“ALEXANDRU IOAN CUZA” UNIVERSITY IAŞI
THE FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION (FEAA)
DOCTORAL SCHOOL OF ECONOMICS AND BUSINESS ADMINISTRATION
FUNDAMENTAL FIELD: SOCIAL SCIENCES
FIELD OF SCIENCE: ECONOMIC SCIENCES
DOCTORAL FIELD: MARKETING

VALUE PROPOSITION WHEN SHIFTING CYBERSECURITY TECHNOLOGIES FROM ON-PREMISES TO THE CLOUD: A CASE STUDY OF ACTIVE DEFENSE CYBERSECURITY

DOCTORAL THESIS ABSTRACT

DOCTORAL STUDENT: GUY WAIZEL
DOCTORAL SUPERVISOR: PROFESSOR ADRIANA ZAIT

2025

Table of Contents

KEYWORDS

Cybersecurity Cloud Adoption; Cloud Migration Strategies; Value Proposition in Cybersecurity ;Cyber-Active Defense Technologies; Transition from On-Premises to Cloud; Cybersecurity Marketing Strategies; Cybersecurity Buyer Behavior; AI in Cybersecurity and Cloud Adoption

INTRODUCTION

This research develops a model to explain consumer behavior during the transition of cybersecurity technologies from on-premises to cloud or hybrid environments, aiming to inform a value proposition plan for marketing departments in cybersecurity companies. This is crucial as vendors increasingly release cloud-exclusive products while phasing out support for on-premises solutions. A strategic marketing approach is essential to retain customers amidst the growing trend of cloud migration.

Key themes of the research include the challenges of cloud adoption for both vendors and customers, customer perceptions of on-premises software and cloud, effective marketing strategies to encourage migration, and the context of active defense technology. The existing literature on cloud adoption provides insights into various thematic areas but lacks specifics on the unique challenges faced by cybersecurity vendors during this transition.

Current studies reveal significant gaps in understanding the difficulties organizations face when adopting cloud solutions, particularly concerning security, compliance, and resources. Additionally, there is limited research on how vendors can facilitate this transition or the factors that influence customer willingness to migrate. This research aims to address these challenges and provide valuable methodologies applicable across various sectors, focusing on strategic marketing and the implications for organizational dynamics, such as skills training and job security. Overall, a well-defined value proposition plan is necessary to effectively communicate the benefits of migrating from on-premises to cloud solutions while addressing the concerns of both vendors and customers.

Research Aims and Objectives

The primary aim of this research was to develop a customer behavior model that explains how customers behave when transitioning from on-premises cybersecurity software to cloud or hybrid cloud solutions. Based on this model, a value proposition plan was created to assist in persuading and retaining customers as they were required to shift to the cloud, particularly when their on-premises support version was being phased out. The research was conducted in three stages, each with specific objectives: Stage 1: Qualitative Analysis: The objective of this stage was to explore how organizations that use cyber-active defense technology perceived the transition from on-premises software to cloud applications. The focus was on four key areas: perceptions of extended cloud functionalities, new ecosystem integrations, cost savings, and trust in cloud security. Stage 2: Quantitative Analysis: Building on the themes identified in Stage 1, the objective of this stage was to conduct a survey with a broader sample to identify the main components influencing customer behavior. Based on these findings, a model explaining customer behavior was developed, followed by the creation of a value proposition plan to assist cybersecurity marketing departments in migrating customers to cloud or hybrid solutions. Stage 3: Qualitative Validation: Using Delphi expert sessions, the objective was to validate and reach a consensus among experts regarding the customer behavior model and the proposed value proposition plan. Adjustments were made based on expert feedback to refine both the model and the plan.

Research Problem

The research problem centers on the challenges organizations face in adopting cloud technology, especially regarding the shift from traditional on-premises systems. Security concerns and the potential for customer attrition when vendors phase out support for legacy products complicate this transition. By investigating these challenges, the research highlights the need for effective marketing strategies to communicate the benefits of cloud adoption and mitigate the risks associated with moving to cloud environments.

Research Questions

The study is guided by a primary research question (PRQ) regarding the components necessary for developing a value proposition plan for security software vendors transitioning

customers to the cloud. Four secondary research questions (SRQs) further investigate perceptions around the shift to cloud applications, including the influence of extended features, ecosystem integrations, cost savings, and trust in cloud security. Together, these questions aim to provide a comprehensive understanding of the factors affecting customer willingness to migrate from on-premises to cloud solutions.

