Cybersecurity and Market Share in Digital Ecosystems with Network Externalities

Daniel Arce
University of Texas at Dallas
800 W. Campbell Rd
Richardson, TX 75013
darce@utdallas.edu

Abstract

Digital ecosystems with network externalities compete for users and face cyberattacks. This paper introduces a game-theoretic benchmark that endogenizes ecosystems' defense, users' adoption, and hackers' targeting within the context of (own-side) network externalities. An ecosystem's cybersecurity strategy corresponds to their defensive intensity to both protect users' network benefits and increase defensive opaqueness. The analysis shows ecosystems' cybersecurity strategies are strategic complements; market share increases in cybersecurity; and hacker targeting increases in market share regardless of an ecosystem's defenses. Paradoxically, more need not be better within this complex system, as conditions exist whereby defensive intensity both decreases and increases the incentives for hacking. In addition, the ecosystems-users-hackers triad can sustain non-monopolistic competition despite strong network externalities. The findings offer strategic guidance for ecosystem managers by accounting for attackers', users', competitors', and their own incentives.

1. Introduction

Users of Microsoft's Office Suite or Google Docs benefit when collaborators use the same suite as well. Similarly, user benefits of social networks such as Facebook, LinkedIn, and Twitter (now 𝕏), increase with additional membership. When users of digital ecosystems benefit from the number of other users, this is known as a (direct or own-side) network externality. Compatibility, ease of collaboration and communication, content sharing, shared code, and Metcalfe's law are phenomena exhibiting network externalities. Consequently, market share matters in competition among digital ecosystems with network externalities.

These and other digital ecosystems exhibiting network externalities experience persistent cybersecurity attacks. Breaches can disrupt service, deliver or relay attacks on users, and erode trust. For example, owing to increasing incidents Microsoft founded and continues Patch Tuesday as part of its Trusted Computing initiative. Facebook's approach emphasizes continuous unbranded security changes rather than a named program. Both efforts show cybersecurity in digital ecosystems is not merely a technical safeguard, but a strategic choice shaped by economic incentives, competition, and hacker behavior.

This paper investigates the interaction between cybersecurity and market share in digital ecosystems with network externalities. We conceptualize cybersecurity as *defensive intensity that protects users' ability to realize network benefits*, rather than the full governance or prevention stack. This abstraction isolates fundamental market mechanisms of ecosystem cybersecurity: cybersecurity acts as a gateway to users' network benefits, while market share affects hackers' ability to operate at scale given users' selection of ecosystems.

Two strands of literature address parts of this problem but largely in isolation. The intrusion detection game literature endogenizes attacker behavior and defensive intensity

[Chen & Leneutre 2009, Collins et al. 2025, Gianini et al, Otrok et al.2013, Rass and Zhu 2016]. Yet, market share is determined by users selecting one ecosystem versus another. This process of selection is absent in intrusion detection games.

By contrast, user market share is of primary consideration in ecosystem selection cybersecurity games **[Arce 2018, O'Donnell 2008]**. Users select an ecosystem based on its network externalities, as measured by market share. That is, users' mixed strategies represent market share or summaries of heterogeneous behavior rather than randomization by individual decision makers. Hackers decide which ecosystem to attack based on the value at stake for each ecosystem. The degree to which users accrue network externalities depends on the ecosystem's level of security, which is exogenous. As a result, neither approach addresses how cybersecurity shapes incentives when ecosystems, users, and hackers all behave strategically.

We develop a unified game-theoretic benchmark that integrates these literatures by endogenizing user adoption, hacker targeting, and ecosystem defense. Two competing ecosystems independently choose their level of defensive intensity. Users select ecosystems to realize network benefits. Hackers sort over the ecosystem they attack according to their expected payoffs. A successful breach compromises users' network benefits. Importantly, market share need not be an argument in hackers' payoffs to matter for their targeting decision. Market share determines the scale at which hackers operate.

The analysis relies on monotone comparative statics **[Milgrom and Roberts 1990, Echenique 2003, Roy and Sabarwal 2012]** to characterize strategic complements and substitutes among ecosystems, users, and hackers. The approach identifies robust incentives without relying on specific equilibrium assumptions (e.g., Nash versus Stackelberg) or

necessitating closed-form solutions.[1] Applying monotone comparative statics to the unified benchmark highlights how strategic responses propagate through a multi-agent environment.

On the theoretical side, the paper makes the following contributions. First, it provides a unified benchmark that endogenizes user adoption, hacker targeting, and ecosystem cybersecurity in the presence of network externalities. Second, it characterizes cybersecurity competition. Ecosystems' defensive intensity moves in tandem, rather than one ecosystem exhibiting high security and the other low. An ecosystem's market share is increasing in its cybersecurity. At the same time, hacking leads to a bifurcated market whereas network externalities might otherwise lead to a monopoly. Moreover, market share matters to hackers because it determines the degree they operate at scale as determined by user adoption. The benchmark captures a complex symbiotic system where the competitive environment influences (in)security and (in)security influences the competitive environment.

A key challenge is characterizing incentives in such complex environments. Increasing defensive intensity attracts users and deters hackers. Attracting users increases market share and market share attracts both hackers and users. Hence, ecosystem security is a complex system. For this reason, the unified game allows for the *Wolff* **[2016]** Effect: more need not be better when it comes to cybersecurity. From a technical perspective, added defense may increase the attack surface. From an economic perspective, with more users, hackers can operate at scale.

Theoretical variations on the unified model include the impact of artificial intelligence

[1] Indeed, deriving a mixed Stackelberg equilibrium for one leader with multiple followers is NP-hard **[Coniglio et al, 2020]**. This is further exacerbated because applying a Stackelberg framework to the game involves two leaders (ecosystems) each with multiple followers (users and hackers).

(AI); imperfect monitoring; resiliency versus security; and different hacker payoff consequences for attacking high versus low market share ecosystems. All results are robust to these variations. At the same time, the variations introduce novel findings such as a measure of materiality of loss due to cyberattacks. This measure sets the threshold for additional defensive intensity to increase market share. Consequently, the model serves as a benchmark for more elaborate theoretical or empirical work on security and market structure for network ecosystems.

Our characterizations of strategic complements and substitutes translate into five managerial questions: (1) is what I am doing now optimal relative to what the competition is currently doing? If not, then in what direction should I be changing? (2) Is my competition optimizing relative to what I am currently doing? If not, what direction do I predict for them? (3) If I change what I am doing, what is my prediction for how the competition will react? (4) How do I respond when the competition changes what they are doing? (5) What is the effect of (1)-(4) on users and hackers? These directional insights, based on marginal strategic incentives, guide security strategy without requiring closed-form equilibrium solutions.

In addition, we identify the limit of technical solutions to cybersecurity. **Hardin [1968]** originally coined the idea and phrase, “no technical solution” within the context of resolving the Tragedy of the Commons. Recognizing this, **Ostrom [1990]** shows communities can successfully manage common pool resources, rather than technology, government, or privatization. For cybersecurity, ‘no technical solution’ translates into the limits of coding solutions **[Arce 2020, Shapiro 2023]**. This opens the door for future work considering governance and resilience, while preserving a clear characterization of strategic incentives.

2. Related Literature

This paper concerns the cybersecurity of ecosystems where users receive network externalities in the sense of **Rohlfs [1974]** and **Metcalfe [1995]**. That is, users benefit from the presence of additional users. Examples include software compatibility, massive multiplayer online games, mobile phones, social media, and collaboration on content management webservers. Such ecosystems exhibit network (same-side or direct) externalities. **Gandal [1994]** and **Metcalfe [2013]** are early empirical validations of network externalities for software and social networks.

