Business Analytics for Dual-Channel SaaS Pricing under Demand, Supply, and Cybersecurity Risk

Aiman Farid Rahman[1], Nur Aisyah Hassan[2], Kelvin T. Lim[3,*]

[1]School of Business and Economics, Universiti Malaysia Sabah, Kota Kinabalu 88400, Malaysia

[2]Faculty of Business and Management, Universiti Teknologi MARA, Shah Alam 40450, Malaysia

[3]Faculty of Computing and Informatics, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia

*Email: ktlim@unimas.my (Corresponding Author)

Abstract

Software-as-a-service (SaaS) firms increasingly sell through dual channels: low-friction self-service subscriptions for individual users and negotiated enterprise contracts for organizational clients. This structure improves market reach but also exposes pricing decisions to demand volatility, cloud supply uncertainty, information asymmetry with infrastructure partners, and cybersecurity-related trust losses. This article develops a business analytics framework for dual-channel SaaS pricing under demand, supply, and cybersecurity risk. Instead of extending a purely mathematical service supply chain model, the study translates the problem into an analytics-driven pricing architecture that combines demand segmentation, cloud-capacity planning, risk scoring, and governance-aware scenario analysis. A stylized numerical experiment is designed for a mid-sized SaaS provider operating B2C and B2B channels. Six scenarios are compared: a transparent benchmark, infrastructure information gaps, stochastic demand, cloud supply risk, cybersecurity exposure, and analytics-enabled mitigation. The results show that unmanaged information and risk reduce expected quarterly operating profit from USD 2.86 million to USD 2.31 million, while analytics-enabled mitigation recovers USD 0.28 million and improves the final profit to USD 2.59 million. Channel-level analysis indicates that the B2B segment is less price-sensitive but more vulnerable to security and service-level shocks, whereas the B2C segment is more sensitive to demand volatility and churn. The study contributes to business analytics research by showing how pricing, capacity, and cybersecurity decisions can be evaluated in one managerial framework without relying on excessive formulaic complexity. The findings provide practical guidance for SaaS managers who must align subscription pricing, cloud commitments, and digital trust investment under uncertainty.

Keywords: SaaS、dual-channel pricing; demand volatility; cloud supply risk; cybersecurity risk; information asymmetry; business analytics; profit assessment; customer segmentation

Article History:

Received: April 23, 2023

Revised: June 18, 2023

Accepted: August 21, 2023

Available Online: September 30, 2023

 https://doi.org/10.63646/jbda.2023.010304

Business Analytics for Dual-Channel SaaS Pricing under Demand, Supply, and Cybersecurity Risk

1. Introduction

SaaS markets have become a dominant form of digital service delivery because they combine recurring revenue, rapid product updates, scalable cloud infrastructure, and data-rich customer interaction. However, the operational economics of SaaS differ from those of traditional software licensing. A SaaS provider does not simply set a price and deliver a static product. It continuously manages subscription conversion, usage intensity, cloud capacity, service reliability, enterprise-level contractual obligations, and user trust. Pricing decisions are therefore inseparable from analytics decisions. A price reduction may increase new sign-ups, but it may also raise computing demand, customer support pressure, and exposure to security incidents. A price increase may improve revenue per account, but it can weaken adoption in the self-service channel and intensify churn among smaller users. These interdependencies make SaaS pricing a suitable topic for business analytics research. Cloud delivery makes subscription growth operationally scalable but also shifts many cost decisions into vendor-managed infrastructure (Armbrust et al.,2010). The information gap between a SaaS firm and its infrastructure partner reflects a classic quality-uncertainty problem (Akerlof,1970).

The dual-channel structure of SaaS increases the complexity of the problem. The B2C channel is usually composed of individual professionals, small creators, students, and microbusinesses who subscribe through public websites or app stores. This segment is highly visible to marketing analytics and often reacts quickly to price, product changes, promotions, and competitor offers. The B2B channel is different. It involves corporate teams, public agencies, universities, or medium-sized firms that purchase seats through negotiated contracts, annual agreements, service-level commitments, and security reviews. B2B customers are normally less price-sensitive than individual users, but they impose stricter requirements on data protection, uptime, compliance documentation, and account-level support. A single B2B churn event may remove more revenue than thousands of individual downgrades, while a B2B breach incident may cause reputational and legal damage beyond direct technical recovery costs. Recent work on language models in supply-chain finance further shows how analytics interfaces can reshape risk interpretation (Yang et al.,2025). A pricing model that learns under demand uncertainty is aligned with research on dynamic pricing without full demand knowledge (Besbes and Zeevi,2009).

The operational foundation of this article is a two-sided SaaS service chain. A SaaS provider designs and sells software subscriptions, while an external cloud infrastructure partner supplies computing, storage, network capacity, and security-related platform services. The SaaS provider is closer to market demand and therefore has richer information about conversion, churn, willingness to pay, and user behavior. The cloud partner, however, has better information about infrastructure costs, reserved capacity, congestion risk, latency, and service recovery capability. This difference creates information asymmetry. Even when the two firms have a formal contract, both parties may retain private information. The SaaS provider may overstate demand forecasts to negotiate better capacity terms, while the cloud provider may quote a higher capacity price if the customer cannot observe its true cost or congestion state. The result is a pricing and capacity decision that may be privately rational but systemically inefficient. The integration of operational data and decision rules is consistent with the broader role of analytics in operations management (Choi et al.,2018). Industry 4.0 research supports the view that digital services increasingly depend on interconnected data and platform infrastructures (Lu,2025).

The broader research direction on dual-channel service-chain risk motivates the present study, but this article deliberately shifts the emphasis from general service supply chain optimization to SaaS business analytics. The focus is not to reproduce a Stackelberg game model or to present a heavy formula-based derivation. Instead, the article asks a more managerial question: how can a SaaS firm organize data, risk signals, pricing rules, and scenario experiments so that it can make better dual-channel pricing decisions under demand, supply, and cybersecurity risk? This question is important

 https://doi.org/10.63646/jbda.2023.010304

because many SaaS firms already collect large quantities of product usage and transaction data, yet the insights are often used separately by marketing, finance, infrastructure engineering, and security teams. Fragmented analytics can create a false sense of precision, because a pricing dashboard may show strong conversion improvement while the infrastructure and cybersecurity cost of the same decision remains invisible. From a business perspective, cloud adoption changes not only cost structures but also risk ownership in digital services (Marston et al.,2011). The dual-channel logic also resembles two-sided information-product design because each market segment influences platform value (Parker and Van Alstyne,2005).

This article develops a business analytics framework that links three risk dimensions with pricing decisions. Demand risk refers to uncertainty in acquisition, conversion, churn, seat expansion, and usage intensity. Supply risk refers to cloud infrastructure uncertainty, including capacity shortage, API latency, data-center incidents, and reserve-cost volatility. Cybersecurity risk refers to the expected business loss from breaches, ransomware, unauthorized access, account takeover, compliance penalties, and trust deterioration. These risks are not independent in practice. A price promotion may create a demand surge, which increases cloud load and expands the attack surface. A cloud incident may damage enterprise service-level performance and trigger credit or contract renegotiation. A security incident may reduce new customer acquisition and increase churn even if the technical service remains operational. The movement toward Web 3.0 reinforces the need to evaluate digital trust, data control, and service governance together (Zhang and Lu,2025). The use of scenario experiments in this article is consistent with analytics-based demand forecasting and price optimization for online firms (Ferreira et al.,2016).

The main contribution of the article is threefold. First, it reframes dual-channel service pricing as an integrated business analytics problem in which demand forecasting, capacity planning, risk scoring, and cybersecurity investment are jointly interpreted. Second, it provides a data-oriented scenario experiment using realistic but stylized SaaS parameter values, which makes the framework understandable for managers without extensive mathematical background. Third, it derives channel-level managerial implications for balancing B2C growth and B2B stability under risk. The article shows that the B2B channel has stronger profit potential but also stronger exposure to supply and cyber risks, while the B2C channel is more sensitive to price and demand variability. These insights support differentiated pricing governance rather than a single universal SaaS pricing rule. Cybersecurity spending is modeled as an economic decision because risk reduction should be compared with marginal investment cost (Gordon and Loeb,2002). The proposed analytics layer is also motivated by the role of data science in redesigning supply-chain decisions (Waller and Fawcett,2013).

