Pricing Strategies in Cybersecurity Markets with Network Effects

1st Jing Hou
Department of Computer Science and Information Systems
California State University San Marcos
San Marcos, CA 92096, USA
jhou@csusm.edu

2nd Xuyu Wang
School of Computing and Information Sciences
Florida International University
Miami, FL 33199, USA
xuywang@fiu.edu

3rd Amy Z. Zeng
Sawyer Business School
Suffolk University
Boston, MA 02108, USA
azeng@suffolk.edu

2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC) | 979-8-3315-0805-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/CCNC54725.2025.10976045

***Abstract*—The cybersecurity market is rapidly growing in the face of ubiquitous vulnerabilities, with vendors delivering solutions ranging from basic software-based approaches to high-end services for diverse business needs. The sustainability of a cybersecurity business relies on its ability to update its solutions to address ever-changing cyber threats continuously. It requires a substantial customer base for data collection and service enhancement, which, in turn, can attract more customers. Therefore, a novel business model that acknowledges this positive network effect and provides incentives for potential customers is crucial to ensure the success of the cybersecurity business. In this paper, we develop an analytical framework with optimization and a Stackelberg game approach to model the cybersecurity market scenario for a cybersecurity vendor offering both a basic software-based service and a premium service. We delve into the market evolution and characterize the conditions under which the dynamic market converges to a unique equilibrium. The optimal pricing strategy for the vendor is analyzed to leverage the network effects for profit maximization.**

***Index Terms*—Cybersecurity market, network externality, pricing, inter-service relationship, incentive**

I. Introduction

The cybersecurity market is experiencing rapid growth with global revenues of $166.2 billion in 2023, projected to reach $273.5 billion by 2028 [1]. Cybersecurity vendors are springing up to satisfy the cybersecurity needs of different sizes of businesses. These vendors provide different layers of cybersecurity solutions that encompass both software-based approaches and the involvement of human expertise. For example, Xonicwave [2] and Cyvatar [3] provide solutions from antivirus and malware software to penetration tests and customized solutions.

A major challenge for these vendors is assessing the value of different services and setting prices. In determining the economic value of different cybersecurity services, inter-service network effects in information intelligence play a crucial role [4]. The quality and resilience of basic cybersecurity software solutions depend heavily on the vendor's knowledge and expertise, shaped by their exposure to extensive cyber threat intelligence. Expert-led vulnerability analysis and threat hunting, typically offered in premium cybersecurity services, enables vendors to significantly improve the quality of their software solution [5]. Such experience provides intelligent information on emerging threats and vulnerabilities, enabling vendors to upgrade their software continuously against evolving cybersecurity challenges. In other words, indirect network effects exist [6] between the premium and basic services.

In this paper, we study the business model of cybersecurity vendors who provide both basic software solutions and premium services that rely heavily on specialized human skills such as penetration testing and forensic analysis. With the growth of premium service subscribers who provide more data for vendors to explore, the quality of cybersecurity software may become more valuable, which could attract more customers. This inter-service dependency or indirect network effect, which significantly influences market dynamics, is often overlooked. Without a thorough understanding of its impact, it's impossible for service providers to develop efficient pricing strategies and deliver effective cybersecurity services. Therefore, we develop a framework that evaluates indirect network effects and informs cybersecurity vendors' pricing strategy to provide more efficient and cost-effective security solutions. The major contributions of the paper are: We are the first to introduce an analytical framework to explore the economic interactions between cybersecurity solution vendors and their subscribers with the inclusion of both premium services involving human intelligence and basic software solutions with endogenous quality level. We examine the indirect network effects between the premium service and the basic software solution. The optimal pricing strategy to maximize expected profits for cybersecurity vendors is also analyzed. The proposed analytical framework will be useful for cybersecurity vendors in deriving service demand and pricing strategies when both software-based solutions and premium services that involve human intelligence are offered. The paper is organized as follows: Section 2 reviews related

literature. Section 3 sets up the model and analyzes customer choices. Section 4 delineates the market dynamics and derives the equilibrium. The optimal pricing strategy for cybersecurity vendor is analyzed in Section 5. Finally, Section 6 concludes with comments and future research directions.