PART I

THEORETICAL BACKGROUND OF THE RESEARCH

Chapter 1 — Key Terms and Definitions

Cloud computing offers a range of services such as storage, networking, and software over the internet, enhancing organizational flexibility and cost efficiency (NIST, 2011). Software as a Service (SaaS) allows users to access applications like Microsoft Office 365 on a subscription basis, while cyber-active defense technology uses deception techniques to improve cybersecurity (Zhang & Vrizlynn, 2021). The cloud-native approach enables rapid application development without vendor lock-in (Al Kiswani & Hasan Ahmed, 2019), and hybrid clouds provide a blend of public, private, and on-premises environments to facilitate gradual cloud transitions while meeting regulatory needs (Google, 2023).

Chapter 2 — Literature Review

This chapter examines the barriers and drivers of cloud adoption, particularly in the context of cybersecurity. Security concerns, including data privacy and breach risks, were the primary barriers to adopting cloud solutions, especially Software as a Service (SaaS) (Shultz, 2016). Other challenges include insufficient resources, regulatory compliance issues, and training gaps, particularly for smaller organizations (Ivan & Ille, 2021; Griffith & Stewart, 2020). Despite these obstacles, both public and private sectors acknowledge the scalability and cost efficiency benefits of cloud adoption (FutureScape, IDC, 2022).

Regulatory frameworks, such as FedRAMP, NIS2, and DORA, are driving cloud adoption in sectors like finance and IT services by addressing security and compliance concerns (Waizel, 2023; DORA, 2023). AI plays a dual role in this landscape, enhancing cloud security but also

introducing new risks, including AI-driven cyberattacks (Wang et al., 2023; Gonaygunta, 2023). Innovations like federated learning show promise in mitigating these risks by enabling secure, collaborative AI model training (Hacks, 2024).

Overall, cloud adoption in cybersecurity is shaped by both technological and regulatory advancements, with AI and new compliance requirements playing pivotal roles in overcoming traditional barriers.

Chapter 3 — Theoretical Framework

Theories relevant to cloud adoption include transaction cost theory, diffusion of innovations theory, and the Unified Theory of Acceptance and Use of Technology (UTAUT), which address factors like security and customer trust (Sobragi et al., 2014; Liu et al., 2008). Marketing theories, such as stakeholder theory, emphasize integrating customer interests into value propositions (Freeman, 1984; Fishbein et al., 1975). Ongoing AI integration in cybersecurity presents both opportunities and challenges, requiring continuous innovation to combat emerging threats (Waizel, 2024).

Chapter 4 — Conceptual Framework

This chapter introduces a research framework for a strategic marketing plan aimed at developing a value proposition plan for vendors persuading cybersecurity customers to shift from on-premises to cloud product versions. It explores technological concepts, relevant literature, and theories on organizational decisions while identifying gaps in current knowledge and marketing strategies. The chapter also illustrates the researcher's position, research aim, design, research questions, and hypotheses. By employing both qualitative and quantitative methodologies, the study developed a customer behavior model that informs effective marketing strategies to facilitate cloud adoption. The conceptual framework is illustrated in Figure 4.1.