The remainder of this paper is organized as follows. Section 2 reviews research streams related to SaaS pricing, business analytics, supply chain risk, dual-channel management, and cybersecurity economics. Section 3 introduces the research context and analytics framework. Section 4 presents the scenario design and risk logic. Section 5 reports numerical experiments and channel-level decomposition. Section 6 conducts sensitivity analysis. Section 7 discusses managerial implications, limitations, and future extensions. Section 8 concludes the study. Emerging financial-technology research also emphasizes that digital platforms increasingly combine analytics, risk control, and automation (Kou and Lu,2025). The pricing component draws on the long tradition of pricing under stochastic demand over finite horizons (Gallego and Van Ryzin,1994).

2. Literature Review

2.1 SaaS Pricing and Dual-Channel Digital Services

Pricing research has long recognized that firms serving heterogeneous customer groups should not rely on one uniform price. SaaS markets make this principle more visible because a provider can combine free trials, self-service monthly plans, annual individual plans, team subscriptions, and enterprise contracts. The B2C plan often works as an acquisition engine. It creates product awareness, generates usage data, and allows

the firm to observe willingness to pay on a scale. The B2B plan operates as a revenue stabilizer because enterprise accounts are larger, contract periods are longer, and switching costs are higher. However, a dual-channel structure also creates strategic tension. If the public self-service price is too low, enterprise customers may challenge negotiated rates. If enterprise features are too aggressively bundled, individual customers may perceive the basic plan as unattractive. Cybersecurity risk is linked to privacy economics because data exposure can change customer trust and willingness to pay (Acquisti et al.,2016). The article separates B2C and B2B behavior because multi-channel research shows that channels differ in both role and customer response (Verhoef et al.,2015).

The literature on dual-channel supply chains emphasizes pricing coordination, service differentiation, and channel conflict. Studies of manufacturer-retailer direct channels show that a second channel can raise total system profit but may also create price competition and incentive misalignment. Work on service competition similarly indicates that service-level differentiation can reduce destructive price rivalry when customer expectations differ across channels. SaaS markets add another layer because the product is continuously consumed through digital infrastructure. The marginal cost of one additional subscription may appear low, but usage intensity, storage, model inference, support, compliance review, and security monitoring can generate substantial variable costs. Therefore, pricing decisions cannot be separated from capacity and risk analytics. Blockchain research in Industry 4.0 similarly highlights transparency as a mechanism for reducing operational uncertainty (Chen et al.,2024). The cybersecurity component treats security as an incentive problem rather than only a technical control problem (Anderson and Moore,2006).

Unlike physical products, SaaS services also exhibit high observability. Providers collect fine-grained data on logins, feature usage, session frequency, API calls, collaboration patterns, support tickets, and billing events. These data permit dynamic segmentation and predictive churn modeling. However, observability does not automatically produce good pricing decisions. A dashboard that tracks monthly recurring revenue may miss cloud risk. A dashboard that tracks compute utilization may miss customer willingness to pay. A security dashboard may measure vulnerabilities without translating them into pricing or contract terms. The business analytics challenge is to connect these views in one decision structure. The pricing scenarios build on revenue-management research that links price choice with capacity allocation (Bitran and Caldentey,2003). AI-enabled supply-chain research motivates the use of predictive models as inputs to managerial pricing decisions (Toorajipour et al.,2021).

2.2 Demand Risk, Subscription Behavior, and Analytics

Demand risk in SaaS differs from demand risk in one-time product sales. A subscription decision creates an ongoing relationship. Demand includes acquisition, activation, retention, expansion, contraction, and cancellation. For B2C users, demand uncertainty is often driven by marketing campaigns, seasonal needs, peer influence, product updates, competitor discounts, and user experience friction. For B2B clients, demand uncertainty is shaped by budget cycles, procurement procedures, security approvals, departmental expansion, and integration with enterprise systems. These differences imply that the same pricing action may have different demand effects across channels. IoT cybersecurity research is relevant because SaaS platforms increasingly connect users, devices, and cloud services through shared digital infrastructure (Lu and Xu,2019). The B2C and B2B channels are not independent profit silos because platform economics often produces cross-side effects (Rysman,2009).

Business analytics literature emphasizes that data-driven forecasting can reduce uncertainty but cannot eliminate it. Forecasting methods provide probability distributions, prediction intervals, and early-warning signals rather than perfect demand. Capacity-risk logic is useful because it frames a practical decision: capacity ordered before demand realization may be too high or too low. For SaaS firms, the “capacity” is not inventory but cloud commitments, support staffing, API quotas, reserved model inference capacity, and onboarding resources. An overly conservative capacity plan may lead to

latency, failed enterprise onboarding, and poor user experience. An overly aggressive plan may create idle cloud spending and unused service capacity. The managerial issue is to price and provision under uncertainty, not merely to forecast demand. The SaaS focus is supported by empirical research showing that software-as-a-service creates both opportunities and risks for IT executives (Benlian and Hess,2011). Digital-finance platform research also shows how decentralized architectures can shift risk allocation among ecosystem participants (Xu et al.,2024).

2.3 Supply Risk in Cloud-Based SaaS Operations

Cloud computing has changed the economics of digital services by allowing firms to rent infrastructure rather than own physical computing assets. This flexibility is valuable, but it does not remove supply risk. Cloud service prices may vary by region, reserved capacity may be misestimated, outages can affect service availability, and congestion may degrade performance. For AI-enabled SaaS firms, the supply problem can be even more complex because inference and data-processing workloads are uneven and may require scarce accelerator capacity. A SaaS provider that signs enterprise service-level agreements without modeling infrastructure risk may face credits, penalties, emergency capacity purchases, or reputational damage. The distinction between B2C and B2B price responses is consistent with empirical evidence that pricing strategy depends on market conditions (Shankar and Bolton,2004). Supply-chain risk models increasingly combine analytics and artificial intelligence to support risk anticipation (Baryannis et al.,2019).

Supply chain risk management research has developed frameworks for disruption identification, mitigation, and resilience. Although much of this research focuses on physical supply chains, its logic applies to cloud-based SaaS operations. Cloud partner is a critical supplier. The SaaS provider depends on the partner for capacity, security primitives, monitoring tools, and recovery capabilities. Information asymmetry is a natural feature of this relationship because the cloud provider knows more about infrastructure constraints, while the SaaS firm knows more about product demand. Contract design, data sharing, and capacity reservation become central tools for reducing inefficiency. Advanced machine-learning research indicates that analytics capability itself is becoming a strategic resource in digital systems (Lu et al.,2024a). Enterprise cybersecurity certification can be interpreted as a signal that reduces uncertainty for business buyers (Spence,1973).

2.4 Cybersecurity Risk and Digital Trust

Cybersecurity risk is a core business risk for SaaS firms. A breach may cause direct response costs, service interruption, compensation obligations, legal exposure, and a durable loss of trust. The economic literature on security investment shows that optimal investment is not equal to maximum possible investment. Managers should compare marginal risk reduction with marginal cost. However, SaaS firms often face cross-channel externalities: the same authentication system, data encryption design, monitoring stack, and incident response capability protect both B2C and B2B customers. Therefore, the return from cybersecurity investment should be evaluated at the platform level rather than channel by channel. The scenario dashboard follows the idea that predictive analytics can improve supply-chain and organizational performance (Gunasekaran et al.,2017). Blockchain-enabled auditing research is relevant because SaaS pricing governance depends on reliable internal control evidence (Wu et al.,2025).

Cybersecurity also interacts with pricing. Enterprise customers may accept a higher price if the provider can document strong security controls, audit trails, compliance readiness, and reliable incident response. Individual customers may not read security documentation, but they react strongly to reputation and trust signals. A security incident may reduce conversion even when the product features remain unchanged. Thus, cybersecurity investment is not simply an IT cost. It is part of the value proposition, especially in B2B SaaS markets where vendor risk assessments are embedded in procurement. Security issues in cloud service delivery help explain why SaaS pricing must account for cyber exposure (Subashini and Kavitha,2011). Channel interpretation uses customer lifetime value logic to explain why enterprise accounts carry

greater economic weight (Gupta et al.,2006).