II. Related Work

The majority of studies in cybersecurity solutions have focused on addressing the technical (e.g., [7]) and policy challenges (e.g., [8]). An economic or operations management perspective in cybersecurity is gaining more and more attention in academic research. One stream of literature considers cybersecurity decisions in the context of interdependent risks [9], [10]. Another stream of literature discusses firms' investment decisions from an economic perspective, such as coordinated cybersecurity investments in supply chain context [11], and equilibrium investment in competitive environments [12]. These models are generally formulated from the standpoint of defenders, such as users of cybersecurity software. However, the widespread adoption and effectiveness of cybersecurity practices are largely dependent on the profitability of the solution providers, which is often overlooked. To fill the gap, our research examines the profits and pricing decisions of cybersecurity vendors, considering the subscription choices of users who place varying degrees of importance on security.

Recent years have seen significant attention to the markets for various IT services, particularly concerning pricing and discount strategies [13]–[15]. Some studies have explored positive network effects, including those between wireless device markets and mobile social services [15], as well as between application service users and service developers in two-sided markets [16]. However, the pricing strategies for different levels of services, considering their interdependent network effects, have not been addressed, which is a common issue in cybersecurity services. In our model, we examine the interrelationship between different cybersecurity service markets offered by the same vendor. Specifically, the value of a basic software solution is indirectly influenced by the premium service, which in turns affects market shares.

III. Customer Model

We consider one cybersecurity vendor who provides both basic software-based cybersecurity service and premium service that involves human intelligence. Each customer has three choices (denoted by s) in terms of service subscription: (i) $s = n$: Not subscribe to any service; (ii) $s = b$: Subscribe to basic service; and (iii) $s = p$: Subscribe to premium service. We denote v_p and v_b as the expected *utility* that a customer can obtain from subscribing to the premium and basic services respectively[1]. v_p and v_b can be seen as the equivalent financial benefit a customer receives by utilizing the services, which could involve reduced losses due to fewer cyber attack disruptions, higher income from improved trust of customers and partners, and reduced cyber risk insurance premiums. We assume that $v_b < v_p$ since the premium service adds a layer of human expertise to the basic software-based service[2].

Given the prices π_b for the basic service and π_p for the premium service, let θ denote the importance a customer places on cybersecurity. Then, the perceived expected payoff for a customer with parameter θ is

$$\Pi^{\mathrm{E}} = \begin{cases} 0 & \text{if } s = n, \\ \theta v_b - \pi_b & \text{if } s = b, \\ \theta v_p - \pi_p & \text{if } s = p. \end{cases} \tag{1}$$

Customers vary in their cybersecurity concerns, represented by the parameter θ. This value reflects a company's cybersecurity needs, influenced by its business model, size, and risk profile, and can differ even among companies within the same industry. For example, a company with an online business or complex IT infrastructure may prioritize cybersecurity more than a brick-and-mortar or small-scale business, resulting in a higher value of θ. For convenience, we assume that θ follows a uniform distribution in [0, 1] among potential customers, with $\theta = 0$ corresponding to no concern for cybersecurity and $\theta = 1$ indicating the highest priority. Each customer selects the service that maximizes their expected utility, defined in (1), so the optimal choice for a type-θ customer is

$$\begin{cases} s^*_\theta = n & \text{iff } 0 > \max\{\theta v_b - \pi_b, \theta v_p - \pi_p\}, \\ s^*_\theta = b & \text{iff } \theta v_b - \pi_b > \max\{\theta v_p - \pi_p, 0\}, \\ s^*_\theta = p & \text{iff } \theta v_p - \pi_p > \max\{\theta v_b - \pi_b, 0\}. \end{cases} \tag{2}$$

Fig. 1 illustrates the ranges of θ with difference optimal choices, where $\theta_{bp} = \frac{\pi_p - \pi_b}{v_p - v_b}$, $\theta_p = \frac{\pi_p}{v_p}$, and $\theta_b = \frac{\pi_b}{v_b}$. There are three possible relationships among θ_{bp}, θ_p, θ_b, and 1. For example, in Fig. 1(a), if $\theta_{bp} < \theta_p$, any customer with $\theta < \theta_p$ will not subscribe to any service, while all other customers will opt for the premium service. Let η_s $(s = n, b, p)$ represent the fraction of population opting for choice s. Therefore, $\eta_n + \eta_b + \eta_p = 1$. Here, η_b denotes the market share of the basic service, and η_p corresponds to the market share of the premium service. We can derive that, conditional on π_b, π_p, v_b, and v_p, the values of η_p and η_b can be computed below:

