964/QĐ-TTg on the "National Cyber Safety and Security Strategy to 2025, vision to 2030"; Decision 49/QĐ-TTg on "Cybersecurity Workforce Training to 2025, vision to 2030"; Decree 53/2022/NĐ-CP detailing provisions of the Cybersecurity Law; Decree 59/2022/NĐ-CP on electronic identification accounts; Decree 13/2023/NĐ-CP on personal data protection, etc...

3.2.1.2. Direct management entities: Boards of directors, communication departments, and cybersecurity communication officers have established databases on online fraud prevention, developed data management systems for updates and analysis

to detect new trends, connected with telecom providers, shared information on fraudulent numbers/websites to block scams, and used specialized tools and Intrusion Detection Systems (IDS). Regular security audits are also carried out...

3.2.2. Current status of management targets

3.2.2.1. Bank staff: Proper management has helped employees gain knowledge and awareness about communication management, protecting the bank's reputation and ensuring stable business operations. Communication officers confirm that cybersecurity communication management has achieved initial effectiveness.

3.2.2.2. Partners and customers: Cybersecurity communication management has positively influenced partner and customer awareness. Most state that they are very concerned about cybersecurity and related communication. They understand they must not engage in actions that disrupt telecommunications, the internet, computer networks, information systems, or electronic devices that could harm cybersecurity.

3.2.3. Current status of management content

3.2.3.1. Strategic communication management and effectiveness measurement Banks have developed strategies and implemented cybersecurity communication management plans. Effectiveness is assessed using statistics, customer feedback, and related indicators, with adjustments made to strategies and content as needed.

3.2.3.2. Managing communication content: Communication about the Cybersecurity Law is prioritized, focusing on prohibited acts and sanctions. Banks highlight the law's significance for themselves, their partners, and customers. They also cooperate with the press through articles, reports, and events—particularly regarding Decree 59/2022/NĐ-CP (September 5, 2022).

3.2.2.3. Managing methods and resources: Banks ensure safety through electronic identification and biometric authentication, guiding customers to conduct secure transactions, and organizing campaigns on cybersecurity, especially regarding Decree 59/2022/NĐ-CP. Task forces on e-ID communication have been formed, and cooperation with community digital teams supports the use of VNeID. Resource management, particularly human resources, is emphasized.

3.2.4. Current status of management methods

3.2.4.1. Management methods: Direct management of cybersecurity communication is prioritized. Data from annual reports (2022–2024) shows flexible

approaches in banks' cybersecurity communication management. Management entities issue and enforce cybersecurity standards, reflected in internal regulations and procedures for measurement, execution, and evaluation....

3.2.4.2. Management forms: Banks establish cooperation networks with departments and service providers for information sharing and incident handling. They produce reports and documentaries on cybersecurity, use intranet platforms for internal communication, post information on official websites and apps, and send SMS or email messages to customers. Partnerships with media agencies and the application of digital tools (Tableau, Power BI, VBA) are also common...

3.2.4.3. Management tools: Banks use various media such as press, television, radio, and social media platforms (Zalo, Facebook, Twitter, Instagram, TikTok), as well as websites, email marketing, and digital content (videos, podcasts, blogs). Events like conferences, seminars, exhibitions, and sponsorships also serve as both communication activities and management tools.

3.2.5. Current status of the management environment

3.2.5.1. External factors: The growth of cyberspace, rising complexity of threats, new vulnerabilities, and increasing cyberattacks affect communication management. Digital transformation with AI, IoT, and Big Data is reshaping communication management. Awareness and capacity of target audiences also influence banks, which therefore classify audiences by their cybersecurity knowledge. Legally, the SBV continues issuing directives and action plans to promote cybersecurity communication. Other financial organizations' cybersecurity efforts also impact SBV banks.

3.2.5.2. Internal factors Bank boards delegate responsibilities to communication departments at headquarters, which monitor and evaluate communication effectiveness to adjust strategies. Resources for communication management are prioritized. Communication teams generally possess expertise and skills in cybersecurity. Communication strategies are designed with feasible goals, overall and detailed plans. Content suits target audiences, and chosen channels enhance interaction, answering queries, and collecting feedback.

3.2.6. Management Effectiveness

The effectiveness of managing information security activities is assessed from two perspectives: advantages and limitations, with advantages being fundamental. The

management of information security activities within the State Bank of Vietnam's system has initially been effective, contributing to the formation of a legal framework and infrastructure for ensuring national information security and safety. The awareness and behavior of those being managed are indicators of the effectiveness of managing information security activities, as this is the goal of management. All stakeholders have shown positive changes thanks to the management of information security activities. The content, methods, and means of managing information security activities have been emphasized. A few limitations have also been identified in the current state of information security management.

3.3. General assessment of the current state of governance

3.3.1. Success and its causes

3.3.1.1. Success

Firstly, the content of information security management at the banks surveyed in this thesis has been highly successful. Secondly, the forms and methods of management are flexible and appropriate to the content of management and the needs of the target audience. Thirdly, the management of information security by the banks has helped build an environment that ensures information security for financial activities.