Table 1. Research positioning of the present study

Stream	Typical focus	Limitation addressed here	SaaS analytics contribution
Dual-channel pricing	Channel competition and price coordination	Often treats infrastructure and cyber risk as external	Links pricing with cloud capacity and risk metrics
Supply chain risk	Disruption, resilience, and capacity mismatch	Often developed for physical products	Reinterprets risk for SaaS cloud operations
Information asymmetry	Private cost or demand information	Often separated from analytics dashboards	Embeds information gaps into pricing governance
Cybersecurity economics	Security investment and breach loss	Often not connected to subscription pricing	Treats cyber investment as a pricing and trust variable
Business analytics	Forecasting, dashboards, and decision support	May remain descriptive rather than prescriptive	Provides scenario-based pricing recommendations

Table 1 summarizes the position of this article. The framework does not attempt to replace formal optimization theory; rather, it translates formal risk logic into a business analytics workflow suitable for SaaS managers. The contribution is especially relevant for firms whose pricing teams, cloud engineering teams, and cybersecurity teams rely on different dashboards and therefore make decisions that are locally rational but not systemically coordinated. Research on quantum financing systems illustrates how advanced computational paradigms may reshape financial risk analytics (Lu and Yang,2024). The modeling of strategic information is grounded in mechanism-design thinking about private information and incentives (Myerson,1981).

3. Research Design and Business Analytics Framework

3.1 Decision Context

The decision setting is a mid-sized SaaS provider that sells workflow automation software through two channels. The B2C channel offers monthly and annual self-service subscriptions to individual professionals and small teams. The B2B channel sells enterprise packages with negotiated volume discounts, administrative controls, compliance documentation, premium support, and uptime commitments. The SaaS provider does not own the full technology stack. It purchases cloud capacity, storage, content delivery, identity management, and monitoring services from an external infrastructure partner. The provider therefore must decide subscription prices, capacity commitments, and cybersecurity investment before final demand and incident outcomes are known. Cloud security research reinforces the need to treat cyber controls as part of service design rather than an afterthought (Zissis and Lekkas,2012). The managerial playbook assumes that analytics capability has value when it is embedded in dynamic organizational routines (Wamba et al.,2017).

The core managerial decision is not a single price. It is a portfolio of interdependent decisions. The B2C price affects acquisition speed and churn. The B2B price affects enterprise willingness to sign annual contracts and the level of service obligations attached to each account. The capacity commitment affects system performance, latency, and unused cloud cost. Cybersecurity investment affects expected breach loss, customer trust, and procurement credibility. A business analytics framework should therefore connect pricing, capacity, and security in one analysis environment. The use of AI-enabled anomaly detection is consistent with broader research on artificial intelligence applications and future prospects (Zhang and Lu,2021). The cross-channel argument is also supported by two-sided market theory, where user groups interact through platform rules (Rochet and Tirole,2003).

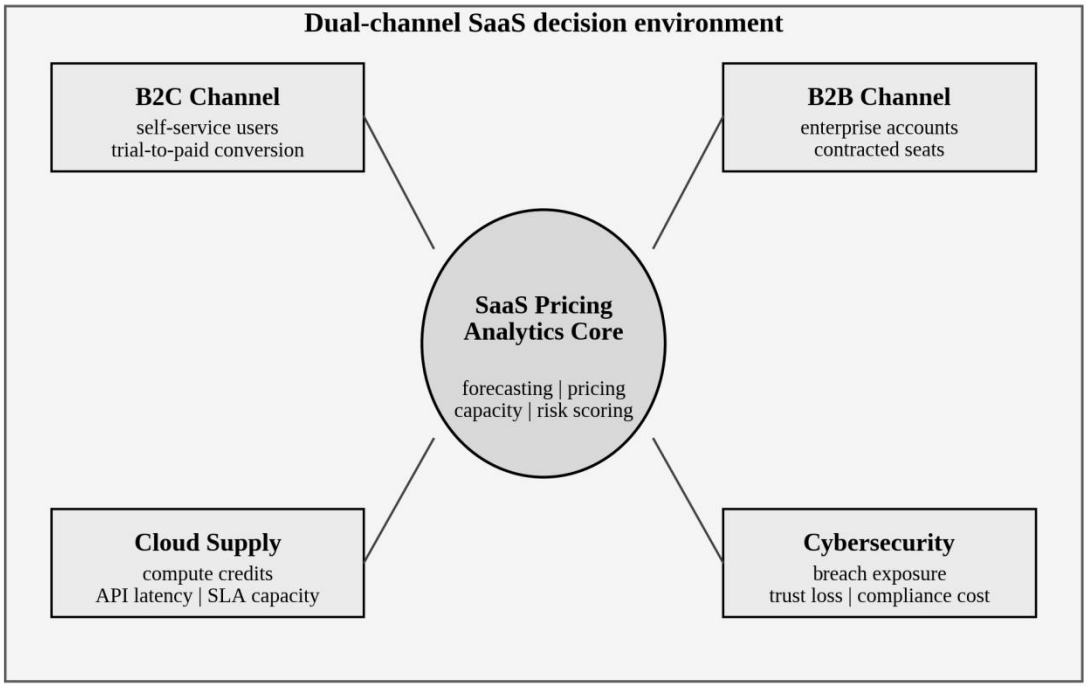

Figure 1. Business analytics framework for dual-channel SaaS pricing under demand, supply, and cybersecurity risk.

Figure 1 presents the conceptual structure used in the study. The figure intentionally avoids a linear arrow-based workflow because SaaS pricing is not a one-directional process. Demand analytics, cloud supply analytics, and cybersecurity analytics interact around a common decision core. The design emphasizes that pricing action cannot be evaluated only by conversion effects; it must also be evaluated by its capacity and trust implications. The customer-facing interpretation follows CRM research that links marketing interventions to customer value over time (Rust and Verhoef,2005). Blockchain and IoT security supports the importance of verifiable infrastructure controls in connected service environments (Xu et al.,2021).

3.2 Data Architecture and Variables

The proposed framework assumes that the SaaS provider maintains a unified analytics layer that integrates billing data, product usage data, cloud utilization data, support data, sales pipeline data, security alerts, and contract metadata. The analytics layer does not need to be perfect. Its purpose is to create a shared measurement language so that teams can evaluate the same decision using comparable metrics. For example, a proposed B2C discount should be described not only by expected conversion uplift but also by expected compute load, incremental support tickets, churn risk, and security monitoring demand. Low-friction digital channels can reduce buyer search costs and thereby intensify price comparison in the B2C segment (Bakos,1997). The expected-loss treatment of cyber events is supported by empirical work on the costs and causes of cyber incidents (Romanosky,2016).

The key variables are grouped into four categories. Demand variables include active users, trial conversion, paid conversion, seat expansion, churn, price elasticity, usage intensity, and seasonality. Supply variables include reserved computers, storage, API throughput, incident frequency, latency, service credits, and emergency capacity cost. Cybersecurity variables include identity risk, vulnerability severity, incident probability, expected breach cost, compliance status, and trust signals from enterprise due diligence.

Financial variables include average revenue per account, gross margin, customer acquisition cost, service-level penalties, and security investment. The paper frames the method as management analytics because the problem combines technology, decision support, and managerial action (Lu,2021). Digital pricing also has roots in market mechanisms for information goods and online platforms (Varian,2007).

Table 2. Data fields used in the SaaS pricing analytics framework

Category	Representative data fields	Analytical use
Demand data	trial starts, conversion rate, churn, usage depth, seat expansion	forecast channel demand and price response
Supply data	reserved capacity, latency, API usage, outage history, emergency cost	estimate cloud supply risk and capacity buffer needs
Cybersecurity data	account takeover signals, vulnerability scores, breach likelihood, compliance gaps	quantify expected cyber loss and investment priority
Financial data	subscription revenue, support cost, cloud cost, acquisition cost, SLA credits	evaluate operating profit and scenario trade-offs
Contract data	enterprise term length, renewal clauses, security obligations, service-level terms	translate B2B risk into pricing and governance rules

Table 2 shows that the analytics design is not merely a forecasting exercise. It requires the integration of behavioral, operational, security, and financial data. Integration is particularly important for B2B pricing because enterprise buyers often request stronger security and service guarantees. These guarantees increase willingness to pay, but they also create risk exposure if capacity or cybersecurity controls are underfunded. The mitigation scenario assumes anomaly detection because data mining and machine learning are widely used in intrusion detection (Buczak and Guven,2016).