- Case (a): if $\theta_{bp} \le \theta_p$, then $\eta_b = 0$, $\eta_p = 1 - \theta_p$;
- Case (b): if $\theta_p < \theta_{bp} \le 1$, then $\eta_b = \theta_{bp} - \theta_b$, $\eta_p = 1 - \theta_{bp}$;
- Case (c): if $\theta_{bp} > 1$, then $\eta_b = 1 - \theta_b$, $\eta_p = 0$;

IV. Market Dynamics and Equilibrium Analysis

To capture the interactions between the cybersecurity vendor and its potential customers, we will model the game between them as a Stackelberg game. Adopting the backward induction, we first obtain the market equilibrium based on the customers' subscription decisions, and then obtain the optimal pricing decision for the vendor in Section V.

[1]Given that v_p and v_b represent the quality levels of the services provided, we will use *service quality*, *service value*, and *expected utility from the services* interchangeably in our models.

[2]Note that this differs from bundled services whose benefits are cumulative. In cybersecurity premium service, the software and the human intelligence in premium service might complement each other and address a broader range of security issues.

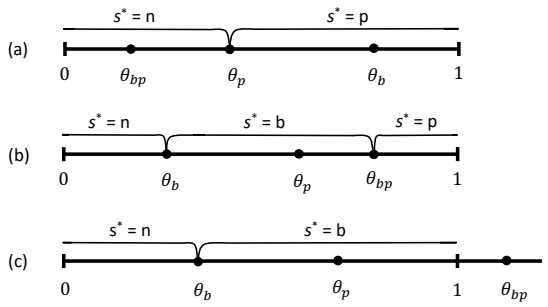

Fig. 1. Illustration of θ_{bp}, θ_b, and θ_p

The premium service value, v_p, is assumed to remain stable. The basic service utilizes software like Signature-based IDS for threats detection, which depends significantly on the pre-existing database of known attacks. The depth and breadth of the vendor's database can be enhanced by an increased adoption of the premium service. This results from the vendor gaining access to more customer data and greater expertise in threat detection, which enables it to continually enrich the database with the latest threats in the industry. Therefore, the value of the basic service, denoted as v_b, is affected by the market share of the premium service. We assume the achieved basic service quality in period t is

$$v_b[t] = \underline{v} + g(\eta_p[t]) \tag{3}$$

where $\underline{v}$ is the base quality level of the basic service. The function $g(\cdot)$ represents the increased service quality contributed by the threat information from the premium service, and actually reflects the positive network externality. The expression of $g(\cdot)$ is application dependent. For the sake of generality, we only assume $g(\cdot)$ is continuous and differentiable, and $g(0) = 0$, $g'(\eta_p) > 0$, $g(1) \leq v_p - \underline{v}$. Then the market shares η_b and η_p can be written as functions of $v_b[t]$ in period t as below:

$$\eta_b[t] = \begin{cases} 0 & \text{if } \pi_b > \pi_p \frac{v_b[t]}{v_p}, \\ 1 - \frac{\pi_b}{v_b[t]} & \text{if } \pi_b \leq \pi_p - v_p + v_b[t] \\ \frac{\pi_p - \pi_b}{v_p - v_b[t]} - \frac{\pi_b}{v_b[t]} & \text{otherwise} \end{cases} \tag{4}$$

$$\eta_p[t] = \begin{cases} 1 - \frac{\pi_p}{v_p} & \text{if } \pi_b > \pi_p \frac{v_b[t]}{v_p}, \\ 0 & \text{if } \pi_b \leq \pi_p - v_p + v_b[t] \\ 1 - \frac{\pi_p - \pi_b}{v_p - v_b[t]} & \text{otherwise.} \end{cases} \tag{5}$$

We denote the difference in terms of market share between time step t and $t-1$, by $\Delta\eta_s$. The market equilibrium is arrived when $\Delta\eta_s = 0$:

Definition 1 (Market Equilibrium)**.** *(η_b^*, η_p^*) is an equilibrium point of the market share if it satisfies $\eta_s^* = \eta_s[t] = \eta_s[t+1]$ for both $s \in \{b, p\}$.*

Proposition 1 (Market Equilibrium)**.** *The market equilibrium depends on the price of the basic service π_b:*

(1) Low Price: if $\pi_b \leq \pi_p - v_p + \underline{v}$, no customer subscribes to the premium service, and the market shares of the basic service is $\eta_b^* = 1 - \frac{\pi_b}{\underline{v}}$.

