RESEARCH PAPER

Analysis Of Emprical And Conceptual Models Of Behavioral Intention For Cybersecurity Compliance In Banks

Devershi Pallavi Bhatt *, Pardeep Kumar[1]
bhattdevershi@gmail.com , yadav.pardeep@gmail.com
Corresponding Author (*) - Devershi Pallavi Bhatt
*Professor, Department of Computer Application, Manipal University Jaipur
[1] Research Scholar, Department of Computer Application, Manipal University Jaipur

ABSTRACT

Consumer confidence and financial data are threatened by the increasing cybersecurity threats against banks. The adherence to the information security policies depends on the employee behavior despite the importance of the technological protection. To assess the effectiveness of the conceptual and empirical behavioral intention models in explaining and improving bank cybersecurity compliance, this paper contrasts them. The Theory of Planned Behavior (TPB), Unified ISP Compliance Model, and Integrated Behavioral Model are not suitable in the banking industry even though they are sound theoretical models. Financial institution surveys and case studies evidence that contextual aspects such as corporate culture, corporate awareness, and the regulatory pressure have an impact. The comparison analysis helps to reveal that empirical studies can be used to give background, but conceptual models can be used to develop in-depth descriptions. The findings indicate that a hybrid, bank-specific paradigm of theory and empirical validation is what improves cybersecurity compliance. The study provides practitioners, regulators and scholars in the financial sector with valuable information by filling the gap between theory and practice.

Keywords: Cybersecurity compliance, behavioral intention, banking sector, Theory of Planned Behavior (TPB), Unified ISP Compliance Model, Integrated Behavioral Model, empirical studies
How to cite this article: Bhatt DP, Kumar P. Analysis of Empirical and Conceptual Models of Behavioral Intention for Cybersecurity Compliance in Banks. Int J Drug Deliv Technol. 2026;16(36s): 973-980. DOI: 10.25258/ijddt.16.36s.113

INTRODUCTION

Cyberattacks are one of the most targeted areas of the banking sector due to the digital nature of the transactions, privacy of customer information and the connectivity of systems involved in the banking industry. Financial institutions have more cyber events, including phishing, malware, insider risks, and large-scale fraud [8, 9]. Individuals are the least point in information security [8, 9]. Rules are also essential and technology. The compliance of security policy is based on the way workers think, what they plan and what they do. To learn about these behavioral traits there are numerous philosophical and empirical models created. What people may do to analyze cybersecurity are the Theory of Planned Behavior (TPB) [15, 18], Unified Model of Information Security Policy Compliance [1, 3], and the Integrated Behavioral Model [5]. These models are based on attitudes, norms, perceived control, deterrents, and culture of the company that explain how people plan to adhere to rules. New observational research has also investigated the behavior of companies when they obey the regulations. Bauer and Bernroider [8] studied the adherence to the rules in a large bank by people, and Ryutov et al. [11] studied the intention to adhere to the rules in the aspect of risk. Such a study illuminates the issues of how conceptual theories can be applied and demonstrated. It does not have a systematic way of comparing conceptual and empirical methods, particularly in banks. Banking is more regulated, transactions are costly and rely on the trust of the customers hence it is very important that they practice cybersecurity regulations. This requires much research on behavioral purpose models to ensure that financial institutions adhere to the rules.

