International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)

International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS Journal) | ISSN (e): 2808-4713
Volumes 6 No. 3 (2026)

IMPROVING MANAGED SECURITY SERVICE ADOPTION THROUGH GO-TO-MARKET STRATEGY TRANSFORMATION: A CASE STUDY OF SQURA CYBERSEC

Imam Rizky Hambali[1], Utomo Sarjono Putro[2]
School of Business and Management, Institut Teknologi Bandung/Indonesia
School of Business and Management, Institut Teknologi Bandung / Indonesia
E-mail: imam.rizkyhambali@gmail.com[1], utomo@sbm-itb.ac.id[2]

Received	: 26 April 2026	Accepted	: 20 May 2026
Revised	: 03 May 2026	Published	: 17 June 2026

Abstract

Indonesia's cybersecurity industry continues to experience rapid growth driven by digital transformation, cloud adoption, increasing cyber threats, and stronger cybersecurity regulations. However, cybersecurity providers continue to face challenges in accelerating Managed Security Service Provider (MSSP) adoption and achieving sustainable recurring revenue growth. This study aims to analyze the internal and external factors influencing MSSP adoption and formulate strategic recommendations to improve the cybersecurity Go-To-Market (GTM) strategy of SQURA Cybersec at PT Aplikanusa Lintasarta. A qualitative case study approach was taken, involving semi-structured interviews with internal stakeholders, enterprise customers and cybersecurity technology principals. The collected data were analysed using thematic coding and interpreted using PESTEL Analysis, Porter's Five Forces, VRIO Analysis, SWOT Analysis, TOWS Matrix, Segmentation–Targeting-positioning (STP) and 7P Marketing Mix framework. The findings show the key challenge, not the lack of cybersecurity capability but how to convert operational capability into sustainable market differentiation and scalable execution. The study identifies major barriers to MSSP adoption as principal dependence, fractured commercial communication, inconsistent service packaging and poor operational coordination. To tackle these challenges, we propose four strategic directions to reinforce market positioning, enhance service integration, fortify proprietary capability development and introduce a more disciplined operating model to support the growth of recurring revenue.

Keywords: Cybersecurity Strategy; Go-To-Market Strategy; Managed Security Services; MSSP; Recurring Revenue

INTRODUCTION

Indonesia's digital economy continues to expand rapidly, driven by increasing internet penetration, cloud computing adoption, and digital transformation initiatives across both public and private sectors. At the same time, the frequency and sophistication of cyber threats continue to increase, making cybersecurity a strategic priority for organizations operating in highly connected digital environments (World Economic Forum, 2024; BSSN, 2024). Consequently, cybersecurity spending and demand for advanced security solutions have grown significantly, creating new opportunities and challenges for cybersecurity service providers.

As cybersecurity threats become more complex, organizations are increasingly shifting their focus from purchasing standalone security products toward acquiring integrated security services that provide continuous monitoring, incident response, threat intelligence, and compliance support. This trend has accelerated the adoption of Managed Security Service Provider (MSSP) models, enabling organizations to access specialized cybersecurity capabilities without maintaining large internal security teams (Tiwana, 2014). Furthermore, customers increasingly expect cybersecurity providers to deliver measurable business outcomes rather than simply supplying technology products (Kotler et al., 2021). Despite increased demand for managed security services, cybersecurity providers continue to struggle to commercialise MSSP offerings effectively. Industry competition is heating up as global technology vendors, system integrators, telecommunications operators and specialist cybersecurity companies are competing for the same customer segments.. As a result, sustainable differentiation increasingly depends on service quality, customer experience, and the ability to communicate value beyond technology features (Porter, 2008).