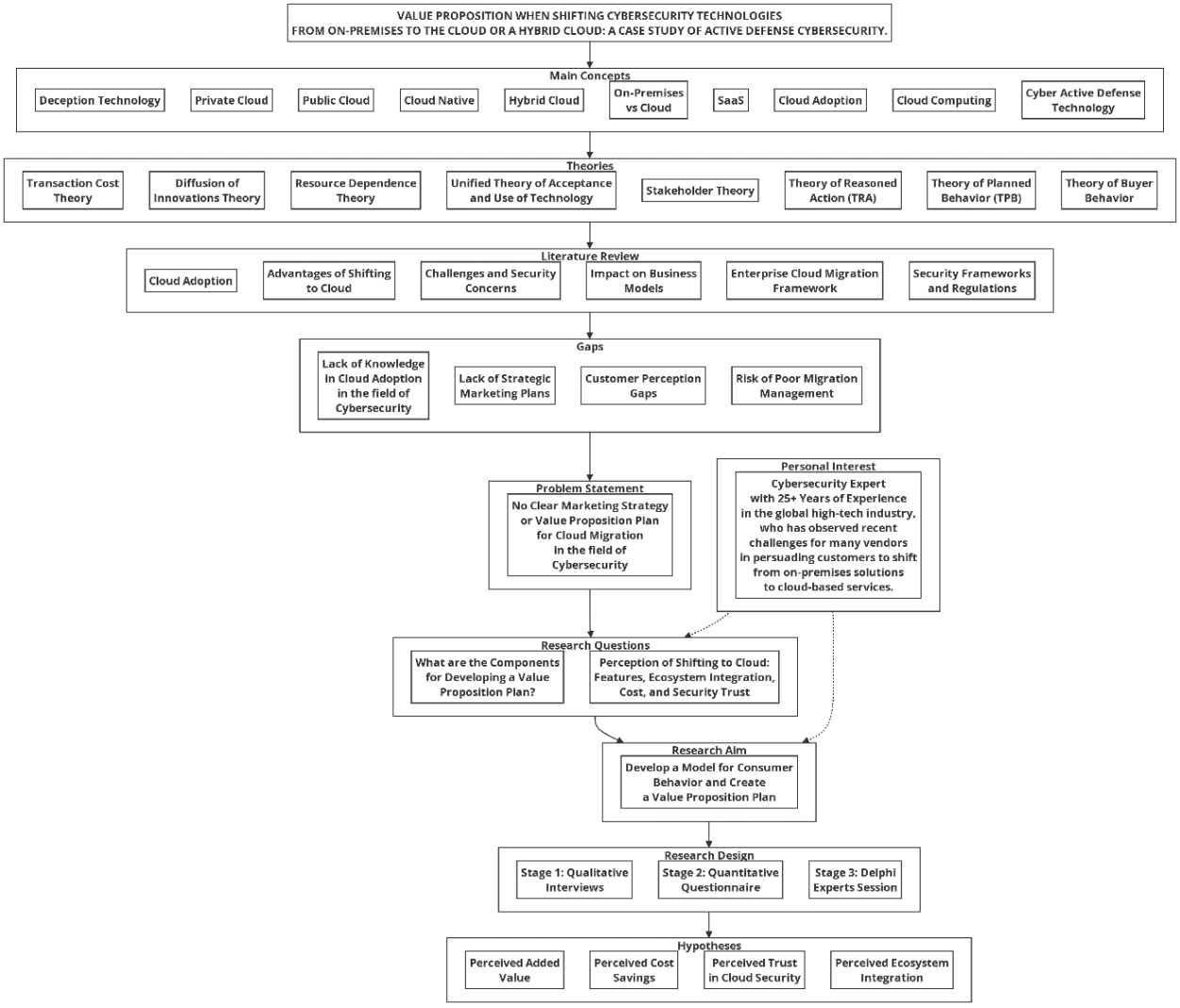


Figure 4.1: Conceptual Framework for the Research

PART II

PERSONAL CONTRIBUTIONS

Chapter 5 — Methodology

The methodology of this research is divided into three stages: qualitative, quantitative, and qualitative validation. The qualitative research aimed to explore organizations' perceptions of the shift from on-premises software to cloud applications, focusing on extended features, ecosystem integrations, cost savings, and trust in cloud security. Data was collected through semi-structured interviews with 13 cybersecurity professionals and analyzed using content analysis. The quantitative analysis aimed to examine the perceptions of a broader sample regarding the factors identified in the first stage, which were used to develop a customer behavior model and a value proposition plan. A closed-ended questionnaire was distributed electronically via GuidedTrack platfom, with SPSS used for data analysis. The survey reached 165 participants recruited through the Positly Platform and LinkedIn. Lastly, Delphi expert sessions were conducted to validate and refine the model and value proposition plan. These sessions involved 8 cybersecurity expert managers and used content analysis for data interpretation.

Chapter 6 — First Stage of the Research: Qualitative Analysis- Interviews

6.1 Purpose and Objectives

The initial phase of this research involved semi-structured interviews with cybersecurity professionals to explore their perceptions of the transition to cloud applications. This qualitative approach addressed specific research questions related to perceptions of cloud functionality, ecosystem integrations, cost savings, and trust in cloud security. The study focused on four key objectives: examining how organizations that use cyber-active defense technology perceive the shift from on-premises software to cloud applications while leveraging extended features and functionalities; exploring perceptions of new cloud ecosystem integrations; analyzing the cost-saving perceptions when migrating from on-premises installations to cloud applications; and exploring perceptions of trust in cloud security during this transition.