Literature Review

Conceptual Models of Behavioral Intention

A number of theoretical models have been proposed in an attempt to define the reasons behind the adherence (or lack of adherence) to cybersecurity regulations by employees. One of the most popular is the Theory of Planned Behavior (TPB). It holds that purpose is determined by attitudes, subjective norms, and the sense of being in control of the ability to influence his or her behavior [15, 18]. TPB has been applied in information security studies to determine the likelihood of people adhering to the rules, and has been found to identify significant variables that influence the behaviour of employees when security matters. On this basis, professionals have developed integrated and cohesive models that are capable of explaining more. The Unified Model of Information Security Policy Compliance [1, 3] incorporates an element of the TPB, the deterrence theory and the rational choice perspective to provide a comprehensive account of how individuals comply with security policies. The Integrated Behavioral Model has also been identified to have been effective with regard to information security awareness focusing on the value of corporate standards and habitual factors [5]. There are two other methods of thinking, namely, the deterrence and the goal setting theories. They demonstrate how penalties, incentives, and organized orchestras can influence the agenda of people to comply with the rules [18]. Organizational factors are also of great importance such as the culture and the sense of security. Goo et al. [6] established that when employees feel backed by the security culture in the company, then they tend to adhere to the information security rules. Additionally, behavioral compliance model, being a composite theory, by Aurigemma, incorporates multiple concepts, and this demonstrates the fact that compliance behavior is multidimensional [21]. Although these theoretical models are founded on good theory, few of them have been directly experimented on in the banking contexts. This creates a disconnect between research and practice since banks practice where failure to do so can cost them, get them into legal trouble and damage the trust of people. When bridging this gap, conceptual models will need to be modified and experimented in a manner that is unique to financial companies. All in all, mental models are a good place to begin a theory though they have not been experimented much in the banking environment yet, and thus they require to be tested in the field.

Table 1. Summary of Conceptual Models of Behavioral Intention in Cybersecurity Compliance

Model	**Key Constructs**	**Application in Cybersecurity**	**Limitations in Banking Context**
Theory of Planned Behavior (TPB) [15], [18]	Attitudes, subjective norms, perceived control	Predicts compliance intentions in organizational contexts	Generic, limited sector-specific insights
Unified Model of ISP Compliance [1], [3]	Attitude, deterrence, rational choice	Strong integration of multiple theories	Limited empirical testing in banks
Integrated Behavioral Model [5]	Awareness, norms, habits	Validated in information security awareness studies	Not widely applied in financial sector
Security Climate Model [6]	Organizational culture and climate	Links culture with compliance intention	Highly context dependent
Composite Framework [21]	Multiple behavioral constructs	Provides multidimensional explanation	Complex, requires extensive validation

Empirical Studies on Cybersecurity Compliance

Emerging empirical research has tested these conceptual frameworks in real-world organizations. Bauer and Bernroider [8], one of the few empirical investigations in a financial institution, found that awareness and reasoning processes strongly influenced compliant action. Ryutov et al. [11] examined employee-based hazards and showed how risk exposure affects intentions. Studies show that compliance is context-dependent. Industry-wide systematic reviews have synthesized findings. Sulaiman et al. [9] examined organizational compliance and violation behaviors, while Almansoori [7] surveyed cybersecurity behavior theories and models. Both studies note industry-specific application needs, especially in financial institutions. Further insights come from emerging region empirical investigations. Tran et al. [17] researched Vietnamese compliance and how cultural context and organizational awareness affect employee behavior. Oyewole et al. [4] examined online banking cybersecurity threats and compliance enforcement prevention measures. Recent breakthroughs examine tech-assisted compliance. DOPAMU et al. [19] investigated AI applications for regulatory compliance in U.S. financial institutions, indicating the potential of AI-driven compliance monitoring. Meshkat et al. [10] used behavioral modeling to mimic cybersecurity compliance and quantify human risk elements. These empirical investigations show that conceptual models explain compliance intentions, but their real-world implementation requires contextual adaptation, especially in banks with high regulatory standards and sector-specific hazards.

Methodology

This study uses a comparison analytical method to look at both theoretical and real-world models of how banks plan to follow cybersecurity rules. There are three main parts to the methodology: choosing the literature, making a classification system, and comparing the literature.

Literature Selection

A structured search strategy was applied to identify relevant studies between 2013 and 2024, covering both conceptual models and empirical studies related to information security policy compliance. Databases including Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library were utilized. Search keywords included combinations of:

- "Cybersecurity compliance," "information security policy compliance," "behavioral intention," "banking," "financial institutions," "TPB," "unified model," "integrated behavioral model," and "deterrence theory."

Inclusion criteria:

Research that directly uses behavior intention theories towards cybersecurity compliance. Theory in the banking or financial institution sector or in a research with transferable organizational implication. Both theoretical replications (proposed conceptual models, concepts), and empirical validation (surveys, case studies, experiments).

Exclusion criteria:

- Purely technical cybersecurity studies without behavioral focus.
- Studies without clear linkages to compliance or organizational policy adherence.