The analysis introduces a benchmark model unifying intrusion-detection and ecosystem-selection cybersecurity games. At their core intrusion detection games are inspection games **[Chen & Leneutre 2009, Collins et al. 2025, Fudenberg & Tirol 1992]**. An inspection game captures the basics of intrusion detection in the following ways. There are two players: malicious actors, called hackers here, who target an ecosystem; and the ecosystem hackers target. No users or network externalities are present. Hackers decide whether to target an ecosystem or not and the ecosystem decides whether to monitor for an attack or not. Owing to the costs of human capital and computational time/resources/energy associated with always-on monitoring, the ecosystem monitors probabilistically to optimize the tradeoff between these costs and the benefits of detection **[Gianini et al. 2013]**. In this way, unpredictability on behalf of the ecosystem's defense substitutes for the cost of always-on monitoring.

In the original form of the inspection game, the probability a defender detects an attacking hacker is equivalent to the probability the defender monitors. Variations on the inspection-game-as-intrusion-detection include defender uncertainty about whether a user

is malicious or legitimate **[Liu, Comanciu and Man 2006, Otrok et al. 2009]**. This imbues monitoring with the potential for type I and II errors. The hacker can also be uncertain about whether the defender is legitimate or is practicing deceptive defense-in-depth (e.g., a honeypot) **[Huang & Zhu 2020]**. **Rass and Zhu [2016]** consider a computer network as a series of inspection games, where penetrating the next network level requires penetrating all previous levels.

In ecosystem selection cybersecurity games, there are two populations of players: hackers attacking ecosystems, and users who both generate and receive network externalities by selecting an ecosystem **[Arce 2018, O'Donnell 2008]**. **O'Donnell [2008]** investigates the market share conditions whereby attacking one and only one ecosystem is a dominant strategy for the hacker. The probability of detection is an exogenous parameter. O'Donnell's conditions show low market share implies little economic interest on the part of hackers. At the time, this was the case for Apple versus Microsoft in terms of low versus high market share for operating systems for desktops and laptops. As O'Donnell determines conditions for a dominant strategy equilibrium, the conditions are independent of the actions of users, defined as which ecosystem to protect. Consequently, O'Donnell does not specify users' payoffs because users' incentives do not matter to hackers if hackers have a dominant strategy.

Arce [2018] recognizes users determine an ecosystem's market share and, owing to network externalities, users select an ecosystem based on market share à la Metcalfe's law. Successful hacking reduces users' benefits from network externalities. Consequently, hacking bifurcates the market, with a proportion of users selecting one ecosystem and the rest selecting the other. Hacker targeting bifurcates as well, as hackers no longer have a dominant

strategy. An ecosystem's relative market share is a function of the square root of the ratio of the competitor's vulnerability (probability of an unmonitored attack) to the ecosystem's vulnerability. This provides an economic rationale for cybersecurity. Once again, however, each ecosystem's cybersecurity is a given parameter.

Intrusion detection games are typically 2-player games between an attacker and a defender. The rationale for why the defender is in business is rarely articulated. Generally, neither users nor network externalities are present. Here, users differ from defenders. The defender is an ecosystem exhibiting network externalities for a population of users who endogenously select the ecosystem. In ecosystem selection cybersecurity games, the ecosystem's level of security is a parameter. In the present study, everyone behaves strategically. Ecosystem cybersecurity protects users' network externalities and their own value at stake in the event of a breach. Hackers attack ecosystems for the value of what is at stake. Users select ecosystems for their network externalities. All parties are active participants, reflecting the full complexity of information systems security.

Analysis of the unified game contributes to the research on intrusion detection games and ecosystem selection cybersecurity games by endogenizing all players. When all three act strategically, this provides new system-level characterizations of the behavior of users, ecosystems, and hackers. It also contributes to the emerging research on the relationship between cybersecurity and market structure. For example, the presence of network externalities is often though to lead to users selecting a single digital ecosystem. That is, network externalities result in monopoly (winner-take-all). When hackers also reap network externalities from compromising ecosystems, the market can instead bifurcate **[Arce 2018]**.[2]

[2] See also **Jegers and Van Hove [2020]**.

In the present model, hackers' payoffs need not be a function of the network externalities created by the ecosystem's users for the market to bifurcate.

Sen, Verma, and Heim [2020] examine hacker population dynamics in software markets with network effects. They find the absence of hackers leads to monopoly due to network effects and tipping. By contrast, when the authors assume hackers target more than one ecosystem, a competitive environment becomes feasible and sometimes stable. In their model the probability hackers successfully target an ecosystem is exogenous. In the present model this probability is endogenous and strategically determined by the ecosystem's defensive intensity and market share. **Geer, Jardine and Levert [2020]** break down the three dimensions of cyber risk (threat, vulnerability, impact), arguing market concentration affects cybersecurity risk across all three dimensions. This implies cyberinsurance must reflect market concentration and not just firm size.

Garcia, Sun, and Shen [2014] develop a model of two-sided competition between platforms servicing users on one side and hackers as adversarial agents on the other side. By assumption, hackers prefer platforms with more users (greater market share). Platforms choose price and security over time. When hackers' exogenous level of sensitivity to a platforms' market share of users is low, hackers target both platforms more evenly. A dominant platform maintains or increases its dominance by increasing its security effort, resulting in market asymmetry or monopoly. When hackers' exogenous level of sensitivity to a platforms' market share of users is high, security costs rise for dominant platforms. Smaller platforms can counter with lower prices and better security. The market evolves toward a competitive one with symmetrical market shares. In their model, users' benefit from security is independent from the network externality generated by selecting an ecosystem. In the

present model, security is the gateway to the network externality. That is, a successful hack compromises the network externality. In addition, the authors assume increasing security pushes hackers toward the ecosystem's competitor. In the present model, security directly protects users' network externalities.

Wolff [2016] identifies cases where increasing security within a complex system ultimately increases hacker targeting. While **Wolff [2016]** makes technical conjectures for why this occurs, the present analysis provides a complementary economic and theoretical underpinning. Specifically, ecosystem security raises its market share. The larger market share allows hackers to operate at scale, thereby affecting hackers' choice of target. A novel aspect of this result is it does not require the assumption that ecosystem market share in an argument in hackers' payoffs. As such, the present analysis is a contribution to the literature establishing not only do digital ecosystem compete for users based on cybersecurity, but cybersecurity influences the competitive environment (market structure) of digital ecosystems. Both the Wolf and competitive effects are system-level phenomena. They are only possible by endogenizing the strategic decisions of all major participants in a unified game. Table 1 summarizes this contribution.

[Insert Table 1 here]

Characterizing this complex system addresses what is absent in both the literature on intrusion-detection and ecosystem-selection cybersecurity games: identifying whether actions are strategic complements or substitutes. Moreover, the characterizations here are not limited to strategic choices over the same variable, such as price, quantity, or quality. The security of information systems is more complex. In the unified game strategic complements and substitutes occur among and between similar actors (ecosystems), co-opetive actors

(ecosystems and users), and adversarial actors (hackers versus ecosystems and users). In this way, the analysis goes beyond labeling competition in terms of the strategic variables – ecosystem selection by users, ecosystems' defensive intensity, and ecosystem targeting by hackers – and characterizes how actors' behavior shape another's incentives, sometimes in unexpected ways. At the same time, our intent is not to model the full governance stack but provide a unifying benchmark linking two literatures that have largely developed in parallel.