One example is SQURA Cybersec, which is the cybersecurity strategic business unit of PT Aplikanusa Lintasarta. Company has deep operational capabilities, SOC infrastructure, strategic partnerships with technology vendors, and access to enterprise customers but subscription-based growth is below strategic expectations. The company still struggles with market differentiation, customer value messaging, principal dependency, fragmented service packaging and inconsistent execution across GTM related functions. Previous researches have mainly focused on adoption of cybersecurity technology, governance frameworks and organisational readiness. There are few studies on cybersecurity Go-To-Market (GTM) strategy from strategic management perspective, especially on MSSP adoption in emerging markets like Indonesia. This gap highlights the need for a more comprehensive analysis that integrates internal capability assessment, external market analysis, and strategic marketing perspectives (Yin, 2018; Creswell & Poth, 2018). Therefore, this study aims to analyse the internal and external factors affecting MSSP adoption and develop strategic recommendations to enhance SQURA's cybersecurity Go-To-Market (GTM) strategy. The study adopts a qualitative case study approach supported by PESTEL Analysis, Porters's Five Forces, VRIO Analysis, SWOT Analysis, TOWS Matrix, Segmentation-Targeting-Positioning (STP) and the 7P Marketing Mix framework to help SQURA transit from a transactional cybersecurity business model to a sustainable recurring service-based model.

LITERATURE REVIEW

Go-To-Market (GTM) Strategy

Go-To-Market (GTM) strategy refers to a structured approach used by organizations to deliver products and services to target markets while creating sustainable competitive advantage. A GTM strategy encompasses customer segmentation, value proposition development, channel selection, pricing strategy, and customer engagement activities designed to accelerate market adoption and revenue growth (Kotler et al., 2021). In service-based industries, an effective GTM strategy plays a critical role in aligning organizational capabilities with customer needs and market opportunities.

PESTEL Analysis

PESTEL Analysis is a strategic framework used to evaluate external macro-environmental factors affecting business performance. The framework examines Political, Economic, Social, Technological, Environmental, and Legal dimensions that may create opportunities or threats for an organization. PESTEL helps organizations understand external conditions and anticipate environmental changes that may influence strategic decisions (Johnson et al., 2020).

Porter's Five Forces Analysis

Porter's Five Forces framework analyzes industry attractiveness and competitive intensity through five dimensions: rivalry among existing competitors, bargaining power of buyers, bargaining power of suppliers, threat of new entrants, and threat of substitute products or services. The framework assists organizations in understanding industry structure and identifying factors that influence long-term profitability and competitive positioning (Porter, 2008).

VRIO Analysis

VRIO Analysis is an internal strategic assessment framework that evaluates organizational resources and capabilities based on four dimensions: Value, Rarity, Imitability, and Organization. Resources that satisfy all four dimensions may become sources of sustainable competitive advantage and contribute to superior organizational performance (Barney & Hesterly, 2015).

SWOT and TOWS Analysis

SWOT Analysis is used to identify organizational Strengths, Weaknesses, Opportunities, and Threats by integrating internal and external strategic factors. The framework provides a structured understanding of an organization's strategic position. Building upon SWOT, the TOWS Matrix systematically combines these factors to generate strategic alternatives by matching internal capabilities with external environmental conditions (Weihrich, 1982).

Segmentation, Targeting, and Positioning (STP)

The Segmentation, Targeting, and Positioning (STP) framework is widely used in strategic marketing to identify attractive customer segments, select priority target markets, and develop a differentiated market position. The framework supports organizations in aligning their value propositions with customer needs and improving market effectiveness (Kotler et al., 2021).

Marketing Mix (7P)

The 7P Marketing Mix extends the traditional marketing mix by incorporating People, Process, and Physical Evidence alongside Product, Price, Place, and Promotion. The framework is particularly relevant in service industries because it provides a comprehensive approach for designing, delivering, and communicating customer value (Kotler et al., 2021).

METHOD

Data Collection Method

This research used a qualitative research method with single case study design to study the strategic challenges in the adoption of Managed Security Service Provider (MSSP) in SQURA Cybersec as a cybersecurity strategic business unit of PT Aplikanusa Lintasarta. A qualitative approach was chosen in order to gain in-depth knowledge of the organisational capabilities, market dynamics, customer expectations and industry perspectives regarding the adoption of cybersecurity services. Primary data was gathered through semi-structured interviews from purposively selected respondents of internal and external stakeholders. Internal respondents included the Chief Cybersecurity Officer (CCSO), GTM Team and Account Manager. External respondents were an enterprise customer representative and a principal representative of cybersecurity technology. These stakeholders were selected based on their direct involvement in the formulation of cybersecurity strategy, the provision of services, and the engagement of customers and the development of the industry ecosystem. The secondary data were obtained from academic journals, industry reports, cyber security publications, company documents, market intelligence reports and regulatory references on cyber security services, digital transformation and strategic management.