From this process, 23 studies were shortlisted for in-depth review.

Classification Framework

The chosen articles were grouped into two categories:

1. Conceptual Models: Research suggesting or simulating theoretical models e.g. TPB [15], Unified ISP Compliance Model [1], [3], Integrated Behavioral Model [5], Security Climate Model [6], and Composite Frameworks [21].
2. Empirical Studies: Studies which tested behavioral intention models in the organization, particularly the banking setting [8], [11], [17], or performed systematic reviews of compliance behavior [7], [9].
3. Every research was evaluated in the four dimensions of comparison:
    a. **Theoretical grounding** (clarity and comprehensiveness of constructs).
    b. **Contextual application** (general organizational vs. banking-specific).
    c. **Validation method** (conceptual replication, survey, case study, simulation).
    d. **Practical relevance** (implications for banking compliance strategies).

Comparative Analysis Approach

In order to critically assess conceptual and empirical models a comparative matrix was created. This matrix correlates models to the four dimensions mentioned above, making it possible to evaluate the following:

- The positive side of conceptual models in the provision of theoretical explanation.
- Empirical studies have the strength of providing practical validation.

The shortcomings of both methods applied to the banking cybersecurity compliance.

Comparative Analysis

This section sums up the information gained in the reviewed literature by comparing conceptual models with studies of behavioral intention in cyberspace in banks.

Conceptual Models

Theory of Planned Behavior (TPB) [15], [18], the Unified Model of Information Security Policy Compliance [1], [3], and the Integrated Behavioral Model [5]. Much of the research concerns the broad organizational contexts, thereby reducing its applicability in banking sector. Moreover, financial institutions tend to make their predictive validity without providing some empirical proof to their claims.

Empirical Studies

These conceptual models have been put into practise through empirical research that has tried to prove them right. Indicatively, Bauer and Bernroider [8] investigated the compliance behavior in a giant banking organization and discovered that the reasoned process of awareness motivates safe behavior. Ryutov et al. [11] investigated compliance among risks which are based on employees, and Tran et al. [17] emphasized on the cultural factors in the Vietnamese banks. Other reviews, e.g. Sulaiman et al. [9] and Almansoori et al. [7], generalized cross- industry results, highlighting the lack of banking-specific validation.

- **Strengths:** empirical research shows context-specific motivators of compliance, cultural and organizational effects, and proves theoretical constructs.
- **Limitations:** They tend to be context dependent and disjointed and cannot be generalized to other banking settings. Not many studies combine the research with the existing conceptualizations.

Comparative Findings

Through the analysis, Conceptual models are good theories but not tested in contexts of banks. Compliance behaviors in practice are proven to be valid by empirical research but lack the theoretical enrichment to be generalized. The most promising way would be a hybrid approach that involves conceptual rigor and empirical insights unique to banking. As an illustration, the frameworks that are both robust and context-sensitive may be obtained by embedding the TPB constructs into compliance programs in banks and considering the empirical evidence of cultural and organizational research. Table 2 presents Comparative Analysis of conceptual and empirical model in cybersecurity compliance and table 3 presents the Results of review across five parameters in Cybersecurity compliance in banks.

Table 2. Comparative Analysis of Conceptual and Empirical Models in Cybersecurity Compliance

Dimension	Conceptual Models	Empirical Studies
Theoretical Grounding	Strong frameworks (TPB [15], Unified ISP [1], Integrated Behavioral Model [5])	Relies on application of existing theories
Contextual Application	Mostly generic organizational settings	Banking-specific studies (e.g., [8], [17]) and cross-industry reviews [7], [9]
Validation Method	Conceptual replication, theoretical extension [1], [3], [21]	Surveys, case studies, simulations, reviews [8], [11], [19]
Practical Relevance	Explains behavioral intention but lacks sector-specific insights	Provides actionable findings for banking compliance but limited generalizability
Limitations	Limited empirical testing in banks; often abstract	Context-dependent, fragmented, and culturally constrained
Banking Relevance	Rarely applied directly in financial institutions	Multiple studies in banking ([8], [17]) highlight sector-specific compliance drivers, but integration with