6.2 Research Questions

The secondary research questions aligned with the objectives are as follows: SRQ1 investigates how organizations that use cyber-active defense perceive the shift to cloud applications while leveraging extended features; SRQ2 focuses on perceptions of new cloud ecosystem integrations; SRQ3 examines perceptions of cost savings associated with this shift; and SRQ4 focuses on perceptions of trust in cloud security.

6.3 Pilot and Research Tool

The questionnaire was developed based on literature and the researcher's experience in the field. It was validated and piloted with four participants: three meeting the profile defined for this stage, focused on cybersecurity, cloud, and technology, and one providing feedback from a social science perspective regarding the structure of the questionnaire, the order of questions, clarity, language aspects, and communication. Based on this validation and pilot test, the final questionnaire was refined and improved, making it ready for use in the first stage of the research.

6.4 Methodology and Participant Recruitment

The study utilized stratified and purposive sampling to recruit thirteen Israeli security professionals, all with at least two years of cybersecurity experience and decision-making authority regarding cloud transitions. Recruitment initially sought fifteen participants through LinkedIn but shifted to WhatsApp for better scheduling and consent.

6.5 Data Collection Procedures

Participants received a meeting invite and a consent form detailing their rights, with assurances of data anonymity. Interviews lasted between 43-47 minutes and were recorded, accompanied by detailed notes on participants' body language and comfort levels.

6.6 Data Analysis Approach

Content analysis was systematically applied, involving data organization, defining units of analysis, creating and refining codes, and validating results. This process generated 234 codes, 24 categories, and 23 overarching themes aligned with the research questions.

6.7 Findings and Key Themes

The findings highlighted significant themes in organizations' perceptions of cloud transitions, particularly the importance of speed and flexibility in enhancing operational efficiency.

Trust factors related to vendor reliability and compliance emerged as critical influences on decision-making.

6.8 Summary and Implications

This initial research stage successfully addressed the research questions and illuminated the complex relationships influencing perceptions of cloud adoption. The results suggest that embracing cloud technologies can enhance response capabilities, yield cost savings, and necessitate a strategic focus on trust to facilitate effective cloud adoption in the cyber-active defense technology landscape.

Chapter 7 — Second Stage of the Research: Quantitative Analysis- Survey

7.1 Purpose and Objectives

The second phase of the research involved a quantitative analysis using an online survey targeted at specific stakeholders. This closed-ended questionnaire, developed from insights gained in the qualitative interviews, aimed to quantify perceptions among a broader sample of 165 participants regarding previously identified factors and themes. The objective was to develop a model explaining customer behavior, leading to a value proposition plan that assists marketing departments in transitioning customers to cloud or hybrid cloud solutions.

7.2 Primary Research Question and Research Hypotheses

The primary research question for this stage was: What components and considerations are necessary to develop a value proposition plan for security software vendors transitioning customers from traditional on-premises solutions to the cloud or hybrid cloud? The corresponding research hypotheses included: perceived extended value features enhance willingness to migrate; greater ecosystem integration improves willingness; perceived cost savings facilitate the transition; and trust in cloud security positively influences adoption**.**

7.3 Survey Development and Pilot Testing

The survey consisted of 23 perception questions across four dimensions aligned with the research questions. It was pilot tested with five participants for validation, followed by a pilot run with 30 participants (20 from Positly and 10 via LinkedIn). The scales for Cost Saving, Features,

Ecosystem Integration, and Trust were formative, so Cronbach's Alpha was not essential (Diamantopoulos & Siguaw, 2006; Stadler et al., 2021). However, all values exceeded 0.7.

7.4 Participant Recruitment and Sampling

Stratified sampling was used to recruit participants via the Positly platform and LinkedIn, targeting security and IT professionals aged eighteen and older with at least two years of experience, achieving a required sample of 165 participants from both the U.S. and Israel.

7.5 Data Collection Procedures

The online survey was conducted on GuidedTrack platform, ensuring secure data export after completion. Validation checks maintained data quality by removing participants who did not meet the established criteria.

7.6 Data Analysis Methodology

Data analysis was performed using SPSS version 28. Descriptive statistics were first conducted, followed by testing the four hypotheses. The dependent variable, willingness to migrate to the cloud (measured on a 1-10 scale), was examined in relation to four independent ordinal variables: perceived extended features, perceived ecosystem integration, perceived cost savings, and perceived trust in cloud security. Separate Spearman correlation tests were conducted for each hypothesis to assess the correlations between the independent variables and the dependent variable.