3.3 Modeling Principles

The article uses six modeling principles. First, demand in the B2C and B2B channels is modeled separately because the two groups differ in price sensitivity, contract behavior, service expectations, and risk tolerance. Second, the demand forecast is treated as uncertain, so the analysis considers overcapacity and undercapacity rather than assuming a precise demand point. Third, cloud supply is modeled as a risk-bearing input, not a frictionless resource. Fourth, cybersecurity risk is treated as a business loss function that affects pricing and trust. Fifth, information asymmetry is modeled as an efficiency penalty created by imperfect visibility between the SaaS provider and its cloud partner. Sixth, the framework prioritizes scenario comparison over complex formula derivation so that decision makers can understand the relative effect of each risk source. The article treats online pricing as transparent because Internet markets often reduce friction in price discovery (Brynjolfsson and Smith,2000).

These principles make the framework compatible with business analytics practice. A SaaS firm can estimate parameters using historical data, expert judgment, vendor reports, and sensitivity analysis. The point is not to claim that one set of numbers is universal. Instead, the framework offers a repeatable decision protocol: define channels, estimate risk parameters, simulate scenarios, compare profit and service outcomes, and adjust pricing and investment policies. Future connectivity research suggests that digital service risk will become more closely tied to network performance and data flow (Lu and Ning,2020).

4. Scenario Design

4.1 Baseline Pricing Scenario

Scenario 1 is the transparent baseline. It assumes that the SaaS provider and the cloud infrastructure partner share sufficient information about demand forecasts, capacity availability, and unit cost. No major demand shock, supply disruption, or cybersecurity events occur. This scenario is not intended to represent normal reality. It functions as a benchmark for measuring the financial impact of uncertainty and information distortion. In this baseline, the B2C plan is priced to balance acquisition and margin, while the B2B plan is priced higher because enterprise clients require administrative controls, support, security documentation, and service-level assurances. The differentiated channel response in the numerical design is consistent with

revenue management under discrete customer choice (Talluri and Van Ryzin,2004).

The baseline scenario reflects the decision that a management team might make if it used clean historical averages and trusted vendor information. It is useful, but potentially misleading. Many SaaS firms make strategic plans based on baseline demand and baseline cloud cost, then experience profit erosion when uncertainty appears. The value of the remaining scenarios is that each one introduces a risk source and measures how it changes pricing and capacity decisions. The trust dimension of the model is consistent with research linking security, privacy, and trust in connected environments (Sicari et al.,2015).

4.2 Information Asymmetry Scenario

Scenario 2 introduces an infrastructure information gap. The cloud partner has more precise knowledge of reserve capacity constraints, congestion probabilities, support burden, and expected unit cost. The SaaS provider observes the quoted capacity price but cannot fully verify whether the markup is cost-based or information-rent-based. In the experiment, this condition increases the effective capacity cost and reduces expected profit. The provider responds by raising prices slightly and reducing capacity commitments, which protects margin but may reduce growth and service availability. The emphasis on shared records and visibility is consistent with empirical evidence on blockchain adoption in supply chains (Queiroz and Wamba,2019).

This scenario captures a common digital supply chain problem. Cloud infrastructure often appears transparent because invoices contain detailed line items. Yet the strategic meaning of these line items is not always transparent. The SaaS firm may not know how much flexibility the provider has, how congested a region is, or how future workload patterns will influence cost. Information asymmetry is therefore not only a legal contracting issue; it is also a data governance issue. The infrastructure-risk scenario is increasingly important as advanced communication systems expand the scope of digital service delivery (Lu and Zheng,2020).

4.3 Demand Risk Scenario

Scenario 3 adds stochastic demand. B2C demand may fluctuate because of promotions, competitor actions, social media visibility, or seasonal usage. B2B demand may change because of procurement delays, account expansion, or macroeconomic budget pressures. Demand risk affects pricing because the provider must choose capacity before the final level of demand is known. If capacity is too low, the firm suffers latency, onboard delays, lost conversion, and dissatisfaction. If capacity is too high, it pays for unused cloud commitments and support capacity. Digital demand acquisition can create auction-like cost dynamics that affect SaaS customer acquisition economics (Edelman et al.,2007).

Demand risk has different meanings across channels. In B2C, it is primarily a volume and churn problem. In B2B, it is a contract reliability problem. A large enterprise may sign up late, expand unexpectedly, or require urgent migration support. Missing that demand can be more costly than missing the same number of individual users because enterprise clients evaluate reliability as part of vendor quality. Therefore, the model assigns a higher undercapacity cost to the B2B channel. Supply-risk mitigation is interpreted as resilience building rather than only as cost minimization (Ponomarov and Holcomb,2009).

4.4 Supply and Cybersecurity Risk Scenarios

Scenario 4 introduces cloud supply risk. Even if SaaS demand is forecast correctly, the provider may face outages, regional latency, unplanned capacity rationing, API performance constraints, or increased emergency procurement costs. Supply risk is particularly damaging for B2B contracts because enterprise agreements often contain service-level credits and renewal consequences. A B2C user may tolerate a short performance issue if the product is inexpensive and substitutable. A B2B account may treat the same issue as a breach of vendor reliability. The model includes cyber exposure because connected digital services expand attack surfaces across devices and data flows (Alaba et al.,2017).

Scenario 5 introduces cybersecurity risk before mitigation. This risk is modeled as an expected loss

associated with breach probability, exposure volume, compliance consequences, and trust deterioration. It reduces profits both directly and indirectly. Direct costs include incident response, legal review, customer communication, and remediation. Indirect costs include lower conversion, delayed enterprise procurement, higher churn, and weakened willingness to pay. In SaaS, cybersecurity risk is inseparable from pricing because the provider sells not only features but also continuity, privacy, and trust. The analytics-enabled mitigation scenario follows the broader development of artificial intelligence applications in management analytics (Lu,2019a).

Scenario 6 adds analytics-enabled mitigation. The provider invests in cybersecurity analytics, automated anomaly detection, identity risk scoring, cloud observability, contract-level risk segmentation, and dynamic pricing review. This investment does not eliminate risk, but it reduces expected loss and allows the firm to align pricing with the risk profile of each channel. The final scenario measures how much profit can be recovered when the firm uses integrated analytics rather than isolated departmental decisions. The analysis recognizes that dynamic pricing is inseparable from learning about demand over time (den Boer,2015).

5. Numerical Experiment and Results

5.1 Parameter Configuration

The numerical experiment represents a mid-sized SaaS firm operating in Southeast Asia with international enterprise clients. The values are stylized and are intended to support managerial interpretation rather than reproduce the financial statements of a specific company. The B2C plan has a lower price and larger potential user pool. The B2B plan has a higher price, lower elasticity, stronger support requirements, and higher cyber exposure. The cloud supply cost is treated as a quarterly capacity commitment rather than a simple per-user expense because many SaaS providers reserve infrastructure or purchase committed spend discounts. The supply-risk discussion also draws on the distinction between resilience and robustness in supply-chain capabilities (Brandon-Jones et al.,2014).

The input parameters are reported in Table 3. The B2C channel has higher price sensitivity, while the B2B channel has higher undercapacity cost and cyber exposure. This configuration reflects the intuition that enterprise accounts are more profitable but less tolerant of service and security failure. The cybersecurity investment budget is initially set to zero in Scenario 5 and optimized in Scenario 6. The paper treats cyber analytics cautiously because intrusion-detection models must operate outside closed laboratory assumptions (Sommer and Paxson,2010).

Table 3. Numerical experiment input parameters

Parameter	B2C channel	B2B channel	Interpretation
Baseline price	USD 29 per month	USD 138 per seat per month	Initial pricing point before risk adjustment
Quarterly addressable demand	54,000 users	3,600 seats	Potential demand under moderate marketing spends
Price sensitivity	High	Medium-low	B2C users react more strongly to price changes
Demand volatility	18%	12%	B2C demand is noisier; B2B demand is contract-based
Undercapacity penalty	USD 11 per affected user	USD 47 per affected seat	Enterprise service failure is more costly
Cloud supply risk multiplier	1.10	1.35	B2B requires stronger service-level reliability
Cyber exposure coefficient	0.65	1.00	B2B has higher data and compliance exposure
Mitigation investment range	0-0.55 million	0-0.55 million	Platform-wide quarterly analytics and security budget

Table 3 also clarifies why a single pricing rule is not appropriate. The B2C and B2B channels differ not only in demand size but also in the type of risk attached to that demand. B2C pricing must protect growth

 https://doi.org/10.63646/jbda.2023.010304

and churn. B2B pricing must protect margin, trust, and contractual reliability. A business analytics model should therefore generate different price and capacity recommendations for each channel even if both channels use the same SaaS product core. Research on blockchain challenges helps justify the emphasis on verifiability in digital service ecosystems (Lu,2019b).