Table 1. Interviewee Profile

Initial	Stakeholder Category	Position
WA	Internal	Chief Cybersecurity Officer (CCSO)
H	Internal	Go-To-Market Representative
PS	Internal	Account Manager
TA	External	Enterprise Customer Representative
NH	External	Principal Representative

Data Analysis Method

The study applied thematic analysis to process and interpret qualitative interview data. Interview transcripts were reviewed and coded systematically to identify recurring patterns, themes, and strategic issues related to MSSP adoption. Similar codes were grouped into broader themes to facilitate the identification of internal strengths and weaknesses, as well as external opportunities and threats. External environmental factors were analyzed using PESTEL Analysis and Porter's Five Forces framework. PESTEL Analysis was utilized to examine political, economic, social, technological, environmental, and legal factors influencing the cybersecurity industry, while Porter's Five Forces was employed to evaluate industry competitiveness and market dynamics. Internal organizational capabilities were assessed using the VRIO framework to determine resources and competencies that contribute to sustainable competitive advantage. The findings from the external and internal analyses were subsequently synthesized through SWOT Analysis to identify key strategic factors. A TOWS Matrix was then developed to formulate strategic alternatives by aligning organizational capabilities with external market conditions.

Finally, the selected strategic alternatives were translated into managerial recommendations through the application of Segmentation, Targeting, and Positioning (STP) and the 7P Marketing Mix framework to support the development of an improved cybersecurity Go-To-Market strategy for SQURA Cybersec.

RESULTS AND DISCUSSION

External Environment Analysis

External environment analysis indicates that the Indonesian cybersecurity market offers significant growth potential but also faces increasing competitive pressures. The PESTEL analysis shows that the regulatory developments such as the Personal Data Protection Law (UU PDP), sector-specific regulations issued by the Financial Services Authority (OJK), and the cybersecurity initiatives promoted by the National Cyber and Crypto Agency (BSSN) have raised the organisational awareness of cybersecurity risk and compliance requirements. Such regulatory developments create a fertile ground for the adoption of cyber security services, particularly in highly regulated sectors such as the financial services, telecommunications, government institutions and critical infrastructure organizations. From an economic perspective, cybersecurity spending across industries continues to be high because of digital transformation initiatives. However, many organizations still prefer capital expenditure (CapEx)-based technology purchases over recurring service subscriptions, which poses challenges for MSSP adoption. Socially, increased awareness of executive leadership about cyber risk has raised cybersecurity from an IT issue to a strategic business issue.

The Porter's Five Forces analysis reveals that the competitive rivalry intensity in the cybersecurity industry is high. Customers can choose from a rich selection of options, including global technology vendors, system integrators, telecommunications operators and specialised MSSPs. The bargaining power of buyers is also important as enterprise customers have many vendor options and increasingly sophisticated procurement processes. Moreover, the major technology vendors have a significant influence on the technology selection decision, which enhances supplier power in the cybersecurity ecosystem. These findings imply that sustainable differentiation would not only depend on technology offerings but also need to be supported by better service delivery, customer experience and outcome-based value propositions.

Internal Capability Analysis

The VRIO analysis reveals that SQURA possesses several valuable organisational capabilities that contribute to its competitive standing in the cybersecurity market. Its strength lies in the company's ecosystem support through PT Aplikanusa Lintasarta, existing relationships with enterprise customers, Security Operations Center (SOC) capabilities, experience in managed security services, and partnerships with leading cybersecurity technology vendors. Many of these capabilities are valuable and difficult to replicate, especially the combination of cybersecurity operational expertise, enterprise customer access and integrated service delivery capability. The analysis also reveals a number of organisational constraints that prevent the firm from fully exploiting these advantages. Limitations include dependence on core technologies, fragmented commercial messaging, inconsistent service bundling and limited proprietary cybersecurity assets. SQURA's technical and operational capabilities are good, but the organization has not yet fully translated these capabilities into clear market differentiation. As a result, customers often view cybersecurity offerings as a technology solution, rather than the broader business value delivered through managed security services.

SWOT and TOWS Analysis

The integration of external and internal findings from SWOT analysis exposes a variety of strategic issues affecting MSSP adoption. Key strengths include ecosystem support, access to enterprise customers, operational cybersecurity expertise and managed security service capabilities. Weaknesses are: dependence on principals; lack of unified communication of value; limited proprietary assets; and inconsistent execution processes.