(2) High Price: if $\pi_b > \frac{\pi_p}{v_p}(\underline{v} + g(1))$, no customer subscribes to the basic service, and the market shares of the premium service is $\eta_p^* = 1 - \theta_p = 1 - \frac{\pi_p}{v_p}$.

(3) Medium Price: if $\pi_p - v_p + \underline{v} < \pi_b \leq \frac{\pi_p}{v_p}[\underline{v} + g(1)]$, there exists a unique market equilibrium if

$$max_{\eta_p \in [0,1]} \frac{(\pi_p - \pi_b) g'(\eta_p)}{(v_p - \underline{v} - g(\eta_p))^2} < 1 \tag{6}$$

and the market equilibrum satisfies

$$\eta_p^* = \begin{cases} 1 - \frac{\pi_p - \pi_b}{v_p - \underline{v} - g(\eta_p^*)} & \text{if } \pi_b \leq \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})], \\ 1 - \frac{\pi_p}{v_p} & \text{if } \pi_b > \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})]. \end{cases} \tag{7}$$

$$\eta_b^* = \begin{cases} 1 - \eta_p^* - \frac{\pi_b}{\underline{v} + g(\eta_p^*)} & \text{if } \pi_b \leq \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})], \\ 0 & \text{if } \pi_b > \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})]. \end{cases} \tag{8}$$

Proof: (1) Proof for the existence and uniqueness of the equilibrium: Let's assume that $E(\eta_p) = 1 - \frac{\pi_p - \pi_b}{v_p - \underline{v} - g(\eta_p)} - \eta_p$ for $\eta_p \in [0, 1]$. By definition, the roots of $E(\eta_p)$ are the equilibrium points as defined in Definition 1. Note that $E(0) = 1 - \frac{\pi_p - \pi_b}{v_p - \underline{v}} \geq 1 - \frac{\pi_p - \pi_b}{v_p - v_b} > 0$ and $E(1) = 1 - \frac{\pi_p - \pi_b}{v_p - \underline{v} - g(1)} - 1 = -\frac{\pi_p - \pi_b}{v_p - \underline{v} - g(1)} < 0$. As $E(\eta_p)$ is continuous on $[0, 1]$, $E(\eta_p)$ has at least one root on $[0, 1]$. Since $E'(\eta_p) = -\frac{(\pi_p - \pi_b) g'(\eta_p)}{(v_p - \underline{v} - g(\eta_p))^2} - 1 < 0$, $E(\eta_p)$ is strictly decreasing on $[0, 1]$. Therefore, $E(\eta_p)$ has only one root within $[0, 1]$. Next we analyze whether this root satisfies $\pi_p - v_p + v_b < \pi_b \leq \pi_p \frac{v_b}{v_p}$. Because $g(\cdot)$ is a continuous function, there exists a value of η_p, denoted by $\eta_{p,a}$, that satisfies $\pi_p - v_p + \underline{v} + g(\eta_{p,a}) = \pi_b$, and another value $\eta_{p,b}$, such that $\pi_b = \pi_p \frac{\underline{v} + g(\eta_{p,b})}{v_p}$. We can derive that $\eta_{p,a} = g^{-1}(v_p - \pi_p + \pi_b - \underline{v})$ and $\eta_{p,b} = g^{-1}(\pi_b \frac{v_p}{\pi_p} - \underline{v})$. Note that as $\pi_b > \pi_p - v_p + \underline{v}$, we have $E(\eta_{p,a}) = -g^{-1}(v_p - \pi_p + \pi_b - \underline{v}) < 0$. As $E(\eta_{p,b}) = 1 - \frac{\pi_p}{v_p} - g^{-1}(\pi_b \frac{v_p}{\pi_p} - \underline{v})$, if $\pi_b \leq \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})]$ then $E(\eta_{p,b}) \geq 0$. In this case, the root satisfies $\pi_p - v_p + v_b < \pi_b \leq \pi_p \frac{v_b}{v_p}$. Otherwise, if $\pi_b > \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})]$, we have $E(\eta_{p,a}) < 0$ and $E(\eta_{p,b}) < 0$, then the root satisfies $\pi_b > \pi_p \frac{v_b}{v_p}$, when no customer subscribes to the basic service.