Analysis Of Emprical And Conceptual Models Of Behavioral Intention For Cybersecurity Compliance In Banks

Dimension	Conceptual Models	Empirical Studies
		conceptual theory is lacking

Table 3. Outcomes of Review Across Five Parameters for Cybersecurity Compliance in Banks

Parameter	Description	Conceptual Models Outcome	Empirical Studies Outcome	Hybrid/Bank-Specific Insight
SQ (Security Quality)	Effectiveness of compliance frameworks	Theoretical constructs emphasize deterrence & norms	Awareness & culture improve SQ [8], [17]	Hybrid ensures sector-specific compliance
PT (Policy Transparency)	Clarity & enforceability of policies	Rational choice assumed	Employees follow clearer, well-communicated policies	Embed TPB constructs into transparent policies
PR (Perceived Risk)	Employee perception of consequences	Deterrence theory central	Higher risk perception drives compliance [11]	Combine deterrence + risk communication
FL (Financial Literacy)	Awareness of financial & security risks	Conceptual models don't directly cover	Empirical studies show financial awareness impacts compliance [9], [17]	Add FL training in compliance programs
BI (Behavioral Intentions)	Willingness to comply with ISP	Central construct in TPB, ISP, IBM	Empirical studies validate BI via culture, awareness, literacy	Hybrid models refine BI prediction & validation

Implications for Banks

The comparison analysis highlights the necessity of bank-specific hybrid models combining the explanatory power of conceptual frameworks and the contextual information of empirical research. Financial institutions might be benefited by:

- Integration of TPB and Unified Models constructs into training on compliance that is specific to the banking staff.
- Using empirical evidence to make compliance programs more culturally and organization-oriented in various banking systems.

Making AI-enhanced compliance behavior reinforcement tools [19] and ensuring compliance with the regulations.

Discussion and Implications

The results of this research highlight the complementary strength and weaknesses of conceptual and empirical research in the area of cybersecurity compliance in the banking industry. Though conceptual models provide organized theoretical framework, empirical studies provide practical confirmation which incorporates organizational realities. The implications of this comparative analysis are discussed as below.

Theoretical Implications

Theory of Planned Behavior (TPB) [15], the Unified ISP Compliance Model [1], [3] and the Integrated Behavioral Model [5] are some of the conceptual models that offer strong explanatory models that could be applied to the cybersecurity compliance in banks.

Table 4 shows the findings and practical implications of conceptual and empirical models

Category	Key Findings	Implications
Theoretical Contribution	Conceptual models provide structured explanations (TPB, Unified ISP, Integrated Behavioral Model)	Require contextual adaptation for banking compliance
Empirical Contribution	Banking-specific studies (e.g., [8], [17]) validate role of culture, awareness, and policy clarity	Show need for real-world validation of conceptual models
Strengths	Conceptual = explanatory depth; Empirical = contextual validation	Combining them yields robust compliance frameworks
Weaknesses	Conceptual = lack of sector testing; Empirical = fragmented & localized	Need hybrid, bank-specific frameworks
Practical Relevance	AI-assisted monitoring ([19]), culture-building, transparent policy	Banks should adopt hybrid strategies aligned with regulations and culture

They are however limited in their use in the financial institutions and this limits predictive reliability. The comparative analysis indicates that the next research should be done on:

- Formulating hybridized models, which combine constructs of various theories (e.g., deterrence, organizational culture, and TPB).
- Carrying out cross-cultural checks of these models in order to explain the differences in the regulatory

environment and employee attitude between banking systems.

- Filling the gap between concept conceptualism and empirical flexibilities, ensuring that the theoretical models do not lose their significance in the fast-changing banking habits.

Practical Implications

To professionals working in the banking industry, the findings point out a few practical conclusions:

- Policy design: Banks must incorporate behavioral theories in the design of cybersecurity policy and should instill attitudes, norms and deterrence measures in training and compliance programs.
- Employee awareness and culture: Empirical studies [8], [17] evidence that organizational culture and security climate have a strong impact on compliance. This means that banks are supposed to instill a culture of security consciousness whereby compliance is supported by the leadership and peer pressure.
- Technology integration: Compliance with the policy can be increased by implementing emerging technologies, including AI-assisted monitoring [19], which offers a flexible, real-time identification of the policy violation and strengthens behavioral intention to comply.
- Sector-specific frameworks: Sector-specific frameworks Compared to generic type of organization, the banking institutions need compliance strategies that are identified with the financial regulation, trust of customer, and security of offering high value transaction.