The characterizations of the competitive environment come in the form of identifying strategic complements and substitutes via monotone comparative statics **[Milgrom and Roberts 1990, Echenique 2003, Roy and Sabarwal 2012]**. Strategic complements and substitutes characterize the *direction* of strategic interdependence between users, ecosystems, and hackers. These directions predict others' reactions and guide manager's own actions. Monotone comparative statics are an ending point in themselves as they are robust to model-specific considerations such as timing or imperfect versus perfect information.[3] This clarifies the nature of complex systems for managers. As such, monotone comparative statics inform our understanding of the competitive environment and the effect of shocks such as AI. They also translate into industry practices such as defense-in-depth, defensive opacity, and AI-augmented detection.

3. Benchmark Game

Table 2 defines the variables for the unified game given in Figure 1. There are two ecosystems {1,2}. Users (U) select ecosystem 1 or 2 for the purposes of accruing network

[3] By contrast, equilibrium comparative statics are sensitive to these considerations, particularly in the presence of strategic substitutes. Under strategic substitutes, feedback effects are sensitive to countervailing best replies.

benefits. Malicious actors (hackers) are the fourth population (H). Ecosystem 1 monitors for hackers with probability $p \in [0,1]$ and ecosystem 2 monitors with probability $q \in [0,1]$. Proportion $\tau \in [0,1]$ of hackers target ecosystem 1 and $1 - \tau$ target ecosystem 2. Proportion $\sigma \in [0,1]$ of users select ecosystem 1 and proportion $1 - \sigma$ select ecosystem 2.

[Table 2 here]

[Figure 1 here]

We refer to populations rather than players because the interpretation of mixed strategies for users and hackers is the 'mass action' one **[Nash 1950]**. In this interpretation, the pure strategies employed by different individuals in a population are cross-sectionally distributed according to the mixtures [**Cornell & Roll 1981, Jacquemin 1987]**. Within the context of cybersecurity, the mass action interpretation explicitly appears in **Arce [2018]** and **Kiennert et al. [2018]**. Consequently, the interpretation of mixed strategies for users and hackers is the mass action one, characterizing the proportion of users and hackers selecting or attacking ecosystems 1 (σ and τ) and 2 ($1 - \sigma$ and $1 - \tau$). In this way, mixtures substitute for unmodeled heterogeneity when player types or capabilities are not explicitly parameterized **[Collins, Xu, and Brown 2025]**.

By contrast, as each ecosystem is a single entity, the mass action interpretation is less common.[4] Instead, the interpretation of monitoring probabilities is as summarizing *defensive intensity*. Such effort can be bounded in the [0, 1] interval without loss of generality. This abstraction follows a long tradition in intrusion-detection games and principal-agent models with monitoring. It captures the idea that ecosystems choose how intensively they deploy

[4] Yet under decentralized responsibility for cybersecurity within the organization, as is often the case, even if each subunit follows a rule, the aggregate behavior appears mixed because subunits are heterogeneous.

detection, opacity, and response capabilities given the associated tradeoffs. Examples include defense-in-depth and opacity-creating tactics such as passive detection. Another interpretation of mixed strategies is as players' beliefs when forming expectations regarding other players' behavior. This is consistent with **Aumann's [1987]** perspective on strategic uncertainty.

In this way, users' ecosystem selection determines whether subgame game G_1 or G_2 occurs in Figure 1. Each of G_1 and G_2 represents an intrusion detection/inspection game between an ecosystem and hackers. The order of payoffs in each cell of G_1 is ecosystem 1, hacker, users. In G_2 the order of payoffs is ecosystem 2, hackers, users. That is, each cell lists the respective ecosystem's payoff first, followed by the payoffs for hackers and then users.

In subgame G_1, ecosystem 1's value at stake if breached is $v > 0$. In G_2 ecosystem 2's value at stake if breached is $\omega > 0$. As is the case in intrusion detection games, the focus is on financially-motivated hacking. Hence, ecosystem and hacker payoffs are zero-sum in what is at stake. For example, when ecosystem 1 does not monitor and a hacker attacks 1, the outcome yields $-v$ to ecosystem 1 and v to the hacker. If ecosystem 1 monitors an attacking hacker, the outcome yields v to ecosystem 1 and $-v$ to the hacker. In subgame G_2, similar arguments hold for ω and $-\omega$ for ecosystem 2 and its interactions with hackers.

Yet the game itself is non-zero-sum due to ecosystems' and hackers' costs. Ecosystem i's monitoring cost is $c_i > 0, i = 1,2$. Ecosystems prefer monitoring to a breach: $v - c_1 > -v$ and $\omega - c_2 > -\omega$. In this way parameter c_1 represents ecosystem 1's exogenous cost of deploying defensive intensity at any given level, p; and c_2 represents the same for ecosystem 2 at any given intensity, q. Ecosystems do not choose c_i. Instead, c_i represents a technological threshold required to justify increasing defensive intensity. The model thereby satisfies

Courtney's [1982] requirement that cybersecurity decisions are made by comparing expected marginal benefit versus marginal cost (= net marginal benefit).

A hacker's cost of attacking ecosystem i is $k_i > 0, i = 1,2$. These costs and the zero-sum nature of payoffs in v and ω determine hackers' payoffs when hackers attack an ecosystem that users select. For example, if users select ecosystem 1, hackers attack 1, and ecosystem 1 monitors, the hackers' payoff is $-v - k_1$ in the northwest cell of G_1. If users select ecosystem 2, hackers attack 2, and ecosystem 2 does not monitor, the hackers' payoff is $\omega - k_2$ in the southeast cell of G_2.

What remains to specify are hackers' payoffs when attacking an ecosystem that users do not select. In these cases, the benchmark normalizes hacker payoffs to zero for attacking an ecosystem with ex-post zero market share. This assumption is relaxed later.

Term $s \in (0,1)$ denotes ecosystem 1's market share of users. Facebook initially had Myspace as a competitor and is in quasi competition with LinkedIn, hence, $s \neq 0$ or 1. Microsoft faced down myriad competitors, including WordPerfect and Lotus, and now contends with Google Docs. Again, $s \neq 0$ or 1. In a fulfilled expectations equilibrium **[Kreps 1977]**, $s = \sigma$. This is an ex-post condition rather than an ex-ante one, which is why payoffs are in terms of s instead of σ. The assumption is used sparingly and then only to characterize behavior between ecosystems (p and q). With respect to users' benefit from network externalities, by Metcalfe's law s is a user's payoff when selecting ecosystem 1 unless ecosystem 1 is breached. A breach corresponds to the strategy combination where hackers attack 1 and ecosystem 1 does not monitor (the southwest cell of G_1), yielding a user payoff of zero. Similarly, users selecting ecosystem 2 receive a payoff of $1 - s$ unless ecosystem 2 is breached. A breach corresponds to the strategy combination when hackers attack ecosystem

2 and 2 does not monitor (the southeast cell of G_2), yielding a user payoff of zero. In this way, cybersecurity is the gateway to the network externalities differentiating each ecosystem for users.

4. Incentive Structure

When users select ecosystem 1, the G_1 part of the game occurs. In G_1 if hackers attack ecosystem 2, then ecosystem 1 does not monitor to avoid the cost of monitoring ($v > v - c_1$). If ecosystem 1 does not monitor, hackers attack 1 ($v - k_1 > 0$). If hackers attack 1, ecosystem 1 monitors ($v - c_1 > -v$). If ecosystem 1 monitors, hackers attack 2 ($0 > -v - k_1$). Hence, G_1 has a clockwise sequence of best replies for ecosystem 1 and hackers. Such a sequence of best replies is a classic property of enforcement games. Thus, G_1 is characterized by mixed strategies. By similar reasoning, when users select ecosystem 2, G_2 has a counterclockwise sequence of best replies for ecosystem 2 and hackers. Again, the implication is mixed strategies characterize G_2.