3.3.1.2. Reasons for success

Firstly, banks receive guidance and attention from leadership and management at all levels; there is timely coordination between coordinating entities and direct management entities. Secondly, the Board of Directors and bank officers and employees generally have awareness and responsibility in managing the financial statements on security. Thirdly, banks have effectively implemented the content and methods of managing financial statements on security. Fourthly, the environment for managing financial statements on security is generally stable and favorable.

3.3.2. Limitations and causes

3.3.2.1. Limitations.

Firstly, the demand for information on financial security from a segment of partners and customers is not high, indicating that the effectiveness of financial management has not yet met strategic objectives. Secondly, coordination among entities managing financial security within the State Bank of Vietnam system is not truly effective, leading to a lack of synchronized internal and external communication.

Thirdly, some communication messages are not aligned with the content of financial management.

3.3.2.2. Reasons for the limitations

Firstly, some stakeholders have not yet fully and correctly understood the role of communication regarding cybersecurity and the management of cybersecurity communications within banks. Secondly, banks are facing the development of the digital economy, giving rise to new economic sectors; and attacks from high-tech criminals on cybersecurity. Thirdly, the human resources for communication and management of cybersecurity communications are insufficient. Fourthly, the inadequate understanding of partners and customers also hinders the management of cybersecurity communications.

Summary of Chapter 3: Research shows that cybersecurity communication management in the state banking system has been largely effective. Leadership entities have issued numerous directives and guidelines, which banks have implemented through planning and organizing cybersecurity communication activities. Content is well managed, methods are appropriately applied, and the management environment is supportive. However, technological advancements pose new cybersecurity challenges. Going forward, banks must strengthen cybersecurity communication management to protect the national financial system and ensure political stability and sustainable economic growth. This will be addressed in the following chapter..

Chapter 4

ISSUES AND SOLUTIONS FOR ENHANCED MANAGEMENT OF CYBER SECURITY COMMUNICATIONS IN THE STATE BANK SYSTEM OF VIETNAM IN THE COMING PERIOD

4.1. Issues Arising for Cybersecurity Communication Management in the State-Owned Banking System of Vietnam

4.1.1. The Discrepancy Between the Requirements of Cybersecurity Communication Management in the State-Owned Banking System and the Awareness and Communication Management Skills of the Managing Entities

4.1.2. The Discrepancy Between the Requirements of Cybersecurity Communication Management in the State-Owned Banking System and the Needs and Awareness of the Target Audience in Communication Management

4.1.3. The Discrepancy Between the Requirements of Cybersecurity Communication Management in the State-Owned Banking System and the Management Content

4.1.4. The Discrepancy Between the Requirement for Innovation in Cybersecurity Communication Management Methods and the Banks' Ability to Meet These Requirements

4.1.5. The discrepancy lies between the requirement to strengthen cybersecurity communication management in state-owned banks and the conditions necessary to ensure effective communication management within individual banks.

4.2. Solutions for Strengthening Cybersecurity Communication Management in the State Banking System in Vietnam

4.2.1. Solutions for Management Entities

4.2.1.1. Enhancing awareness of the role of cybersecurity communication management in the SBV system, improving management capacity, clarifying responsibilities of each management entity, and building coordination mechanisms among them. A deeper understanding is needed since managing cybersecurity communication in the context of digital transformation is unprecedented globally and in Vietnam. Enhancing management capacity also requires clearly defining the accountability of leaders: “promptly renewing thinking and actions…; maximizing and tightly integrating resources, with internal strength being decisive.”

4.2.1.2. Training and developing human resources with the capacity to meet banks’ requirements. Boards of directors should actively enhance awareness and training programs, equipping communication staff with cybersecurity knowledge and communication management skills..

4.2.1.3. Effective collaboration among management entities and stakeholders.. Communication theories, management theories, and stakeholder theories must be applied comprehensively, as analyzed in this dissertation, to assess the situation and propose solutions for improved effectiveness in cybersecurity communication management in the SBV system.

4.2.2. Solutions for Management Targets

4.2.2.1. Researching characteristics of management targets in cybersecurity communication at banks, equipping them with knowledge and skills to jointly build a safe cyberspace and ensure effective communication management.

4.2.2.2. Influencing attitudes and encouraging active participation of targets in cybersecurity communication. Banks should study their target groups and segment customers to design appropriate messages. The principle is to "place humans and intellect at the center, as the decisive factor, while making full use of achievements in science and technology" in cybersecurity communication management at SBV banks.

4.2.3. Solutions for Management Content

4.2.3.1. Innovating content of cybersecurity communication management improving security solutions in online and card-based payments, and managing e-ID and biometric authentication. Banks should strengthen message management and communication strategies on cybersecurity to achieve communication goals while adapting to changing environments, technologies, and audience behaviors.

4.2.3.2. Developing internal regulations on cybersecurity and communication management through e-authentication activities to prevent, respond to, and resolve cybersecurity incidents in banks. This will also provide a mechanism for mutual recognition of authentication results based on cross-validation data, enhancing cooperation among banks and ensuring consistency and synchronization in cybersecurity.