(2) Proof for the convergence of the market: We define $F(\eta_p) = 1 - \frac{\pi_p - \pi_b}{v_p - \underline{v} - g(\eta_p)}$. Let $\eta_{p,a}$ and $\eta_{p,b}$ be two different real numbers arbitrarily chosen from the interval $[0, 1]$, and suppose without loss of generality that $\eta_{p,b} > \eta_{p,a}$. As $F(\cdot)$ is continuous and differentiable on $[0, 1]$, according to the mean value theorem, there exists $\eta_{p,c} \in (\eta_{p,a}, \eta_{p,b})$ such that $F'(\eta_{p,c}) = \frac{F(\eta_{p,b}) - F(\eta_{p,a})}{\eta_{p,b} - \eta_{p,a}}$, or

$$\begin{aligned} &|F(\eta_{p,b}) - F(\eta_{p,a})| = |F'(\eta_{p,c})||\eta_{p,b} - \eta_{p,a}| \\ &= \frac{(\pi_p - \pi_b) g'(\eta_p)}{(v_p - \underline{v} - g(\eta_p))^2} |\eta_{p,b} - \eta_{p,a}|. \end{aligned} \tag{9}$$

We denote $k = \max_{\eta_p \in [0,1]} \frac{(\pi_p - \pi_b) g'(\eta_p)}{(v_p - \underline{v} - g(\eta_p))^2}$. If $k < 1$, then $\forall \eta_{p,a}, \eta_{p,b} \in [0, 1]$, there is a value of k such that $|F_1(\eta_{p,a}) - F_1(\eta_{p,b})| \leq k|\eta_{p,a} - \eta_{p,b}|$. According to the contraction mapping theory [17], η_p converges to a fixed point η_p^*. □

Prop 1 indicates that the market will always reach a unique equilibrium if the network externality increases slowly with η_p, or if the premium service coverage has a small impact on the basic service quality. This assumption is realistic since the bug-hunting expertise gained in premium service is limited in enhancing the IDS effectiveness due to the ever-evolving nature of cyber threats. Besides, there is an inherent time delay in the process of cybersecurity experts generating signature for newly identified threats from the premium service and incorporating them into the software used in the basic service.

V. Profit Maximization

The vendor needs to optimize its pricing decision π_b for its basic service to maximize its expected profit. Given the market share equilibrium (η_b^*, η_p^*), the vendor's expected profit is

$$\Pi^V = \eta_p^*(\pi_p - c_p) + \eta_b^*(\pi_b - c_b) - c_0 \tag{10}$$

where c_p and c_b are the operating costs proportional to the market shares of the basic service and the premium service respectively. We assume $c_b < c_p$ since c_p includes not only the infrastructure and maintenance cost, but also higher personnel cost due to the salaries paid to cybersecurity professionals hunting for vulnerabilities. c_0 denotes the fixed cost, which includes expenses like upgrade costs, insurance, and equipment depreciation. According to Proposition 1, under low price, $\Pi^V = (1 - \frac{\pi_b}{\underline{v}}) * (\pi_b - c_b) - c_0$; and under high price, $\Pi^V = (1 - \frac{\pi_p}{v_p})(\pi_p - c_p) - c_0$. Under medium price, if the condition (6) holds, the market equilibrium can be obtained by solving (7) and (8). As $\eta_p^* = 0$ when $\pi_b \leq \pi_p - v_p + \underline{v}$ and $\eta_b^* = 0$ when $\pi_b > \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})]$, we will focus on the case of $\pi_p - v_p + \underline{v} < \pi_b \leq \frac{\pi_p}{v_p}[\underline{v} + g(1 - \frac{\pi_p}{v_p})]$.

Due to the difficulty in deriving the optimal price π_b^* to maximize (10), we first convert the original profit maximization problem, with π_b as the decision variable, into an equivalent problem with the market share η_p as the decision variable. The conversion is possible due to the one-to-one mapping between η_p and π_b. By substituting (7) and (8) into (10), the optimization problem becomes

$$\begin{aligned} &\max_{\eta_p \in [0,1]} \Pi^V(\eta_p) = \eta_p(\pi_p - c_p) \\ &+ (1 - \eta_p - \frac{\pi_b(\eta_p)}{\underline{v} + g(\eta_p)})(\pi_b(\eta_p) - c_b) - c_0. \end{aligned} \tag{11}$$

which is a straightforward nonlinear programming problem. Once we obtain the optimal value η_p^*, according to (7), the optimal value of π_b can be derived using $\pi_b(\eta_p) = \pi_p - (1 - \eta_p)(v_p - \underline{v} - g(\eta_p))$.