5.2 Scenario-Level Profit Comparison

The scenario results show a clear pattern. The transparent baseline produces the highest expected quarterly operating profit, USD 2.86 million. Introducing an infrastructure information gap reduces profit to USD 2.68 million. Adding demand volatility lowers profit further to USD 2.55 million. Cloud supply risk reduces the value to USD 2.43 million, and unmitigated cybersecurity exposure reduces it to USD 2.31 million. The analytics-enabled mitigation scenario increases profit to USD 2.59 million. This final value does not fully recover the baseline because residual uncertainty and information gaps remain, but it recovers a substantial portion of the loss. The higher B2B profit contribution is consistent with customer-lifetime-value logic for resource allocation (Venkatesan and Kumar,2004).

The profit path demonstrates why SaaS pricing should not be evaluated only by revenue growth. A price promotion may increase gross bookings while lowering net profit if it expands demand into a period of cloud congestion or weakens the capacity buffer needed for enterprise accounts. Similarly, a cybersecurity upgrade may appear costly when evaluated by the security budget alone, but it may improve pricing power and enterprise conversion when evaluated as part of the full business analytics framework. The discussion of supply-chain visibility is consistent with research on blockchain support for supply-chain management objectives (Kshetri,2018).

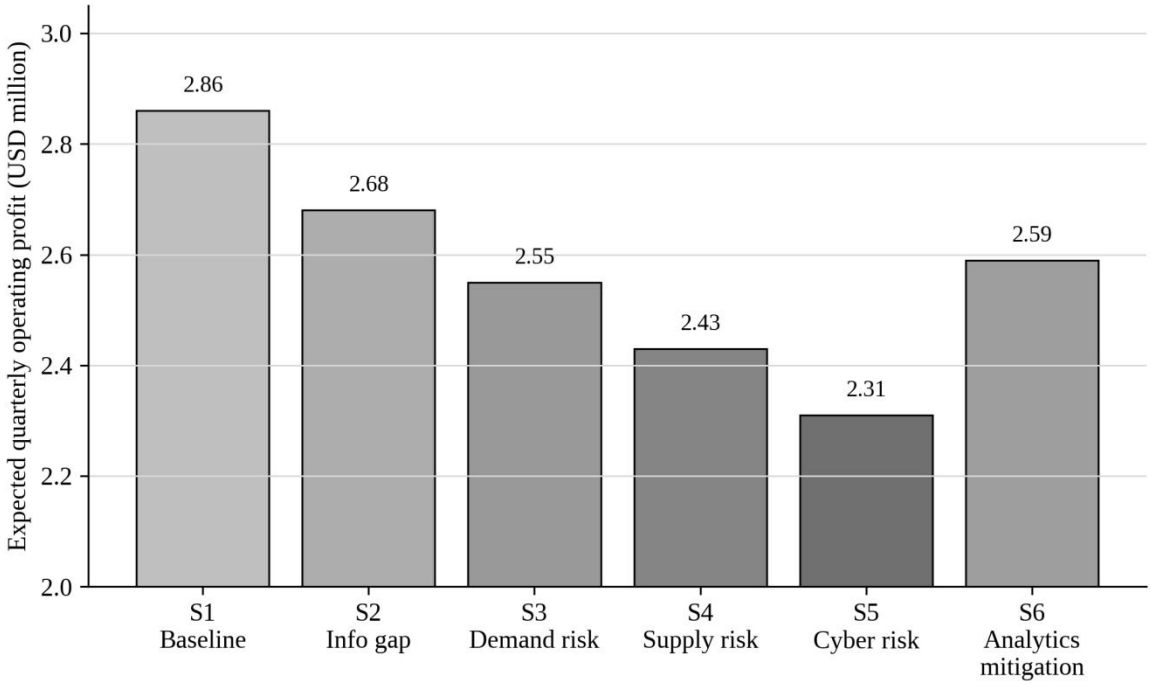

Figure 2. Expected quarterly operating profit across six SaaS pricing scenarios.

Figure 2 shows that the largest single reduction occurs when the information gap is introduced. The result indicates that the economics of SaaS pricing depends strongly on the quality of information exchange between the SaaS provider and the infrastructure partner. Demand and supply risks then compound the loss. Cybersecurity risk creates a visible additional loss, but it is also the most responsive to structured mitigation because investment in identity monitoring, anomaly detection, backup architecture, and response playbooks reduces expected loss across both channels. The anomaly-monitoring investment is compatible with the

growing use of deep learning in cybersecurity defense (Mahdavifar and Ghorbani,2019).

Table 4. Scenario results for dual-channel SaaS pricing

Scenario	B2C price	B2B price	Capacity stance	Expected profit	Key interpretation
S1 Transparent benchmark	USD 29.2	USD 136.0	Balanced reserve	USD 2.86M	Ideal benchmark with shared information and stable risk
S2 Information gap	USD 30.4	USD 139.5	Reduced reserve	USD 2.68M	Higher cloud cost premium weakens joint efficiency
S3 Demand risk	USD 31.0	USD 141.0	Demand buffer added	USD 2.55M	Volatility requires more cautious provisioning
S4 Supply risk	USD 31.3	USD 143.4	Higher B2B buffer	USD 2.43M	Service-level exposure shifts capacity toward B2B
S5 Cyber risk	USD 31.8	USD 146.7	Trust loss visible	USD 2.31M	Security exposure reduces conversion and margin
S6 Analytics mitigation	USD 31.5	USD 144.2	Risk-adjusted reserve	USD 2.59M	Integrated analytics recovers part of lost profit

Table 4 provides more detail than the profit chart. The B2B price increases more strongly than the B2C price as risk is added because enterprise accounts absorb more of the supply and cybersecurity burden. However, the mitigation scenario reduces the required risk premium slightly. This is important managerially: investment in better risk analytics can lower the price increase required to protect margin, which may improve competitiveness in enterprise procurement. The digital-service chain is part of a wider Industry 4.0 movement toward integrated cyber-physical and information systems.

5.3 Channel-Level Interpretation

The B2B channel contributes a larger share of operating profit even though the number of accounts is smaller. This outcome reflects higher average revenue, lower price elasticity, and stronger retention when service quality is acceptable. Nevertheless, B2B profitability is fragile. Supply and cybersecurity failures have a larger financial impact because enterprise contracts include service-level obligations and trust-sensitive procurement. In the experiment, the B2B channel accounts for about 57% of the baseline profit but nearly 64% of the loss caused by supply and cyber risks. The B2C interpretation avoids equating retention with profitability because long customer tenure is not always economically attractive (Reinartz and Kumar,2000).

The B2C channel behaves differently. It is less exposed to contract penalties but more exposed to demand volatility. When the B2C price rises too much, conversion falls and churn increases. Therefore, the optimal B2C response is not simply to pass risk costs through to users. A better approach is to use plan design, usage thresholds, and annual billing incentives to smooth demand and reduce high-cost usage spikes. For example, the firm may include a fair-use threshold in the individual plan while offering paid add-ons for heavy usage. Such design choices are pricing decisions, not purely product decisions. The integrated treatment of cloud supply and cybersecurity risk is consistent with cyber supply-chain risk management research (Boyson,2014).

The interaction between channels is also important. B2C provides early signals about feature adoption and performance pressure, which can support B2B sales forecasting. B2B contracts provide stable cash flow that can fund infrastructure and cybersecurity investment benefiting all users. A business analytics framework should identify these spillovers. If teams optimize channels independently, the firm may underinvest in shared security and overreact to short-term B2C conversion metrics. AI-driven cybersecurity research supports the idea that mitigation investment should include security intelligence models (Sarker et al.,2021).