For hackers, mixed strategies imply heterogeneous behavior in the form of a cross-section of hackers targeting ecosystem 1 with the rest targeting 2. For each ecosystem, mixtures represent reduced-form summaries of (i) defensive intensity and opacity, (ii) organizational heterogeneity, and (iii) imperfect hacker learning under these conditions. What matters is not literal randomness, but that hackers cannot condition a best response on a predictable action.

Finally, under these mixed strategies the following outcomes occur with positive probability: (i) hackers attack 1 and neither ecosystem 1 nor ecosystem 2 monitor (southwest cells of G_1 and G_2), and (ii) hackers attack 2 and neither ecosystem 1 nor

ecosystem 2 monitor (southeast cells of G_1 and G_2). In the first situation, users prefer ecosystem 2 ($1 - s > 0$). In the second situation, users prefer ecosystem 1 ($s > 0$). Consequently, users do not unilaterally prefer ecosystem 1 over ecosystem 2 or ecosystem 2 over ecosystem 1. The result is a cross-section of users selecting ecosystem 1 with the rest selecting ecosystem 2. That is, mixed strategies characterize user heterogeneity when selecting an ecosystem. As in **Arce [2020]** and **Sen, Verma, and Heim [2020]**, *the presence of hackers is pivotal for non-monopolistic competition*. Here, the result is novel in it applies to ecosystems with network externalities. Hence, it contributes to the emerging literature establishing the symbiotic relationship between cybersecurity and market structure.

Given the incentive structure, our analysis takes the perspective of interior behavior: $p, q, \sigma, \tau \in (0,1)$. The following rationales justify this approach. First, in focusing on interior behavior, the results characterize incentives away from corners. This is consistent with the empirical reality where neither perfect security nor zero attacks are observed. Similarly, monopoly ecosystems are not observed. When all players are active, this facilitates determining how strategic changes alter marginal incentives and propagate through a multi-agent environment. Second, the game in Figure 1 slices ecosystem-hacker interaction according to whether users select ecosystem 1 (G_1) or ecosystem 2 (G_2). Slices G_1 and G_2 are inspection games. Inspection games have unique mixed strategy Nash and Stackelberg equilibria **[Fudenberg & Tirole 1992, Andreozzi 2004]**. Third, ecosystem selection cybersecurity games between users and hackers are parameterized by p and q. This is an alternative way to slice the game. Given p and q the games have unique mixed strategy Nash and Stackelberg equilibria **[Arce 2018]**. While we take the interior perspective, the

methodology characterizes boundary behavior (pure strategies) as well.[5]

5. Methodology

The analysis begins by characterizing the strategic environment resulting from the benchmark unified game, as captured by strategic complements and substitutes. These properties are predictors of strategic interdependence between players. Strategic complements and substitutes characterize players' relative marginal incentives. If an increase in player *j*'s strategy raises player *i*'s marginal net benefit of increasing their own strategy, the two are strategic complements. Canonical examples include price (Bertrand) competition, coordination on standards, and advertising battles. Aggressive actions invite rivals to follow suit, with the potential for contagion or cascading effects. Standing still becomes relatively worse than responding in kind.

In contrast, if an increase in player *j*'s strategy decreases player *i*'s marginal net benefit of increasing their own strategy, the two are strategic substitutes. Canonical examples include quantity (Cournot) competition, capacity expansion in congested markets, and R&D races. Aggressive actions invite moderation by rivals, thereby potentially dampening the effects of the aggressive action. Responding in kind becomes relatively worse than holding back. Together, strategic complements and substitutes characterize the competitive environment.

These characterizations rely on monotone comparative statics **[Milgrom and Roberts 1990]** as extended to mixed strategies for one-dimensional strategy spaces (e.g.,

[5] No slicing according to a hacker parameterization is considered, as hackers are active players in both intrusion-detection and ecosystem-selection cybersecurity games.

price or quantity but not price *and* quantity simultaneously) **[Echenique 2003, Roy and Sabarwal 2012]**. The key difference between traditional comparative statics and monotone comparative statics is

- Traditional comparative statics compare equilibrium values across different scenarios.
- Monotone comparative statics analyze a player's marginal incentive to be more or less aggressive, irrespective of whether the strategies in question are in equilibrium.

Monotone comparative statics predictions do not depend on the system being in equilibrium, enabling a deeper understanding of the underlying mechanisms in a complex system.

The process begins with deriving the expected payoff difference for each player's pure strategies given the mixtures of the other players. Since expected payoffs are linear in each of these mixtures, the sign of the partial derivative of i's expected payoff with respect to player j's mixture, $j \neq i$, coincides with the sign of i's marginal payoff difference function, $\hat{\Delta}_i$, for pure strategies. This allows for identification of strategic complements or substitutes at a pairwise level in the **Milgrom and Roberts [1990]** sense. Characterization requires the change in mass of the underlying mixture to satisfy first order stochastic dominance, which holds trivially given each player's pure strategy set is binary. Furthermore, when strategic complements or substitutes hold for mixtures, they also hold for the underlying pure strategies as well, as the increasing difference properties continue to hold for pure strategies.

In practice, strategic complements and substitutes are defined in terms of increasing payoff differences for a "more aggressive" pure strategy, a_i, versus a less aggressive one, $\bar{a}_i$, **[Bulow et al. 1985, Milgrom and Roberts 1990]**. The ordering increases from $\bar{a}_i$ to a_i. For the present game, any mixed strategy for player i places positive probability on both a_i and $\bar{a}_i$. For ecosystem 1, $a_i = M$ and $\bar{a}_i = N$ is consistent with the interpretation of ecosystem's

mixture on M as defensive intensity. Consequently, given the mixed strategies of players other than i, x_{-i}, marginal (expected) payoff differences are characterized using the difference in expected payoff function: $\Delta_i(x_{-i}) \equiv E_i[a_i, x_{-i}] - E_i[\bar{a}_i, x_{-i}]$. Increasing marginal differences, $\frac{\partial \Delta_i}{\partial x_j} > 0; i \neq j$, correspond to strategic complements. Decreasing marginal differences, $\frac{\partial \Delta_i}{\partial x_j} < 0; i \neq j$, correspond to strategic substitutes.

To avoid any confusion, note that function Δ_i is not the relative payoff difference operator, $\hat{\Delta}_i(a_i, \bar{a}_i, y)$, as originally defined in the monotone comparative statics literature. The sign of $\hat{\Delta}_i(a_i, \bar{a}_i, y)$ tests for increasing or decreasing differences with respect to y = another player's ordered strategy pairs, $(a_j, \bar{a}_j)$, or one of i's parameters, θ. For pure strategies, the sign of $\hat{\Delta}_i(a_i, \bar{a}_i, a_j, \bar{a}_j)$ measures incentives in terms of marginal payoff differences for a_i versus $\bar{a}_i$ when j becomes more aggressive. **Echenique [2003]** and **Roy and Sabarwal [2012]** extend the theory to mixed strategy behavior. When (i) each player's strategy set is one-dimensional, and (ii) expectations are linear, then $\text{sign}\{\partial \Delta_i / \partial y\} \gtreqless 0 \Leftrightarrow \text{sign}\{\hat{\Delta}_i(a_i, \bar{a}_i, y)\} \gtreqless 0$. In particular, holding $x_{-\{i,j\}}$ constant, $\partial \Delta_i / \partial x_j$ returns $\hat{\Delta}_i(a_i, \bar{a}_i, a_j, \bar{a}_j)$. This is why the characterization holds for both mixed and pure strategies. Finally, characterization is possible without deriving the closed form of mixtures.