4.2.4. Solutions for Management Methods

4.2.4.1. Innovating management forms combining diverse and flexible methods. This is essential to adapt to the rapidly changing communication environment, particularly digital technologies.

4.2.4.2. Innovating management approaches, enhancing modern communication methods in the digital transformation environment, updating and applying the latest communication trends, using chatbots, AI, and social media platforms. Leveraging technological tools optimizes communication processes from content creation, distribution, to effectiveness measurement.

4.2.4.3. Enhancing IT application and effective use of communication tools. AI and chatbots can be used to interact with partners and customers, modernizing communication tools. Influencer marketing and active use of platforms like Facebook, Instagram, and Twitter should also be applied.

4.2.5. Solutions for the Management Environment

4.2.5.1. Promoting digital transformation and digital communication investing in infrastructure for cybersecurity communication management in banks. "Internet+"

technologies, including Big Data and IoT, can integrate communication industries with the internet, supporting innovation in communication technology and forming linkages in cybersecurity communication management across the SBV system..

4.2.5.2. Improving coordination mechanisms among cybersecurity, communication, and banking fields; enhancing cooperation among ministries and agencies to create a safe cyberspace for communication management. Banks should expand cooperation with organizations and agencies, actively participate in cybercrime prevention, and build strong and regular partnerships with capable organizations and businesses in cybersecurity communication management..

4.2.5.3. Developing a Code of Conduct for Internet use to ensure cybersecurity through e-authentication for the banking system. This should be based on the Ministry of Information and Communications' Code of Conduct for Social Media, banking regulations, and official documents such as 2516, 2517, and 2518/BTTTT-CATTT dated June 27, 2024.

Summary of Chapter 4: This chapter identifies four core directions that interact to improve the effectiveness of cybersecurity communication management in the SBV system in Vietnam. It also defines five groups of solutions, with specific measures within each group, to enhance communication management effectiveness in banks.

In the context of digital transformation—an inevitable and vital trend for national development—banks must innovate their operations, particularly in communication and cybersecurity communication management.

CONCLUSION

Communication management in general, and cybersecurity communication management in particular, in the state banking system of Vietnam is a new issue. There has not yet been any scientific research that provides a comprehensive theoretical and practical analysis, clarifies its components, or proposes concrete solutions.

The dissertation focuses on researching the theoretical and practical foundations of cybersecurity communication management in the state banking system of Vietnam. It defines key concepts such as cybersecurity, cybersecurity communication, cybersecurity communication management, the state banking system, and cybersecurity communication management in the SBV system. It analyzes the roles, subjects, targets, content, methods, effectiveness, and environment of cybersecurity communication management. It also examines the political and legal bases as well as objective and subjective factors influencing this management process.

Survey results at Vietcombank, BIDV, and Vietinbank show that cybersecurity communication management in the state banking system has initially achieved effectiveness. Leaders have issued many guidelines, while banks have actively planned and organized communication activities. Content management is relatively effective; methods and tools are diverse; and the management environment is generally favorable. However, certain limitations remain due to increasingly sophisticated cyber threats, limited human resources, and varying awareness among stakeholders.

Based on the Party's viewpoints and State laws, and in line with science and technology development, digital transformation, and the Government's and banking sector's strategies, the dissertation proposes four directions and five groups of solutions to enhance cybersecurity communication management in the state banking system of Vietnam. These include:

Strengthening the role of management entities and improving coordination.

Enhancing the awareness and capacity of management targets.

Innovating communication content and strategies.

Diversifying methods and tools in line with digital transformation.

Improving the management environment through investment, coordination mechanisms, and regulatory frameworks.

In the context of digital transformation—an inevitable trend—strengthening cybersecurity communication management is both urgent and essential. It is vital to protect the national financial system, ensure national security, maintain political stability, and foster sustainable economic growth.

LIST OF THE AUTHOR'S SCIENTIFIC PUBLICATIONS RELATED TO THE DISSERTATION

1. Le Minh Ngoc (2025), "Digital Communication Management on Social Networks in Relation to Cybersecurity Assurance in the State Bank of Vietnam Today", Journal of Political Theory and Communication, Special Issue No. 1 (March 2025), pp. 187–188.

2. Le Minh Ngoc (2025), "Cybersecurity of the State Banking System – Some Initial Results", Journal of Party History, https://tapchilichsudang.vn/an-ninh-mang-cua-he-thong-ngan-hang-nha-nuoc-mot-so-ket-qua-buoc-dau.html

3. Le Minh Ngoc (2025), "Ensuring Cybersecurity for Technological Platforms Serving the Ideological and Theoretical Work of the Party Today", https://lyluanchinhtri.vn/bao-dam-bao-an-ninh-mang-cho-cac-nen-tang-cong-nghe-phuc-vu-cong-tac-tu-tuong-ly-luan-cua-dang-hien-nay-7153.html

4. Le Minh Ngoc (2025), "Cybersecurity communication in the Vietnamese banking system in the current digital transformation environment", https://lyluanchinhtrivatruyenthong.vn/truyen-thong-ve-an-ninh-mang-tai-he-thong-ngan-hang-o-viet-nam-trong-moi-truong-chuyen-doi-so-hien-nay-p29453.html