6. Sensitivity Analysis

6.1 Cybersecurity Investment and Profit Recovery

 https://doi.org/10.63646/jbda.2023.010304

The sensitivity analysis evaluates how net expected profit changes as quarterly cybersecurity analytics investment increases from zero to USD 0.55 million. The investment includes improved identity analytics, security event correlation, enterprise audit automation, automated vulnerability prioritization, backup validation, and risk-based account monitoring. The curve is expected to be concave: initial investment removes high-probability weaknesses and yields strong returns, while later investment addresses increasingly rare events and provides smaller marginal benefits. Cyber-physical system research reinforces the need to analyze technology, operations, and business value together (Lu,2017b).

The result shows an optimal investment zone around USD 0.24 million per quarter. Below this level, the firm remains exposed to preventable security loss and weakened enterprise trust. Above this level, the marginal benefit of additional investment falls below the cost. This does not mean that all firms should invest the same amount. It means that SaaS managers should estimate the point at which the marginal reduction in expected breach and trust loss equals the marginal cost of security analytics. The business analytics contribution is to make this comparison explicit and revisable as data change. The subscription perspective follows service research in which usage and satisfaction interact over time (Bolton and Lemon,1999).

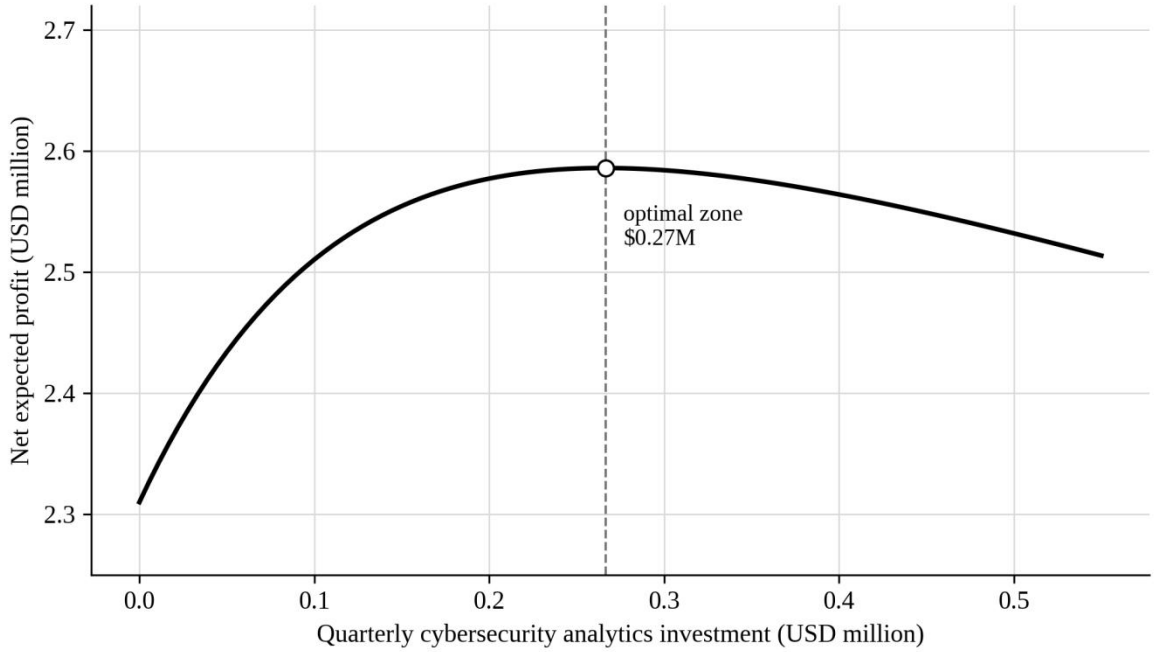

Figure 3. Net expected profit under alternative cybersecurity analytics investment levels.

Figure 3 supports practical interpretation. Cybersecurity investment has a positive return over a wide range, but not indefinitely. The firm should avoid two common errors: treating cybersecurity as a fixed compliance cost that is minimized or treating it as an unlimited safety budget with no economic threshold. The analytics view treats cybersecurity as a variable decision with measurable impact on pricing power, churn, enterprise conversion, and expected loss. The discussion of analytics-based pricing recognizes that transaction history can affect future price design.

6.2 Demand Volatility and Cyber Exposure

A second sensitivity analysis examines how recommended B2B price adjustment changes when demand volatility and cyber exposure rise together. The result is presented as a grayscale heatmap. The purpose is not to produce a universal pricing formula but to show how managers can translate risk states into pricing guidance. When both demand volatility and cyber exposure are low, the required risk premium is modest. When both are high, the recommended price adjustment increases because the provider must protect capacity, service-level obligations, and trust-related loss. The cloud-cost discussion also reflects the broader shift

toward externally provided computing resources (Sultan,2010).

The heatmap also reveals a useful governance lesson. A price increase should not be triggered automatically by one risk indicator. If demand volatility is high but cyber exposure is low, plan design and capacity flexibility may be better responses than a major price increase. If cyber exposure is high but demand volatility is low, targeted enterprise security packages and audit fees may be more appropriate than raising all channel prices. Business analytics should therefore support differentiated action rather than a single risk surcharge applied to all customers. The study contributes to management analytics by showing how data-driven modeling can inform cross-functional business decisions (Lu et al.,2024b).

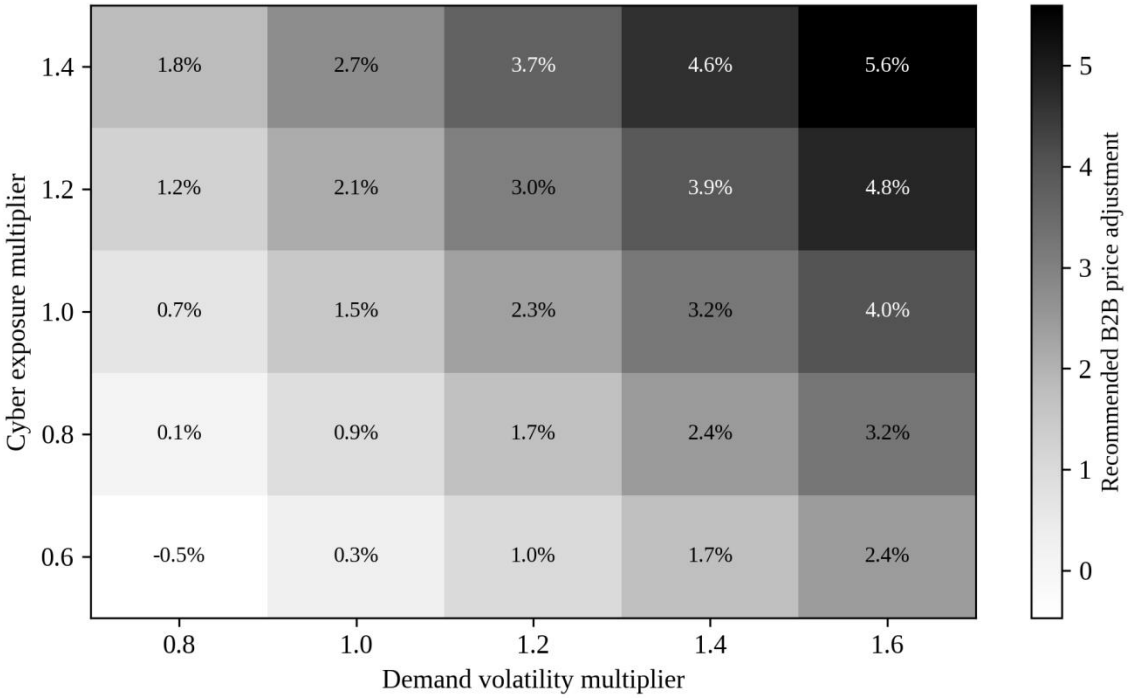

Figure 4. Recommended B2B price adjustment under combined demand volatility and cyber exposure.

Figure 4 indicates that the highest recommended B2B price adjustments occur when demand volatility and cyber exposure are both above baseline. This pattern suggests that SaaS firms should combine pricing review with risk classification. Enterprise accounts with heavy integration requirements, sensitive data, and strict uptime needs should be priced with explicit recognition of security and service obligations, while lower-risk accounts can be protected through standardized controls and moderate pricing. The role of trust in SaaS purchasing is consistent with online-shopping research that combines trust and technology acceptance.