Implications for Future Research

The comparative results present a number of perspectives of inquiry in the future:

- Model refinement: It is required to refine conceptual models on the basis of empirical banking information, developing bank-specific behavioral intention frames that combine theory and sector realities.
- Longitudinal research: The existing empirical research is usually cross-sectional in nature [11]. The longitudinal approaches need to be applied in the future studies involving banks to trace how the behavior of compliance changes over time.
- Interdepartmental solutions: The integration of psychological, organizational behavior, financial, and artificial intelligence knowledge might result in broad-based principles of banking cybersecurity compliance.
- Regulatory lens: The relationship between regulatory international banking standards [2], [22] and employee conduct needs to be studied further, and a way to bridge the gap between macro-level regulatory needs with micro-level intent and action in financial institutions.

Conclusion

The paper compared and contrasted conceptual and empirical models of the behavioral intention on cybersecurity compliance by banks. Theory of Planned Behavior (TPB) [15], Unified ISP Compliance Model [1], [3], and the Integrated Behavioral Model [5] are conceptual models that offer a solid theoretical basis on recognizing reasons why employees adhere to security policies. Their use in the banking sector is however limited with most of the frameworks having been designed on generic organizational settings. The role of organizational culture, awareness, and regulatory factors in the development of compliance behavior is proven by the empirical studies, as evidenced by the research carried out in the banking organizations [8], [17], and so on. Compliance is influenced by culture, awareness and regulations. These studies are sector-specific but lack the conceptual frameworks which have theoretical generalizability. It compares the two approaches that are needed but not enough. Conceptual frameworks elucidate more than background which empirical research offers. The hybrid approach that is institution-specific and integrates empirical validation and theoretical rigor is required in financial institutions to achieve the optimal cybersecurity compliance. Building a culture of security, harmonizing compliance regulations with behavioral theories, and applying AI-aided monitoring in order to enhance compliance are among the important conclusions. Researchers need to cross-culturally test their models, revise them with the help of empirical banking statistics, and perform longitudinal research of cybersecurity in the financial sector. The gap between the theory and practice can be bridged by offering empirically validated practices that would address the regulatory requirements and risks posed on financial institutions and ensure cybersecurity compliance within the banking industry.

REFERENCES

[1] D. K. Young, D. Carpenter, and A. J. McLeod, "A conceptual replication of the unified model of information security policy compliance," *Annals of Telecommunications and Regulatory Review*, vol. 6, no. 1, p. 7, 2020, doi: 10.17705/1ATRR.00050.

[2] N. S. Uzougbo, C. G. Ikegwu, and A. O. Adewusi, "Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations," *Int. J. Sci. Res. Archive*, 2024, doi: 10.30574/ijsra.2024.12.1.0802.

[3] M. Kajtazi, N. Holmberg, S. Sarker, C. Keller, B. Johansson, and O. Tona, "Toward a unified model of information security policy compliance: A conceptual replication study," *Annals of Telecommunications and Regulatory Review*, vol. 7, no. 1, p. 2, 2021, doi: 10.17705/1ATRR.00067.

[4] A. T. Oyewole, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu, "Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio," *World J. Adv. Res. Rev.*, 2024, doi: 10.30574/wjarr.2024.21.3.0707.

[5] A. E. Schütz and T. Fertig, "The forgotten model – Validating the integrated behavioral model in context of information security awareness," in *Proc. HICSS*, 2023, doi: 10.24251/hicss.2023.828.

[6] J. Goo, M.-S. Yim, and D. J. Kim, "A pathway to successful management of individual intention to security compliance: A role of organizational security climate," in *Proc. Hawaii Int. Conf. Syst. Sci.*, pp. 2959–2968, 2013, doi: 10.1109/HICSS.2013.51.