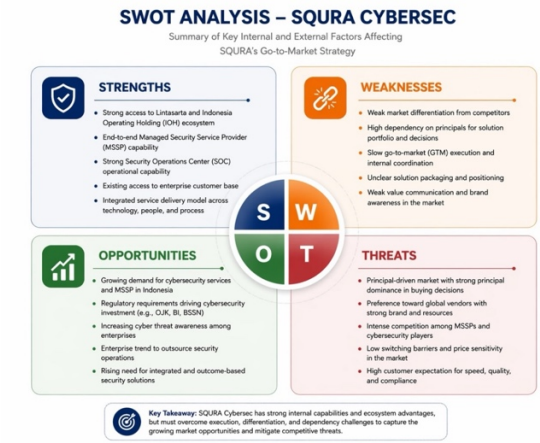

Figure 1. SWOT Analysis (author analysis)

Opportunities on the outside include: increased cybersecurity awareness, expanded regulatory requirements, increased demand for managed services, and continued digital transformation initiatives. Meanwhile, threats include fierce market competition, substantial principal impact on customer buying decisions, talent shortages and a persistent customer preference for traditional technology procurement methods. The TOWS analysis synthesizes these aspects into four strategic pathways to enhance SQURA's competitive position and encourage MSSP uptake. These strategic directions are not isolated initiatives, but rather an integrated transformation framework.

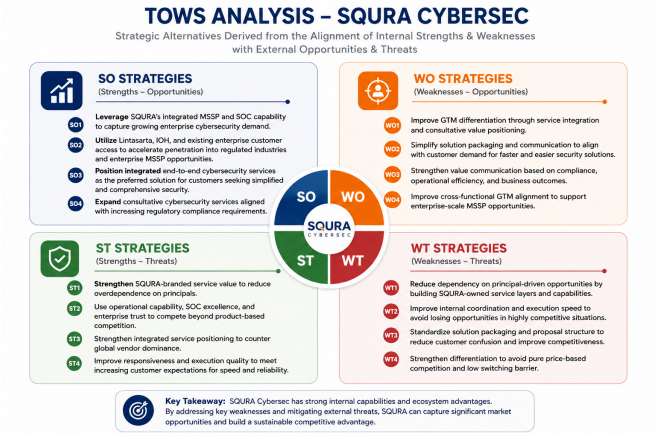

Figure 2. TOWS Analysis (author analysis)

STP Strategy

Segmentation

Industry verticals, cybersecurity maturity, regulatory exposure, and operational complexity segmented the market. The analysis identified financial services, telecommunications, government institutions and large enterprises as the most attractive segments because of their high cybersecurity requirements and increasing regulatory obligations.

Targeting

SQURA should focus on enterprise organisations in highly regulated industries that require always-on cybersecurity operations but have limited internal cybersecurity resources. These companies have higher demand for MSSP solutions and recurring cybersecurity services.

Positioning

SQURA needs to position itself as an integrated security partner that delivers measurable business outcomes via managed security services and not as a traditional technology reseller. The positioning proposed emphasises resilience, compliance readiness, operational continuity and cybersecurity foresight.

7P Marketing Mix

Table 2. Proposed 7P Marketing Mix

Element	Strategic Direction
Product	Integrated MSSP offerings supported by the SQURA Orchestrated Platform
Price	Outcome-based subscription pricing aligned with customer value realization
Place	Direct enterprise engagement supported by ecosystem partnerships
Promotion	Outcome-focused communication emphasizing resilience, compliance, continuity, and foresight
People	Dedicated GTM, customer success, and cybersecurity specialist teams
Process	Integrated operating model with standardized customer journey and governance
Physical Evidence	Unified cybersecurity dashboard, executive reporting, compliance reporting, and service performance metrics

The STP and 7P analyses translate the strategic recommendations into practical Go-To-Market initiatives. The proposed positioning focuses on business outcomes rather than technology features, while the marketing mix aligns service design, pricing, promotion, operational processes, and customer experience with the objective of accelerating MSSP adoption and recurring revenue growth.

Strategic Recommendations

SQURA Orchestrated Platform

The integration of external and internal findings through SWOT analysis highlights several strategic issues influencing MSSP adoption. Key strengths include ecosystem support, enterprise customer access, operational cybersecurity expertise, and managed security service capabilities. Key weaknesses include principal dependency, fragmented value communication, limited proprietary assets, and inconsistent execution processes.