To assess whether background variables—such as years of experience, organization size, sector, age, gender, education level, and familiarity with IT/cybersecurity technologies—moderated the correlations, Spearman correlation tests were conducted between each background variable and the dependent variable.

Multiple regression analyses were performed to examine whether education level, familiarity with IT/cybersecurity technologies, age, and customer sector moderated the correlations between the independent variables (perceived features, perceived ecosystem integration, perceived cost savings, and perceived trust) and the dependent variable (willingness to shift to the cloud). Reliability was checked using Cronbach’s Alpha, with all values above 0.7.

7.7 Findings and Insights

The study tested hypotheses that higher perceptions of extended features, ecosystem integration, cost savings, and trust in cloud security would lead to greater willingness to transition to cloud applications. All four hypotheses were confirmed, showing positive correlations between these perceptions and cloud adoption.

The study also examined the influence of demographic and organizational factors on willingness to adopt cloud applications:

Familiarity with IT and cybersecurity technologies and educational level showed significant positive correlations; Age and sector exhibited negative correlations, with age being close to statistically significant.

Linear regression analysis revealed that: Educational level moderated the effect of features and functionalities, weakening their impact; Familiarity with IT and cybersecurity technologies moderated all independent variables, weakening their influence; Age moderated the effect of most independent variables, except for trust; Sector moderated the effect of extended features and functionalities.

These findings highlight the significant role of both perceived demographic and organizational factors, with moderating effects from education, familiarity, age, and sector in shaping cloud adoption willingness.

7.8 Development of the CLIFFDO Model

The developed CLIFFDO model encapsulates key factors influencing security cloud adoption, focusing on cost savings, trust, integrations, features, familiarity, and demographic and organizational factors. It illustrates the interplay among these components and their impact on customer willingness to transition to the cloud, as illustrated in the developed CLIFFDO cybersecurity cloud adoption triangle (Figure 7.8.1) and extended model. (Figure 7.8.2)

C: COST SAVING

L: LEVEL OF TRUST

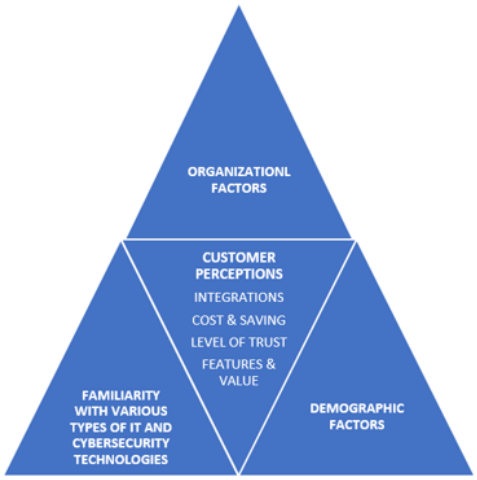
I: INTEGRATIONS

F: FEATURES & VALUE

F: FAMILIARITY

D: DEMOGRAPHIC FACTORS

O: ORGANIZATIONAL FACTORS



CLIFFDO

Symbolize a man (cybersecurity buyer) standing on a CLIFF and DOing Cloud Adoption while he sees the clouds around.