[7] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories," *Appl. Sci.*, vol. 13, no. 9, p. 5700, 2023, doi: 10.3390/app13095700.

[8] S. Bauer and E. W. N. Bernroider, "From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization," *ACM Trans. Manage. Inf. Syst.*, vol. 48, no. 3, pp. 44–68, 2017, doi: 10.1145/3130515.3130519.

[9] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, "Cyber–information security compliance and violation behaviour in organisations: A systematic review," *Soc. Sci.*, vol. 11, no. 9, p. 386, 2022, doi: 10.3390/socsci11090386.

[10] L. Meshkat, R. L. Miller, C. Hillsgrove, and J. King, "Behavior modeling for cybersecurity," in *Proc. Reliability and Maintainability Symp.*, 2020, doi: 10.1109/RAMS48030.2020.9153685.

[11] T. Ryutov, N. D. Sintov, M. Zhao, and R. S. John, "Predicting information security policy compliance intentions and behavior for six employee-based risks," *J. Inf. Privacy Security*, vol. 13, no. 4, pp. 260–281, 2018, doi: 10.1080/15536548.2017.1418632.

[12] Y. Gangire, A. Da Veiga, and M. Herselman, "A conceptual model of information security compliant behaviour based on the self-determination theory," in *Proc. ICTAS*, pp. 1–6, 2019, doi: 10.1109/ICTAS.2019.8703629.

[13] A. Furfaro, T. Gallo, A. Garro, D. Saccà, and A. Tundis, "Cybersecurity compliance analysis as a service: Requirements specification and application scenarios," *Concurrency Comput.: Pract. Exper.*, vol. 30, no. 12, 2018, doi: 10.1002/cpe.4289.

[14] Y. Hong and S. Furnell, "Organizational formalization and employee information security behavioral intentions based on an extended TPB model," in Proc. CYBERSECPODS, pp. 1–4, 2019, doi: 10.1109/CYBERSECPODS.2019.8885405.

[15] T. Sommestad, H. Karlzén, and J. Hallberg, "The theory of planned behavior and information security policy compliance," *J. Comput. Inf. Syst.*, vol. 59, no. 4, pp. 344–353, 2019, doi: 10.1080/08874417.2017.1368421.

[16] V. B. Hinsz, "Motivating cybersecurity behaviors: A beyond reasoned action conceptualization," *Organ. Cybersecurity J.*, 2024, doi: 10.1108/ocj-08-2023-0015.

[17] D. V. Tran, P. V. Nguyen, L. P. Le, and S. T. N. Nguyen, "From awareness to behaviour: Understanding cybersecurity compliance in Vietnam," *Int. J. Organ. Anal.*, 2024, doi: 10.1108/ijoa-12-2023-4147.

[18] I. Hwang and H.-Y. Lee, "The employee's information security policy compliance intention: Theory of planned behavior, goal setting theory, and deterrence theory applied," *J. Digit. Convergence*, vol. 14, no. 7, pp. 155–166, 2016, doi: 10.14400/JDC.2016.14.7.155.

[19] O. Dopamu, J. Adesiyan, and F. Oke, "Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity," *World J. Adv. Res. Rev.*, 2024, doi: 10.30574/wjarr.2024.21.3.0791.

[20] S.-H. Kim, K. H. Yang, and S. Park, "An integrative behavioral model of information security policy compliance," *Sci. World J.*, vol. 2014, p. 463870, 2014, doi: 10.1155/2014/463870.

[21] S. Aurigemma, "A composite framework for behavioral compliance with information security policies," *J. Organ. End User Comput.*, vol. 25, no. 3, pp. 32–51, 2013, doi: 10.4018/JOEUC.2013070103.

[22] A. Marotta and S. E. Madnick, "Analyzing the interplay between regulatory compliance and cybersecurity (revised)," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3569902.

[23] Z. Ren, G. O. Cowan, R. Ren, L. Xin-jing, Y. Wang, and P. Huang, "Cybersecurity crafting intervention model based on behaviors change wheel," in *Advances in Information Security and Assurance*. Springer, 2024, pp. 281–307, doi: 10.1007/978-3-031-52272-7_12.