7. Discussion and Managerial Implications

7.1 Pricing Governance for SaaS Managers

The findings indicate that SaaS pricing governance should include finance, product analytics, cloud operations, cybersecurity, and enterprise sales. A pricing committee that focuses only on market willingness to pay may understate operating and trust costs. A cloud engineering team that focuses only on cost efficiency may understate conversion and customer experience effects. A security team that focuses only on compliance may understate revenue implications. Integrated governance allows the firm to evaluate a pricing change as a business decision rather than a departmental adjustment. The separation of onboarding, renewal, and usage signals follows customer-journey thinking in service markets (Lemon and Verhoef,2016).

The results also support the use of scenario dashboards. A useful dashboard should show the expected

profit under baseline, demand shock, cloud capacity stress, and cybersecurity incident assumptions. It should also display channel-level effects. If a B2C discount increases total subscriptions but consumes capacity needed for enterprise onboarding, the dashboard should make that trade-off visible. If an enterprise security investment reduces procurement delays and increases renewal probability, the dashboard should show the associated pricing power rather than treating the investment as a pure cost. The governance argument follows digital business strategy research that treats digital resources as central to competitive decision-making (Bharadwaj et al.,2013).

Table 5. Managerial playbook for dual-channel SaaS risk pricing

Risk condition	Analytics signal	Recommended action	Pricing implication
High B2C demand volatility	large forecast interval; fast churn movement	use annual incentives, fair-use thresholds, and campaign throttling	avoid excessive public discounts during capacity stress
High B2B service exposure	large enterprise pipeline; strict SLA terms	reserve capacity and negotiate service-level clauses	use account-specific risk premium or support tier
Cloud cost opacity	unexpected invoice changes; weak cost explainability	create shared capacity reports and vendor review cadence	reduce information-rent premium through transparency
Elevated cyber risk	identity anomalies; unresolved vulnerabilities; audit gaps	prioritize cross-channel security analytics investment	protect enterprise price premium through trust evidence
Cross-channel spillover	B2C usage spike affects B2B latency	coordinate release, promotion, and capacity planning	separate growth price from reliability price

Table 5 translates the analytical results into actions. The central message is that risk-adjusted pricing should not be a mechanical surcharge. It should be tied to observable analytics signals and specific operational responses. Managers should be able to explain why a price changes, which risk it addresses, and how the associated investment improves service quality or customer trust. The scenario-based format is aligned with management-analytics research that emphasizes better decision-making in modern business practice.

7.2 Implications for B2B and B2C Strategy

The B2C channel should be managed as an experimentation and demand-generation channel. It provides high-frequency data on product usage and willingness to pay. It also creates a large base of users who may later influence enterprise adoption. However, B2C demand should not be allowed to destabilize the platform. Usage thresholds, modular add-ons, and annual billing incentives can reduce volatility. The B2C price should remain simple and transparent because users in this segment are more sensitive to perceived complexity. The article treats SaaS pricing as a digital innovation problem because product, data, and infrastructure are jointly organized (Yoo et al.,2010).

The B2B channel should be managed as a trust and reliability channel. The enterprise price should reflect support, compliance, security assurance, data governance, and service-level obligations. A lower B2B price may increase short-term sales but can be harmful if it does not cover the risk-bearing cost of enterprise commitments. The experiment shows that B2B contracts benefit more from cybersecurity investment because the investment protects trust and reduces procurement friction. Therefore, enterprise pricing should be paired with security documentation and measurable assurance rather than only feature bundles. The dashboard approach reflects the transition from business intelligence to business impact through analytics (Chen et al.,2012).

The two channels should not be separated completely. B2C growth creates brand visibility and product data. B2B revenue funds infrastructure resilience and security maturity. A platform-level analytics system should allocate shared costs and shared benefits across channels. For example, identity risk monitoring protects both individual and enterprise users. Cloud observability reduces latency for both segments. Therefore, channel profitability reports should include shared risk-adjusted infrastructure metrics instead of

attributing all platform investment to one segment. The data architecture relies on the idea that large data sets become valuable only when linked to suitable analytic methods (Gandomi and Haider,2015).

7.3 Limitations and Future Research

This study has several limitations. First, the numerical experiment is stylized. It is designed to illustrate managerial logic rather than estimate a particular market. Future research could calibrate the framework using real SaaS billing, usage, and incident data. Second, the model assumes that B2C and B2B demand are related through shared infrastructure but does not explicitly estimate correlated demand shocks. In practice, a successful product launch or macroeconomic event may affect both channels simultaneously. Third, cybersecurity risk is represented through expected loss, whereas real incidents may be rare but severe. Future studies could use extreme-value methods or scenario trees to capture tail risk. B2C data in the framework is useful because consumer analytics can transform marketing and pricing decisions (Erevelles et al.,2016).

Fourth, the analysis treats the cloud partner as a single infrastructure supplier. Many SaaS providers use multiple cloud regions, content delivery networks, managed security vendors, and AI model providers. Extending the framework to multi-vendor sourcing would improve realism. Fifth, the current study emphasizes pricing and capacity decisions, but SaaS firms also manage product packaging, feature gating, free trials, and customer success investment. Future research could integrate these levers with risk-adjusted pricing. Finally, the framework assumes that managers are willing to share data across departments. Organizational politics and data silos may prevent integration even when the analytical logic is clear. Implementation research is therefore needed. The variable design recognizes that Big Data is defined by scale, variety, and the decision context in which it is used (De Mauro et al.,2016).

8. Conclusion

This article developed a business analytics framework for dual-channel SaaS pricing under demand, supply, and cybersecurity risk. The study reinterpreted a service supply chain risk problem in the context of SaaS monetization, emphasizing subscription pricing, cloud capacity, information asymmetry, and digital trust. Instead of relying on extensive formal derivations, the article presented scenario-based analytics design that managers can use to evaluate pricing decisions across B2C and B2B channels.

The numerical experiment showed that unmanaged information and risk reduced expected quarterly operating profit from USD 2.86 million to USD 2.31 million. Analytics-enabled mitigation increases expected profit to USD 2.59 million, recovering USD 0.28 million of the loss. The results also showed that B2B pricing requires stronger attention to supply and cybersecurity risk because enterprise customers impose higher service and trust obligations. B2C pricing requires stronger attention to demand volatility, churn, and capacity spillover. Cybersecurity investment has a positive but diminishing return, with an optimal investment zone that should be estimated from platform-specific data.

The practical message is straightforward: SaaS pricing should be governed as a cross-functional analytics problem. Pricing, capacity, and cybersecurity decisions should not be optimized separately. A SaaS firm that coordinates these decisions can protect margin, reduce risk exposure, and justify price differences between B2C and B2B offerings. The theoretical contribution is to connect dual-channel pricing, information asymmetry, cloud supply risk, and cybersecurity economics in a coherent business analytics framework. Future research can extend the model with real transaction data, multi-vendor cloud sourcing, dynamic learning, and tail-risk cybersecurity analysis.

Acknowledgement

The authors gratefully acknowledge the constructive comments of anonymous reviewers and the editorial team of the Journal of Business and Data Analytics. The authors also thank their respective institutions for providing research environments that supported this study. Any remaining errors are the responsibility of the authors.

Funding Statement

This research received no specific grant from any public, commercial, or not-for-profit funding agency.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Data Availability Statement

The numerical data used in this study are synthetic and are included in the tables and figures of the article for reproducibility and instructional use.