For mixtures, strategic complements imply that when the other player becomes more aggressive *in expectation*, the marginal benefit for player i to increase intensity (choose a_i over $\bar{a}_i$) increases (in the sense of first order stochastic dominance). Similar logic applies to strategic substitutes. This recognizes managerial decision making occurs within the context of uncertainty. It is also consistent with the interpretation that mixture x_j represents i's belief about j.

These characterizations capture incentive relationships that are essential to managerial decision making. Indeed, **Courtney [1982]** recognizes cybersecurity decisions must be economic. That is, made within a net marginal benefit context. For example, if a higher likelihood of attack increases the net marginal benefit of defensive intensity, then attacks and defensive intensity are strategic complements. Greater threat exposure raises the value of protection. Conversely, if increases in defensive intensity reduce the attractiveness of attacking a given ecosystem, decreasing the net marginal benefit of attacking, then defensive intensity and hacker targeting are strategic substitutes. Monotone comparative statics provide a method for determining how strategic changes alter marginal incentives and propagate through multi-agent information systems.

Furthermore, the partial derivative of $\Delta_i(x_{-i})$ is a function of i's primitives a_i and $\bar{a}_i$, with respect to pure strategy $a_{j\neq i}$ of another player or parameter θ. As such, characterizations using monotone comparative statics hold *irrespective of timing* (Nash or Stackelberg). This is because characterizations come from the relative payoff difference for player i, stemming from player i's more "aggressive" pure strategy versus their less aggressive one. As neither Nash nor Stackelberg assumptions change the structure of the payoffs, the monotone comparative statics do not change either.

6. Characterizing the Competitive Environment

Characterizations of the competitive environment are well-established for price (strategic complements) versus quantity competition (strategic substitutes). Within the context of management information systems, when consumers are parameterized to respond to service quality, duopolistic competition in IT-enabled service quality is characterized by strategic

complements **[Barua 1991]**. Given single-homing populations of buyers and sellers, competition between two-sided platforms over cross-side network externalities results in strategic substitutes **[Bakos and Katsamakas 2008].** Assuming exogenous hacker behavior, precautionary security efforts are strategic substitutes for end-users of the same vendor **[Png & Wang 2009]**, thereby generating a free-riding externality and suboptimal security. By contrast, end-user precautions can be strategic complements in the cloud **[Clement & Arce 2025]** because security creates selective incentives (private benefits) in the form of the profits end-users make in the cloud and the profits cloud service providers make from end-users.

Relative to these studies, more players, asymmetry, and heterogeneity are present in the benchmark. Ecosystem cybersecurity competition for users exists owing to the presence of hackers. Hence, there is a need to characterize both cybersecurity competition between ecosystems with asymmetric payoffs and ecosystems facing distinct types of actors: users and hackers. In addition, hacker targeting affects users' benefits from ecosystems, and users' ecosystem selection affects hackers' ability to operate at scale.

We derive the relationships for ecosystem 1 and its users, as those for ecosystem 2 and its users are similar. For ecosystems, the more aggressive strategy is monitoring, p and q, corresponding to defensive intensity. As the results are with respect to ecosystem 1, without loss of generality the aggressive strategy for hackers is targeting ecosystem 1, τ, and for users it is selecting 1, σ. Again, these relationships are independent of timing (Nash or Stackelberg). Moreover, given the asymmetry between ecosystems and hackers, hackers and users, and users and ecosystems, the default assumption that $\frac{\partial \Delta_i}{\partial x_j}$ and $\frac{\partial \Delta_j}{\partial x_i}$ have the same sign no longer holds. Hence, all characterizations taking the form: $\frac{\partial \Delta_i}{\partial x_j} > 0$ imply strategies are

strategic complements from j to i. Similarly, $\frac{\partial \Delta_i}{\partial x_j} < 0$ implies strategies are strategic substitutes from j to i.

For users, the expected payoffs difference for selecting ecosystem 1 versus 2 is a function of mixed strategies $p, \tau,$ and q. Thus, from figure 1

$$\Delta_{U_1} = E_U[1] - E_U[2]$$

$$\Delta_{U_1} = \underbrace{s\{p\tau + p(1-\tau) + (1-p)(1-\tau)\}}_{E_U[1]} - \underbrace{(1-s)\{q\tau + q(1-\tau) + (1-q)\tau\}}_{E_U[2]}$$

Rearranging terms:

$$\Delta_{U_1} = E_U[1] - E_U[2] = s\{1 + q + (p-q)\tau\} - [q + (1-q)\tau] \quad (1)$$

Property 1. The characteristics of the competitive environment for market share are:

i. $\frac{\partial \Delta_{U_1}}{\partial p} = s\tau > 0 \Rightarrow \sigma$ and p (and their associated pure strategies) are strategic complements from ecosystem 1 to users.

ii. $\frac{\partial \Delta_{U_1}}{\partial q} = (1-\tau)(s-1) < 0 \Rightarrow \sigma$ and q (and their associated pure strategies) are strategic substitutes from ecosystem 2 to users.

iii. $\frac{\partial \Delta_{U_1}}{\partial \tau} = s(p-q) - (1-q) < 0 \Rightarrow \sigma$ and τ (and their associated pure strategies) are strategic substitutes from hackers to users.

Properties 1(i) and (ii) characterize an ecosystem's expected market share as increasing in its own cybersecurity and decreasing in that of its competitor. When users expect ecosystem 1 to increase defensive intensity, they respond by increasing its market share. Strategic complements is indicative of this positive feedback look. This provides an economic rationale for cybersecurity that does not exist in intrusion detection games.

While not a measure of an ecosystem's profits, market share is nonetheless an important indicator of performance owing to users' interest in an ecosystem's network externalities. For example, Microsoft's focus on market share as a deliberate goal – rather than as a byproduct of innovation – led to a low security monoculture with the potential for cascading attacks **Geer et al. [2007]**. Security crises like the Nimda worm (2001) and Blaster worm (2003) exploited vulnerabilities in Windows systems, causing widespread damage **[Walters 2023]**. These issues damaged Microsoft's reputation for security, threatening erosion in trust and enterprise confidence. Competitors capitalized on the situation. Linux-based operating systems (like Ubuntu, Red Hat, and SUSE) promoted themselves as more secure and transparent alternatives. Cloud and SaaS competitors emerged, such as Salesforce and Google Apps, whose web-based alternatives require no local patching. Consequently, Microsoft introduced Patch Tuesday in October 2003 as part of its Trustworthy Computing initiative. Announcing such programs affects users' expectations. The initiative likely slowed future market share erosion. Ultimately, Microsoft itself moved to a cloud-first, secure-by-design strategy, thereby matching competitors.

Proving the remaining characterizations for ecosystems and hackers follows similarly. As such, the remaining proofs are in the appendix.

Property 2. The characteristics of the competitive environment for cybersecurity are:

i. $\frac{\partial \Delta_1}{\partial \tau} > 0 \Rightarrow$ p and τ (and their associated pure strategies) are strategic complements from hackers to ecosystem 1.

ii. $\frac{\partial \Delta_1}{\partial \sigma} > 0 \Leftrightarrow \tau > \frac{1}{2}\frac{c_1}{v} \Rightarrow$ Establishes a threshold such that p and σ (and their associated pure strategies) are strategic complements from users to ecosystem 1.