Outcome-Based Commercial Architecture

The second strategic direction transforms SQURA's market positioning from technology-centric selling toward outcome-based value communication. Four customer outcome commitments are proposed: Resilience, Compliance Ready, Continuity, and Foresight. These commitments translate cybersecurity capabilities into business-relevant outcomes that are easier for executive decision makers to understand and evaluate.

SQURA Orchestrated Platform

The third strategic direction addresses principal dependency by developing proprietary cybersecurity capabilities tailored to the needs of the Indonesian market. The proposed approach is focused on cybersecurity compliance and risk management solutions based on local regulatory frameworks such as UU PDP, OJK regulations, and BSSN requirements. The aim of the initiative is to boost strategic autonomy while increasing market differentiation.

Integrated Operating Model

The fourth strategic direction establishes an integrated operating model that aligns sales, marketing, solution, customer success, and delivery functions. The model aims to improve operational coordination, standardize service packaging, strengthen governance, and increase execution consistency. Because all customer-facing initiatives depend on reliable execution, this strategic direction serves as the foundational enabler supporting the successful implementation of the other three initiatives.

Discussion

The findings demonstrate that the primary challenge facing SQURA is not the absence of cybersecurity capability, but rather the difficulty of transforming existing operational strengths into sustainable market differentiation and recurring revenue growth. This finding supports previous strategic management literature suggesting that competitive advantage increasingly depends on the organization's ability to align internal capabilities with evolving customer expectations and market conditions. The proposed transformation framework contributes to cybersecurity GTM literature by integrating market positioning, service innovation, proprietary capability development, and operational execution into a unified strategic model. Rather than focusing exclusively on technology acquisition, the framework emphasizes customer outcomes, service integration, and organizational capability development as key drivers of MSSP adoption within emerging cybersecurity markets.

CONCLUSION

The results suggest that the main challenge for SQURA is not a lack of cybersecurity capability but the challenge of translating operational capabilities into a clear market differentiation and customer perceived value. The analysis revealed that the biggest challenges to fast-tracking MSSP adoption are principal dependency, fragmented commercial communication, inconsistent service packaging, and poor cross-functional execution. Meanwhile, the growing awareness around cybersecurity, regulatory requirements and increasing demand for managed security services provide tremendous opportunities for future growth. The study puts forward four integrated strategic directions to address these challenges: SQURA Orchestrated Platform, Outcome-Based Commercial Architecture, Proprietary Cybersecurity Capability Development, and an Integrated Operating Model. Taken together, these initiatives represent a comprehensive transformation framework that will strengthen market positioning, integrate services, reduce strategic dependence on external vendors, and improve organizational execution capability. The study contributes to the cybersecurity GTM literature by demonstrating how internal capabilities, external market dynamics and strategic marketing approaches can be integrated in a unified framework to accelerate MSSP adoption in emerging markets. From a managerial perspective, the proposed framework offers practical guidance for cybersecurity service providers to move from a transactional technology sales to a sustainable recurring service-based business model.

REFERENCES

Barney, J. B., & Hesterly, W. S. (2015). Strategic Management and Competitive Advantage: Concepts and Cases (5th ed.). Pearson.

Badan Siber dan Sandi Negara (BSSN). (2024). National Cybersecurity Landscape Report. Jakarta: BSSN.

Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th ed.). Sage Publications.

Deloitte. (2024). Cybersecurity Outlook 2024. Deloitte Insights.

Johnson, G., Scholes, K., & Whittington, R. (2020). Exploring Strategy (12th ed.). Pearson Education.

Kotler, P., Keller, K. L., & Chernev, A. (2021). Marketing Management (16th ed.). Pearson.

Porter, M. E. (2008). The Five Competitive Forces That Shape Strategy. Harvard Business Review, 86(1), 78–93.

Tiwana, A. (2014). Platform Ecosystems: Aligning Architecture, Governance, and Strategy. Morgan Kaufmann.

Weihrich, H. (1982). The TOWS Matrix—A Tool for Situational Analysis. Long Range Planning, 15(2), 54–66.

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. Geneva: World Economic Forum.

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Sage Publications.