Reference

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58. DOI: 10.1145/1721654.1721672

Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84(3), 488-500. DOI: 10.2307/1879431

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. DOI: 10.1080/17517575.2025.2541199

Besbes, O., & Zeevi, A. (2009). Dynamic pricing without knowing the demand function: Risk bounds and near-optimal algorithms. Operations Research, 57(6), 1407-1420. DOI: 10.1287/opre.1080.0640

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868-1883. DOI: 10.1111/poms.12838

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. DOI: 10.1007/s10796-021-10221-w

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing: The business perspective. Decision Support Systems, 51(1), 176-189. DOI: 10.1016/j.dss.2010.12.006

Parker, G. G., & Van Alstyne, M. W. (2005). Two-sided network effects: A theory of information product design. Management Science, 51(10), 1494-1504. DOI: 10.1287/mnsc.1050.0400

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996-1015. DOI: 10.1002/sres.3151

Ferreira, K. J., Lee, B. H. A., & Simchi-Levi, D. (2016). Analytics for an online retailer: Demand forecasting and price optimization. Manufacturing & Service Operations Management, 18(1), 69-88. DOI: 10.1287/msom.2015.0561

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. DOI: 10.1145/581271.581274

Waller, M. A., & Fawcett, S. E. (2013). Data science, predictive analytics, and big data: A revolution that will transform supply chain design and management. Journal of Business Logistics, 34(2), 77-84. DOI: 10.1111/jbl.12010

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. DOI: 10.1186/s40854-024-00668-6

Gallego, G., & Van Ryzin, G. (1994). Optimal dynamic pricing of inventories with stochastic demand over finite horizons. Management Science, 40(8), 999-1020. DOI: 10.1287/mnsc.40.8.999

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-492. DOI: 10.1257/jel.54.2.442

Verhoef, P. C., Kannan, P. K., & Inman, J. J. (2015). From multi-channel retailing to omni-channel retailing: Introduction to the special issue on multi-channel retailing. Journal of Retailing, 91(2), 174-181. DOI: 10.1016/j.jretai.2015.02.005

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. DOI: 10.1007/s10796-022-10248-7

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. DOI: 10.1126/science.1130992

Bitran, G., & Caldentey, R. (2003). An overview of pricing models for revenue management. Manufacturing & Service Operations Management, 5(3), 203-229. DOI: 10.1287/msom.5.3.203.16031

Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. Journal of Business Research, 122, 502-517. DOI: 10.1016/j.jbusres.2020.09.009

Lu, Y., & Xu, L. D. (2019). Internet of Things cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. DOI: 10.1109/JIOT.2018.2869847

Rysman, M. (2009). The economics of two-sided markets. Journal of Economic Perspectives, 23(3), 125-143. DOI: 10.1257/jep.23.3.125

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52(1), 232-246. DOI: 10.1016/j.dss.2011.07.007

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. DOI: 10.1080/17517575.2024.2397630

Shankar, V., & Bolton, R. N. (2004). An empirical analysis of determinants of retailer pricing strategy. Marketing Science, 23(1), 28-49. DOI: 10.1287/mksc.1030.0034

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. International Journal of Production Research, 57(7), 2179-2202. DOI: 10.1080/00207543.2018.1530476

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024a). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. DOI: 10.1016/j.jii.2024.100736

Spence, M. (1973). Job market signaling. Quarterly Journal of Economics, 87(3), 355-374. DOI: 10.2307/1882010

Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2017). Big data and predictive analytics for supply chain and organizational performance. Journal of Business Research, 70, 308-317. DOI: 10.1016/j.jbusres.2016.08.004

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003. DOI: 10.1080/17517575.2024.2448003

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. DOI: 10.1016/j.jnca.2010.07.006

Gupta, S., Hanssens, D., Hardie, B., Kahn, W., Kumar, V., Lin, N., Ravishanker, N., & Sriram, S. (2006). Modeling customer lifetime value. Journal of Service Research, 9(2), 139-155. DOI: 10.1177/1094670506293810

Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. DOI: 10.1016/j.jii.2024.100663

Myerson, R. B. (1981). Optimal auction design. Mathematics of Operations Research, 6(1), 58-73. DOI: 10.1287/moor.6.1.58

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592. DOI: 10.1016/j.future.2010.12.006

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. DOI: 10.1016/j.jbusres.2016.08.009

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. DOI: 10.1016/j.jii.2021.100224

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. Journal of the European Economic Association, 1(4), 990-1029. DOI: 10.1162/154247603322493212

Rust, R. T., & Verhoef, P. C. (2005). Optimizing the marketing interventions mix in intermediate-term CRM. Marketing Science, 24(3), 477-489. DOI: 10.1287/mksc.1040.0107

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. DOI: 10.1109/JIOT.2021.3060508

Bakos, Y. (1997). Reducing buyer search costs: Implications for electronic marketplaces. Management Science, 43(12), 1676-1692. DOI: 10.1287/mnsc.43.12.1676

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135. DOI: 10.1093/cybsec/tyw001

Lu, Y. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181-192. DOI: 10.15828/2075-8545-2021-13-3-181-192

Varian, H. R. (2007). Position auctions. International Journal of Industrial Organization, 25(6), 1163-1178. DOI: 10.1016/j.ijindorg.2006.10.002

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. DOI: 10.1109/COMST.2015.2494502

Brynjolfsson, E., & Smith, M. D. (2000). Frictionless commerce? A comparison of Internet and conventional retailers. Management Science, 46(4), 563-585. DOI: 10.1287/mnsc.46.4.563.12061

Lu, Y., & Ning, X. (2020). A vision of 6G-5G's successor. Journal of Management Analytics, 7(3), 301-320. DOI: 10.1080/23270012.2020.1802622

Talluri, K., & Van Ryzin, G. (2004). Revenue management under a general discrete choice model of consumer behavior. Management Science, 50(1), 15-33. DOI: 10.1287/mnsc.1030.0147

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164. DOI: 10.1016/j.comnet.2014.11.008

Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. International Journal of Information Management, 46, 70-82. DOI: 10.1016/j.ijinfomgt.2018.11.021

Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. DOI: 10.1016/j.jii.2020.100158

Edelman, B., Ostrovsky, M., & Schwarz, M. (2007). Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. American Economic Review, 97(1), 242-259. DOI: 10.1257/aer.97.1.242

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. International Journal of Logistics Management, 20(1), 124-143. DOI: 10.1108/09574090910954873

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28. DOI: 10.1016/j.jnca.2017.04.002

Lu, Y. (2019a). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. DOI: 10.1080/23270012.2019.1570365

den Boer, A. V. (2015). Dynamic pricing and learning: Historical origins, current research, and new directions. Surveys in Operations Research and Management Science, 20(1), 1-18. DOI: 10.1016/j.sorms.2015.03.001

Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. Journal of Supply Chain Management, 50(3), 55-73. DOI: 10.1111/jscm.12050

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305-316. DOI: 10.1109/SP.2010.25

Lu, Y. (2019b). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. DOI: 10.1016/j.jii.2019.04.002

Venkatesan, R., & Kumar, V. (2004). A customer lifetime value framework for customer selection and resource allocation strategy. Journal of Marketing, 68(4), 106-125. DOI: 10.1509/jmkg.68.4.106.42728

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. DOI: 10.1016/j.ijinfomgt.2017.12.005

Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. Neurocomputing, 347, 149-176. DOI: 10.1016/j.neucom.2019.02.056

Lu, Y. (2017a). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. DOI: 10.1016/j.jii.2017.04.005

Reinartz, W. J., & Kumar, V. (2000). On the profitability of long-life customers in a noncontractual setting.

Journal of Marketing, 64(4), 17-35. DOI: 10.1509/jmkg.64.4.17.18077

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353. DOI: 10.1016/j.technovation.2014.02.001

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2, 173. DOI: 10.1007/s42979-021-00557-0

Lu, Y. (2017b). Cyber physical system-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. DOI: 10.1142/S2424862217500142

Bolton, R. N., & Lemon, K. N. (1999). A dynamic model of customers' usage of services: Usage as an antecedent and consequence of satisfaction. Journal of Marketing Research, 36(2), 171-186. DOI: 10.1177/002224379903600203

Acquisti, A., & Varian, H. R. (2005). Conditioning prices on purchase history. Marketing Science, 24(3), 367-381. DOI: 10.1287/mksc.1040.0103

Sultan, N. (2010). Cloud computing for education: A new dawn? International Journal of Information Management, 30(2), 109-116. DOI: 10.1016/j.ijinfomgt.2009.09.004

Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024b). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. DOI: 10.15828/2075-8545-2024-16-3-257-266

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51-90. DOI: 10.2307/30036519

Lemon, K. N., & Verhoef, P. C. (2016). Understanding customer experience throughout the customer journey. Journal of Marketing, 80(6), 69-96. DOI: 10.1509/jm.15.0420

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471-482. DOI: 10.25300/MISQ/2013/37:2.3

Lu, Y., Pisarenko, Z. V., Yang, L., & Ye, C. (2024c). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. DOI: 10.15828/2075-8545-2024-16-5-431-440

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. Information Systems Research, 21(4), 724-735. DOI: 10.1287/isre.1100.0322

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188. DOI: 10.2307/41703503

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137-144. DOI: 10.1016/j.ijinfomgt.2014.10.007

Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. Journal of Business Research, 69(2), 897-904. DOI: 10.1016/j.jbusres.2015.07.001

De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. Library Review, 65(3), 122-135. DOI: 10.1108/LR-06-2015-0061