Under fulfilled expectations, $\sigma = s$:

iii. $\frac{dp}{dq} > 0$.

Property 2(i) is the litmus test of the model. As expected, observing or expecting concentrated hacker attention implies the marginal net benefit of defensive intensity increases. Industry practices in this vein in include opaque defense such as suppressing or normalizing error messages and delayed or deferred response. These keep hackers from learning through feedback from raising alarms. Defense-in-depth also qualifies. Versions include the cyber kill chain, zero-trust and MITRE's ATT@CK framework. Port, service, and path randomization also contribute to opaqueness. These practices create a positive feedback loop: hacker aggression justifies raising ecosystem defense.

Alternatively, concentrated hacker attention indicates previously unknown vulnerabilities. Defensive intensity helps find them. Using AI to find zero days in code is an example. Yet strategic complements from hackers to ecosystems reveals nothing about the actual deterrence value of defensive practices, as captured by $\frac{\partial \Delta_H}{\partial p}$ rather than $\frac{\partial \Delta_1}{\partial \tau}$.

Property 2(ii) characterizes defensive intensity as increasing in market share provided the threat (τ) or material loss (v) are sufficiently large to meet threshold $\tau > \frac{1}{2}\frac{c_1}{v}$. In this way, property 2(ii) gets to the heart of the meaning of cybersecurity. For example, in reconsidering cybersecurity from first principles, cybersecurity practitioner **Rick Howard [2023: 39]** develops the following 'ultimate cybersecurity first principle': "Reduce the probability of material impact due to a cyber event over the next three years." In other words, *property 2(ii) sets ecosystems' thresholds for increasing defensive intensity to increase market share*. The meaning of 'material impact' is also quantified as v such that $\tau > \frac{1}{2}\frac{c_1}{v}$.

When this threshold is met, if ecosystem 1 expects more users it has a strong incentive to increase defensive intensity. An ecosystem anticipating greater user adoption has stronger reputational incentives to appear secure. Defensive intensity protects a larger user base, raising its net marginal benefit. Users' selection of ecosystem 1 encourages defensive effort because more users ⇒ larger attack surface ⇒ defensive intensity is justified. User adoption increases returns to defensive intensity

Property 2(iii) is in terms of ecosystem 1's strategy – rather than marginal net benefit – because q is not an argument in ecosystem 1's expected payoff. To link p with q, an assumption is necessary regarding their relationship in the system. Fulfilled expectations do not introduce additional information asymmetry between players. By contrast, alternatives to fulfilled expectations require assuming at least one player is less informed about the relationship between s and σ than the other players. Since the assumption is used to characterize ecosystem 1, the less informed party would have to be ecosystem 1, which is unlikely given users and hackers are decentralized. Finally, treating the difference between $\frac{dp}{dq}$ versus $\frac{\partial \Delta_1}{\partial q}$ as inconsequential requires (i) that players' beliefs about the relationship between s and σ are correct, which holds by assumption; and (ii) $\frac{dp}{dq}$ is positive, which it is. In this case $\frac{dp}{dq}$ and $\frac{\partial \Delta_1}{\partial q}$ have the same sign, indicating feedback effects between p and q are reinforcing rather than countervailing.

Consequently, if one ecosystem increases defensive intensity, so will the other. For managers, intensity moves in tandem. The market does not bifurcate into a highly secure ecosystem and a less secure ecosystem. Managers must be cognizant of and match changes in competitors' cybersecurity because rapid change is a hallmark of strategic complements.

August et al. [2014] observe sheltering in the cloud leads to less cybersecurity risk as compared to maintaining on-site cybersecurity, but more cybersecurity risk from hackers targeting a particular cloud solution and conjecture sheltering may result in less overall risk. Strategic complements, $\frac{\partial \Delta_1}{\partial \tau} > 0$, explain the rationale for taking refuge in the cloud and property 3 characterizes the collective risk, $\frac{\partial \Delta_H}{\partial \sigma}$.

Property 3. The characteristics of the strategic environment for hackers are:

i. $\frac{\partial \Delta_H}{\partial \sigma} \lesseqgtr 0 \Leftrightarrow v - k_1 - 2vp \lesseqgtr -(\omega - k_2 + 2\omega q)$.

ii. $\frac{\partial \Delta_H}{\partial p} < 0 \Rightarrow \tau$ *and* p (*and their associated pure strategies*) are *strategic substitutes from ecosystem 1 to hackers*.

The inability to sign $\frac{\partial \Delta_H}{\partial \sigma}$ a priori is due to the following dichotomy. By property 2(ii), larger relative size rewards defensive intensity: $\frac{\partial \Delta_1}{\partial \sigma} > 0$. Hence, if hackers incorporate this into their beliefs, size deters hacking, $\frac{\partial \Delta_H}{\partial \sigma} < 0$. In contradistinction, $\frac{\partial \Delta_H}{\partial \sigma} > 0$ is the *Sutton Effect*, named after infamous bank robber Willy Sutton, who claimed he robbed banks because, "that is where the money is." For example, larger relative size is commensurate with a greater attack surface. The dichotomy explains why market share matters for hackers even though market share is not a primitive in hackers' payoffs in Figure 1.

Surveying the empirical literature leaves little doubt the evidence supports the Sutton Effect. That is, τ *and* σ (*and their associated pure strategies*) are *strategic complements from users to hackers*, $\frac{\partial \Delta_H}{\partial \sigma} > 0$. Indeed, we cannot find evidence to the contrary. For example, **Vasek, Wadleigh, and Moore [2016]** find market share is a positive risk factor for content

management webserver compromise. In examining firm-level risk within 12 different industries, **Alan, Karagozoglu, and Zhou [2021]** find large and well-known firms are more likely to be attacked. **Florakis et al. [2023]** find a positive association between their measure of cyber risk and the logarithm of firm size. **Gandal et al. [2023]** find high revenue firms are more frequently targeted compared to medium and low revenue firms in the same industry. **Chang et al. [2024]** find large and publicly-traded U.S. institutions are more likely to be attacked. **Jiang et al. [2024]** find firm size is a particularly important predictor of the likelihood of future cybersecurity attacks.

Overall, in their review of empirical studies of cybersecurity risk and data breaches across 12 disciplines, **Liu and Babar [2026]** find market prominence and firm visibility are predictors of breach likelihood. **Leverett et al. [2020]** take this a step further, empirically showing the power law relationship fitted to ransomware demands has nothing to do with the technical elements of the ransomware and everything to do with Sutton's Law. Ransomware demands are driven by the concentrated financial wealth in terms of big firms, large cities, and giant organizations.

The Sutton Effect implies hackers infer greater value (e.g., greater data density) from an increasing user base and rationally allocate more attention to the associated ecosystem. Simply put, market share matters – even though it is not an argument in hacker's payoffs – because it allows hackers to operate at scale. This is the essence of Sutton's famous quote. The Sutton Effect implies high cybersecurity claims by ecosystems with low market share must be taken with a grain of salt. Such systems may not attract hackers due to low market share making them economically uninteresting to hackers, who devote costly resources to attack an ecosystem. Hence, hackers target ecosystems where they can spread TTP

development costs over scale/market share. Indeed, Microsoft's hegemony through the mid-2000's made it the hacker's target of choice **Berghel [2003].**

Strategic complements or substitutes are often symmetric. This is the case when competition is on the same playing field between members of a single population. Examples of competition on the same strategy include quality or R&D contests. The analysis here is much more heterogeneous. Ecosystems compete for users via cybersecurity. Under Moore's law, users are in co-opetition, with payoffs also depending on the actions of ecosystems and hackers. Hacker-ecosystem and hacker-user interactions are adversarial.