Figure 7.8.1: The CLIFFDO Cybersecurity Cloud Adoption Triangle Model

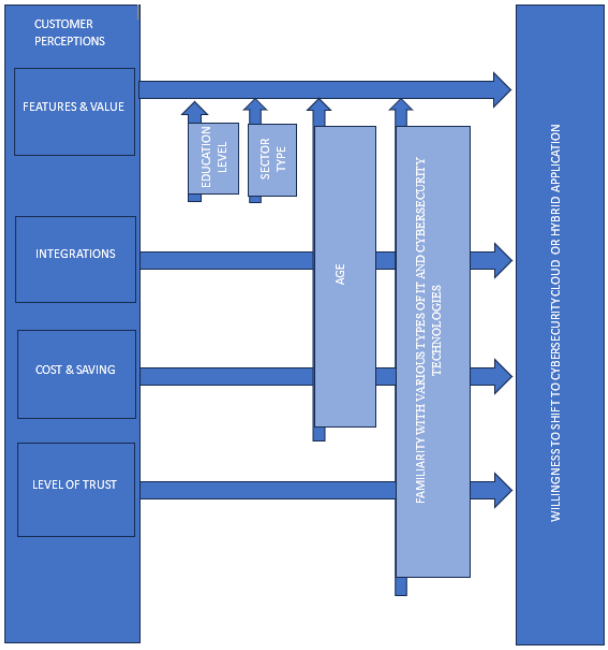


Figure 7.8.2: The developed CLIFFDO cybersecurity cloud adoption extended model

7.9 Recommendations for Value Proposition

Based on the CLIFFDO model, recommendations for a value proposition plan, exemplified by the proposed "Shift2CyberCloud Plus" plan emphasize enhanced features, seamless integrations, cost-saving potential, trusted security, and tailored education for different sectors, addressing diverse customer needs.

7.10 Summary and Implications

The findings illuminate the dynamics affecting customers' willingness to transition to cloud applications in cybersecurity. The identified positive correlations underscore the necessity for vendors to prioritize feature enhancements, ecosystem integrations, cost savings, and trust-building strategies. Recognizing demographic influences enables the development of targeted marketing strategies, ultimately equipping organizations to effectively promote cloud adoption and optimize customer engagement in the evolving cybersecurity landscape.

Chapter 8 — Third Stage of the Research: Qualitative Analysis — Delphi Expert Sessions

8.1 Purpose and Objectives

Delphi expert sessions were conducted with a sample group of eight cybersecurity experts from various industries. The main goal was to validate and achieve consensus on the model explaining consumer behavior during the transition from on-premises cybersecurity technologies to cloud or hybrid cloud solutions, as well as to validate and refine the proposed value proposition plan.

8.2 Primary Research Question

The primary research question for this stage was: What components and considerations may develop a value proposition plan for security software vendors transitioning customers from traditional on-premises solutions to the cloud or a hybrid cloud?

8.3 Pilot and Research Tool

The initial questionnaire guide, based on the CLIFFDO cybersecurity model, was developed and piloted with three experts: a security expert, a marketing expert, and an education sociology expert. The pilot refined the questionnaire by improving clarity, structure, and the inclusion of open-ended questions, ensuring content validity and alignment with the research

objectives. Feedback led to a revised version, which was finalized for use in the first round of the Delphi expert sessions.

8.4 Research Design and Methodology

This research involved Delphi expert sessions aimed at validating the consumer behavior model and refining the value proposition plan. A questionnaire based on the CLIFFDO model was developed and pilot-tested to ensure clarity and validity.

8.5 Data Collection Process

Participants were selected through stratified and purposive sampling via LinkedIn and recruited through WhatsAPP, resulting in a final group of eight Israeli security and IT professionals, each with over five years of relevant experience and decision-making authority. Data was collected through individual Zoom interviews lasting approximately 45 minutes, with responses recorded and field notes taken. Five rounds were used to achieve consensus, understand limitations and considerations, and refine the value proposition plan accordingly.

8.6 Data Analysis and Insights

Content analysis was used to analyze data from the Delphi sessions, refining codes and categories based on participant feedback. This iterative process ensured that the themes aligned with research objectives and were validated through expert consensus.

8.7 Findings and Themes

The Delphi sessions identified eleven key themes for the CLIFFDO model and five additional themes for the value proposition plan. Consensus was reached on several critical factors influencing cloud adoption, including the perceived value of features, trust, and cost-saving potential. Key insights included the trust's role in meeting compliance and regulatory requirements, Migration tools to simplify the shift to the cloud, and Cost-saving potential, varying by deployment model and organizational needs.

Further feedback emphasized the use of interactive formats, educational resources, and case studies to demonstrate value. All considerations and feedback were incorporated into the revised value proposition plan to enhance its effectiveness in promoting cloud adoption.

8.8 Conclusion and Implications

The sessions successfully validated the CLIFFDO cybersecurity cloud application model and provided valuable insights for refining the value proposition plan. Marketing departments should focus on advanced features, seamless integration, and building customer trust, while also emphasizing educational initiatives to communicate the benefits of cloud solutions effectively. This comprehensive approach enhances the appeal of cloud offerings and mitigates risks associated with the transition from on-premises products.

CONCLUSIONS

This research developed a value proposition plan for cybersecurity vendors, focusing on customer behavior during the transition from on-premises to cloud applications. Using a mixed-methods approach, the study began with qualitative interviews, followed by a quantitative survey of IT and security experts. The findings revealed positive perceptions of the cloud transition, particularly regarding extended features, ecosystem integration, cost savings, and trust in cloud security, which led to the creation of the CLIFFDO model to explain customer behavior.