VI. Conclusion

The expansion of the cybersecurity market, particularly in the realm of threat intelligence, is highly affected by the network effects, given that the timeliness and accuracy of security solutions are critically dependent on the information collected and expert experience. This paper studies the positive effects between two services offered by one cybersecurity vendor, and analyzes how the evolution of market is conditioned by the service quality, price and their interrelationship. We analyzed the optimal pricing strategy so that the vendor could leverage the network effects for profit maximization. Our results show that the market always reaches a unique equilibrium if the premium service coverage has a low impact on the basic service quality. This paper examines the interrelationship between a single vendor's services. Future research should explore a market model where cybersecurity vendors collaborate and compete.

Acknowledgments

The work was partially supported by the (CNS-2415209, CNS-2321763, CNS-2319343, and CNS-2317190).

References

[1] "Cybersecurity: market data analysis." https://www.statista.com/study/124902/cybersecurity-report/, 2023. [Online; accessed 2-Nov-2023].

[2] "Xonicwave." https://lp.xonicwave.com/, 2023. [Online; accessed 2-Nov-2023].

[3] "All-in-one managed cybersecurity subscriptions.." https://cyvatar.ai/membership-pricing/, 2023. [Online; accessed 2-Nov-2023].

[4] Z. Rashid, U. Noor, and J. Altmann, "Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem," *Future Generation Computer Systems*, vol. 124, pp. 436–466, 2021.

[5] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an industry: A cyber threat intelligence perspective," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 135–154, 2020.

[6] J. Church, N. Gandal, and D. Krause, "Indirect network effects and adoption externalities," *Review of Network Economics*, vol. 7, no. 3, 2008.

[7] A. Zainudin, R. Akter, D.-S. Kim, and J.-M. Lee, "Federated learning inspired low-complexity intrusion detection and classification technique for sdn-based industrial cps," *IEEE Transactions on Network and Service Management*, 2023.

[8] A. Calderaro and A. J. Craig, "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building," *Third World Quarterly*, vol. 41, no. 6, pp. 917–938, 2020.

[9] L. Xu, Y. Li, Y. Lin, C. Tang, and Q. Yao, "Supply chain cybersecurity investments with interdependent risks under different information exchange modes," *International Journal of Production Research*, pp. 1–26, 2023.

[10] M. Lelarge, "Coordination in network security games: a monotone comparative statics approach," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2210–2219, 2012.

[11] J. Simon and A. Omar, "Cybersecurity investments in the supply chain: Coordination and a strategic attacker," *European Journal of Operational Research*, vol. 282, no. 1, pp. 161–171, 2020.

[12] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," *Journal of Economic Surveys*, vol. 36, no. 1, pp. 157–187, 2022.

[13] M. Asghari, S. Yousefi, and D. Niyato, "Pricing strategies of iot wide area network service providers with complementary services included," *Journal of Network and Computer Applications*, vol. 147, p. 102426, 2019.

[14] M. Harishankar, N. Srinivasan, C. Joe-Wong, and P. Tague, "To accept or not to accept: The question of supplemental discount offers in mobile data plans," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pp. 2609–2617, IEEE, 2018.

[15] X. Wang, L. Duan, and J. Zhang, "Mobile social services with network externality: From separate pricing to bundled pricing," *IEEE Transactions on Network Science and Engineering*, vol. 6, no. 3, pp. 379–390, 2019.

[16] N. Haile and J. Altmann, "Value creation in it service platforms through two-sided network effects," in *Economics of Grids, Clouds, Systems, and Services: 9th International Conference, GECON 2012, Berlin, Germany, November 27-28, 2012. Proceedings 9*, pp. 139–153, Springer, 2012.

[17] K. Conrad, "The contraction mapping theorem," *Expository paper. University of Connecticut, College of Liberal Arts and Sciences, Department of Mathematics*, 2014.