Strategic complements and substitutes characterize the directions of marginal incentives, not equilibrium correlations. Asymmetry in signs $\left(\text{sign } \frac{\partial \Delta_i}{\partial x_i} \neq \text{sign } \frac{\partial \Delta_j}{\partial x_i}\right)$ is both admissible and managerially meaningful. To this end, property 3 establishes two forms of asymmetry with respect to market structure and hacker targeting. First, $\frac{d\Delta_{U_1}}{d\tau} < 0$ implies ecosystem 1's expected market share, σ, decreases with hacker targeting, τ. In contradistinction, the Sutton Effect, $\frac{d\Delta_H}{d\sigma} > 0$, implies hacker's targeting of ecosystem 1, τ, increases with ecosystem 1's market share, σ. Second, $\frac{\partial \Delta_1}{\partial \tau} > 0$ implies ecosystem 1 increases defensive intensity in response to increasing targeting. Fortunately, $\frac{\partial \Delta_H}{\partial p} < 0$ (property 3(ii)) suggests defensive intensity works as intended. At the same time, however, defensive intensity increases market share, which increases targeting.

6.1 Implications of the Model as a Complex System

Taken as a whole, the unified game embodies the following complex system:

- Hacker targeting of ecosystem 1 decreases users' marginal benefit of ecosystem 1 and

increases ecosystem 1's marginal benefit of defensive intensity.

- Ecosystem 1's defensive intensity decreases hackers' marginal benefit of targeting ecosystem 1 and increases users' marginal benefit of ecosystem 1.
- Users' selection of ecosystem 1 increases hackers' marginal benefit of targeting ecosystem 1 and increases ecosystems 1's marginal benefit of defensive intensity.

Consequently, *defensive intensity both deters and creates incentives for hacking*. This is a system-level phenomenon that does not exist in separate intrusion-detection or equilibrium-selection cybersecurity games. Its existence provides an (own-side) network externalities counterpart to **Arce's [2020]** proof that there is no technical cybersecurity solution for two-sided platforms exhibiting cross-side externalities. In so doing, it provides a theoretical underpinning of **[Shapiro's 2023: 285]** critique of engineering 'solutionism': "Cybersecurity is not a primarily technological problem that requires a primarily engineering solution. It is a human problem that requires an understanding of human behavior."

This system complexity also raises the open question of whether $\frac{\partial \Delta_{U_1}}{\partial p} > 0$ together with $\frac{\partial \Delta_H}{\partial \sigma} > 0$ dominate, or $\frac{\partial \Delta_H}{\partial p} < 0$ dominates. Indeed, when $\frac{\partial \Delta_{U_1}}{\partial p} > 0$ together with $\frac{\partial \Delta_H}{\partial \sigma} > 0$ dominate, one may counterintuitively observe $\frac{\partial \Delta_H}{\partial p} > 0$. For example, **Sen and Borle [2016]** find such an observation is consistent with industry evidence of suboptimal mixes of security controls within complex organizations. Moreover, security controls themselves may introduce vulnerabilities or increase the attack surface. In addition, **Wolff [2016]** applies **Merton's [1932]** theory of unintended consequences and the "duality of technology" (that technologies simultaneously enable and constrain) to case studies indicating more need not be better when it comes to defensive intensity. Wolff finds technical security controls have both intended local

effects (e.g., $\frac{\partial \Delta_H}{\partial p} < 0$) and unintended systemic effects (e.g., observing $\frac{\partial \Delta_H}{\partial p} > 0$) owing to complexity and interaction effects.

The present analysis adds ecosystem characteristics to the mix through the interaction between $\frac{\partial \Delta_{U_1}}{\partial p} > 0$ and $\frac{\partial \Delta_H}{\partial \sigma} > 0$. Hence, the Sutton Effect is a necessary condition for the network externalities version of the Wolff Effect. In addition, security is the gateway to the own-side network effects an ecosystem seeks to defend. Such security enables users and constrains hackers. Yet network effects also enable hackers to operate at scale. **Wolf [2006]** additionally emphasizes the importance of keeping security as secret as possible, consistent with the present focus on defensive opacity-cum-mixtures.

7. Application: The AI Shock

Artificial intelligence is revolutionizing information technology. Cybersecurity is no exception. AI affects cybersecurity along at least three dimensions. First, the attack surface increases with AI use. Examples include indirect prompt injection, cross-domain attacks, insecure vibe-coding, and jailbreaking.

The focus here is on the other two dimensions: AI-assisted attack and defense. The first-order effects of both dimensions are increases in scale, speed, and automation **[Agrawal et al 2018, Lohn 2026]**. AI facilitates zero-day testing at scale, thereby bolstering both attack and defense. Within the context of the present model, AI collapses the costs of defensive intensity, c_1 and c_2, and hacking, k_1 and k_2. Indeed, the decrease in k_1 reflects the current reality of the impact of AI as one of old attacks, new amplifiers. For example, AI-generated phishing is more plausible. As of this writing, there is only one confirmed case of a

large-scale AI agent attack with limited human input.[6]

To derive monotone comparative statics for $i \in$ {ecosystem 1, ecosystem 2, users, hackers} with respect to parameter values c_1, c_2, k_1, and k_2, marginal payoff difference function Δ_i must be a function of c_1, c_2, k_1, or k_2. As Δ_U is not a function of any of these parameters, *the direct effect of AI on cybersecurity attack and defense on users' ecosystem selection* (*ecosystem market share*) *cannot be determined*. Indirect effects on σ through the effects of AI on p and τ remain, with characterizations given below.

Property 4. Given AI decreases both the cost of ecosystem 1's defense, c_1, and for attacking ecosystem 1, k_1, its effects are as follows:

i. $\frac{\partial \Delta_1}{\partial c_1} < 0 \Rightarrow$ as c_1 decreases, ecosystem 1 increases defensive intensity, p.

ii. $\frac{\partial \Delta_H}{\partial k_1} < 0 \Rightarrow$ as k_1 decreases, the hacker population distribution, τ, reallocates toward ecosystem 1.

Within a decision-theoretic setting **[Lohn 2025]** finds AI produces greater economies of scale for defenders with AI augmented defense-in-depth versus AI-enable attacks. Hence, AI works asymmetrically in favor of defenders. Such comparisons of magnitude are not possible under monotone comparative statics because the meaning of larger support is not comparable across different probability distributions (mixtures) over different variables (e.g., p versus τ).

As AI decreases both c_1 and k_1, property 4 predicts direct increases in the incentives for ecosystem 1 to increase defensive intensity and hackers to target ecosystem 1. Matching or

[6] A Claude-based agent conducted an espionage campaign across roughly 30 entities in September 2025.

exceeding the rival's action becomes more attractive at the margin. No dynamic instability is implied. Instead, the likelihood of adversarial interaction rises due to mutually reinforcing defensive and offensive responses. Consequently, the assertion of "no coding solution" is both more coherent and predictable.

8. Variations on the Theme

This section addresses payoff variations of the benchmark model as tests of robustness. In particular, the three following phenomena arise. First, monitoring is no longer tantamount to detection. Instead, monitoring is imperfect. AI figures within this context as well. Second, users no longer experience a total loss in network effects during a breach. The ecosystem exhibits resiliency in the sense of Netflix's approach to chaos engineering **[Rosenthal & Jones 2020]**. Third, hackers may learn something when attacking an ecosystem with low market share.