The final phase, Delphi expert sessions, validated and refined the CLIFFDO model and the value proposition plan, enhancing their applicability to marketing strategies. The study highlights the importance of addressing customer concerns to help vendors tailor marketing messages effectively. The CLIFFDO model extends beyond cybersecurity, offering a foundation for future research in sectors like healthcare and finance, where similar cloud adoption challenges exist.

Key insights from this research emphasize the role of perceived value of features, ecosystem integration, and cost savings, while also highlighting the critical role of trust in cloud adoption. The model underscores the importance of seamless integrations and the need for vendors to convey cost-saving benefits and security features. The implications also include moderating effects of demographic factors like educational level, familiarity with technologies, age, and sector, which influence the willingness to adopt cloud solutions. This research contributes to the literature on cloud adoption and provides actionable insights for developing targeted marketing strategies and enhancing customer relationships in the context of cybersecurity and cloud migration.

Contribution to Literature

The implications of these findings are significant and contribute to the existing literature as outlined in Table 9.1

Table 9.1: Research Questions, Literature Connections, Personal Contributions, and Conclusions

Research Question / Component	Current Literature Relation	Contribution to Literature & Conclusion
PRQ & SRQ1 Perceived Extended Value Features & Functionalities	Boillat & Legner (2013), Sobragi et al. (2014), Liu et al. (2008), Ajzen (1985)	CLIFFDO emphasizes advanced cloud features (automation, AI) to differentiate offerings, reinforcing loyalty and aiding transitions from on-premises (Waizel, 2024).
PRQ & SRQ2 Perceived Ecosystem Integration	Dimitrakos (2014), Pfeffer & Salancik (2003), Gonaygunta (2023)	CLIFFDO stresses seamless integrations for enhanced scalability and efficiency, offering strategic advantages for vendors in addressing integration barriers.
PRQ & SRQ3 Perceived Cost Savings	Kundra (2011), Sobragi (2012), Rogers (1995), Howard & Sheth (1969), Murphy (2024)	CLIFFDO demonstrates cost reductions in cloud adoption, emphasizing operational efficiency and resource savings to prevent customer attrition.
PRQ & SRQ4 Perceived Level of Trust	Tawfique & Vejseli (2018), UTAUT (Peake, 2018; Slade et al., 2015; Carter & Bélanger, 2005; Venkatesh et al., 2003), Fishbein & Ajzen (1975), Ables (2023); Praveenraj et al. (2023)	CLIFFDO integrates trust factors (security, transparency, vendor reliability), helping vendors foster customer trust and smooth cloud adoption transitions (Waizel, 2024; Waizel & Zait, 2024).
PRQ Moderating Effects		CLIFFDO acknowledges moderating factors (familiarity, age, education, sector) that influence cloud adoption, allowing vendors to tailor marketing messages effectively.

LIMITS AND FUTURE RESEARCH DIRECTIONS

This research provides a foundation for understanding consumer behavior in transitioning from on-premises cybersecurity solutions to cloud environments, but it has limitations that highlight areas for future study. It primarily focuses on customer perceptions of cloud adoption without capturing the vendor's perspective on migration strategies. Future research could explore how cybersecurity vendors formulate marketing strategies and address customer concerns, offering a more comprehensive view of market challenges. Additionally, applying the value proposition recommendations by marketing departments could provide further insights, and implementing the CLIFFDO model in various industries may reveal different approaches to cloud adoption.

EXTRACTS FROM 155 REFERENCES

Ables, J. (2023). Explainable intrusion detection systems using white box techniques (Order No. 30812542). Available from ProQuest Dissertations & Theses Global. https://www.proquest.com/dissertations-theses/explainable-intrusion-detection-systems-using/docview/2903798888/se-2

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. User Modeling and User-Adapted Interaction, 29, 701-750. https://doi.org/10.1007/s11257-019-09298-2

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. (Eds.), Action control: From cognition to behavior (pp. 11-39). Springer.

Ajzen, I., & Fishbein, M. (2000). Attitudes and the attitude-behavior relation: Reasoned and automatic processes. European review of social psychology, 11(1), 1-33.

Al Kiswani, J. H. A., & Hasan Ahmed, R. (2019). Smart-Cloud: A Framework for Cloud Native Applications Development. Doctoral dissertation, University of Nevada, Reno.

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organizations. Telematics and Informatics, 35(1), 38-54. https://doi.org/10.1016/j.tele.2017.10.001

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organizations. Telematics and Informatics, 35(1), 38-54. https://doi.org/10.1016/j.tele.2017.10.001

Boillat, T., & Legner, C. (2013). From on-premise software to cloud services: The impact of cloud computing on enterprise software vendors' business models. Journal of Theoretical and Applied Electronic Commerce Research, 8(3), 39-58. https://doi.org/10.4067/S0718-18762013000300005

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. British Journal of Management, 17(4), 263-282. https://doi.org/10.1111/j.1467-8551.2006.00500.x

Freeman, R. E. (1984). Strategic management: A stakeholder approach. Pitman.

FutureScape, IDC. (2022). IDC FutureScape: Worldwide IT industry 2022 predictions.

Gai, K. (2014). A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. International Journal of Computer Applications, 95(3), 40-44. https://doi.org/10.5120/16915-9207

Gonaygunta, H. (2023). Factors influencing the adoption of machine learning algorithms to detect cyber threats in the banking industry. Doctoral dissertation. Available from ProQuest Dissertations & Theses Global.

Gonaygunta, H., & Liu, S. (2023). Integrating AI-driven security measures in cloud environments: Threat detection and mitigation strategies. Journal of Cloud Computing and Cybersecurity, 5(2), 98-114. https://doi.org/10.1007/jccc.2023.0976

Gusman, J. (2024). The deployment of artificial intelligence and machine learning within the field of cybersecurity for intelligent decision-making: A qualitative study. ProQuest Dissertations & Theses Global. Available from Publicly Available Content Database. https://www.proquest.com/dissertations-theses/deployment-artificial-intelligence-machine/docview/2863689117/se-2

Hacks, C. (2024). Federated learning: A paradigm shift in data privacy and model training. Medium. https://medium.com/@cloudhacks_/federated-learning-a-paradigm-shift-in-data-privacy-and-model-training-a41519c5fd7e

Ivan, T. R., & Ille, E. E. (2021). Applying multi-criteria decision-making to the technology investment decision-making process. Acquisition Research Program.

NIST. (2011). Managing information security risk: Organization, mission, and information system view (NIST Special Publication No. 800-39). https://doi.org/10.6028/NIST.SP.800-39

Pearson, S. (2013). Privacy, security, and trust in cloud computing. In Privacy and security for cloud computing (pp. 3-42). Springer.

Pfeffer, J., & Salancik, G. R. (2003). The external control of organizations: A resource dependence perspective. Stanford University Press.

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. Computers in Human Behavior, 62, 61-69. https://doi.org/10.1016/j.chb.2016.04.027

Shultz, A. (2016). Controlling the emerging data dilemma: Building policy for unstructured data access. In Information Security Management Handbook (Vol. 5, pp. 229-242). Auerbach Publications.

Sobragi, C. G., Maçada, A. C. G., & Oliveira, M. (2014). Cloud computing adoption: A multiple case study. BASE: Revista de Administração e Contabilidade da Unisinos, 11(1), 75-91. https://doi.org/10.4013/base.2014.11.1.07

Waizel, G. (2023a). A qualitative analysis of cloud adoption in the public and private sectors from cybersecurity vendors' perspective. Review of Economic and Business Studies, 31, 19-37.

Waizel, G. (2023b). The potential effects of recent EU cybersecurity and resilience regulations on cloud adoption and EU cyber resilience. Centre for European Studies (CES) Working Papers, 15(3).

Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. In International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings (Vol. 1, pp. 141-156).

Wang, Y., Yan, Q., Ivanov, N., & Chen, X. (2023). A practical survey on emerging threats from AI-driven voice attacks: How vulnerable are commercial voice control systems? Journal of Cybersecurity and Privacy, 1(2), 123-146. https://doi.org/10.3390/jcp1020008

Zhang, L., & Vrizlynn, L. L. T. (2021). Three decades of deception techniques in active cyber defense: Retrospect and outlook. Cornell University Library, arXiv.org. https://doi.org/10.1016/j.cose.2021.102288

Zhang, X., & Yue, W. T. (2020). Integration of on-premises and cloud-based software: The product bundling perspective. Journal of the Association for Information Systems. https://doi.org/10.17705/1jais.00524