8.1 *Variation 1*: *Imperfect Monitoring*

Consider the case where monitoring is imperfect. That is, monitoring has detection rate $\alpha_i \in (0,1)$ for ecosystem $i = 1, 2$. In this case, when hackers target a monitoring ecosystem 1, ecosystem 1's expected payoff is $\alpha_1 v - (1 - \alpha_1)v - c_1 = (2\alpha_1 - 1)v - c_1$. In the benchmark game $\alpha_1 = 1$ and ecosystem 1's payoff is $v - c_1$ instead. Ecosystem 2's expected payoff is $(2\alpha_2 - 1)\omega - c_2$ when imperfectly monitoring an attack. Under imperfect monitoring, hackers targeting a monitoring ecosystem 1 have an expected payoff of $-\alpha_1 v + (1 - \alpha_1)v - k_1 = -(2\alpha_1 - 1)v - k_1$; and the expected payoff for those targeting ecosystem 2 is $-(2\alpha_2 - 1)\omega - k_2$. Hence, for Figure 1 the payoff vector in northwest cell of G_1 becomes

$[(2\alpha_1 - 1)v - c_1, -(2\alpha_1 - 1) - k_1, s]$ instead of $[v - c_1, -v - k_1, s]$. Similarly, the payoff vector in the northeast cell of G_2 becomes $[(2\alpha_2 - 1)\omega - c_2\ , -(2\alpha_2 - 1)\omega - k_2\ , 1 - s]$ instead of $[\omega - c_2, -w - k_2, 1 - s]$. No other payoff vectors change. Furthermore, users' payoffs do not change because their payoffs are not functions of the $\alpha's$. An alternative variation affecting users arises below.

Strategies are mixed if each ecosystem prefers to monitor an attacking hacker: $\alpha_1 > \frac{c_1}{2v}$ and $\alpha_2 > \frac{c_2}{2\omega}$. Hence, the cost of monitoring must be low enough or the value of what is at stake material enough to justify imperfect monitoring. Understandably, they hold for prior (one defender) imperfect monitoring analyses in the intrusion detection literature **[Chen and Leneutre 2009, Liu, Comaniciu and Man 2006, Otrok et al. 2009, Rass and Zhu 2016].** Consequently, the conditions continue to hold for this variation of the unified game.

As the Δ_i's are defined in terms of relative expected payoffs, and only the payoffs for ecosystems and hackers change, only the signs of their Δ_i's potentially change. All other properties remain intact.

Property 2′. In the presence of imperfect monitoring

i. $\frac{\partial \Delta_1'}{\partial \tau} > 0 \Rightarrow$ The marginal value of defensive intensity again increases with targeting.

ii. $\frac{\partial \Delta_1'}{\partial \sigma} > 0 \Leftrightarrow \tau > \frac{1}{2}\frac{c_1}{\alpha_1 v} \Rightarrow$ Higher threshold for raising defensive intensity when market share increases.

iii. $\frac{\partial \Delta_1'}{\partial \alpha_1} > 0 \Rightarrow$ Defensive intensity increases with accuracy.

With the advent of AI-assisted defense, the difference between monitoring and detecting is likely to decrease, $\alpha_1 \to 1$, making imperfect monitoring less of a concern. On the

other hand, the only way to justify inaccurate intensity, $\alpha_1 \to 0$, is in the presence of a larger threat or material loss: $\tau > \frac{1}{2}\frac{c_1}{\alpha_1 v}$. From property 2(ii), the benchmark threshold for increasing defensive intensity in response to increasing market share is $\tau > \frac{1}{2}\frac{c_1}{v}$. As $\alpha_1 \in (0,1)$, $\frac{1}{2}\frac{c_1}{\alpha_1 v} > \frac{1}{2}\frac{c_1}{v}$. The threshold is higher under imperfect monitoring.

Property 3′. In the presence of imperfect monitoring

i. The conditions for the Sutton Effect, $\frac{\partial \Delta_H'}{\partial \sigma} > 0$, are less restrictive.

ii. $\frac{\partial \Delta_H'}{\partial p} < 0 \Rightarrow$ τ and p (and their associated pure strategies) are again strategic substitutes from ecosystem 1 to hackers.

iii. $\frac{\partial \Delta_H'}{\partial \alpha_1} < 0 \Rightarrow$ The greater ecosystem 1's divergence between monitoring and detecting is, the greater are hackers' marginal incentives to target ecosystem 1.

As the Sutton Effect is necessary for the Wolff Effect, property 3′(i) implies greater potential for the Wolff Effect. Property 3′(iii) provides a rationale for AI-assisted defense having nothing to do with users' scale or the scale effects of AI. To the degree AI-assisted defense closes the gap between monitoring and detection, it serves as a deterrent.

8.2 Variation 2: Partial User Losses in the Event of a Breach

The game in Figure 1 assumes a total loss for users in the case of an unmonitored attack. In practice, attacks often result in partial losses or temporary disruption, rather than a complete nullification of value. The total loss assumption is prevalent in extant inspection game models. Alternative cybersecurity games with partial losses include **Arce [2020], Garcia et al. [2014],** and **Geer, Jardin, and Leverette [2020]**.

Consider the case where in an unmonitored attack, users retain proportion $\rho_i \in (0,1)$ of ecosystem's $i = 1, 2$ network benefits and lose proportion $1 - \rho_i$. Then ρ_i measures the resilience of ecosystem i and $1 - \rho_i$ measures the degree of material losses under a successful attack. Alternatively, ρ_i represents heterogeneity in the impact of an attack (proportion of users, regions, or specific services). Then ρ_i is the proportion of users in the ecosystem left intact and $1 - \rho_i$ the proportion of affected users.

The payoff for users in the southwest cell of G_1 of Figure 1 becomes $\rho_1 s$. Similarly, the payoff for users in the southeast cell of G_2 in Figure 1 becomes $\rho_2(1 - s)$. Hence, only characterizations of Δ_U potentially change.

Property 1′′. Under partial user losses in the event of a breach

i. $\frac{\partial \Delta_{U_1}''}{\partial p} > 0 \Rightarrow \sigma$ and p (and their associated pure strategies) are again strategic complements from ecosystem 1 to users.

ii. $\frac{\partial \Delta_{U_1}''}{\partial q} < 0 \Rightarrow \sigma$ and q (and their associated pure strategies) are again strategic substitutes from ecosystem 1 to users.

iii. $\frac{\partial \Delta_{U_1}''}{\partial \tau} \gtreqless 0 \Leftrightarrow \frac{(1-q)(1-\rho_2)}{(1-p)(1-\rho_1)} \gtreqless \frac{s}{1-s}$

iv. $\frac{\partial \Delta_{U_1}''}{\partial \rho_1} = s(1-p)\tau > 0.$

Property 1′′(iv) implies *user market share is increasing in resiliency*. The left-hand side of the second inequality of (iii) is increasing in ecosystem 1's resiliency. For a given relative market share, $s/(1 - s)$, *resiliency implies users may stay with an ecosystem even under increasing attacks*. For managers, *resiliency serves to maintain market share even in the face of breaches*.

8.3 Variation 3: Value of Attacking Low Market Share Ecosystems

In the benchmark game, if hackers target an ecosystem users do not choose, the hacker payoff is normalized to zero. In practice, targeting a low share ecosystem can still yield data or footholds that matter. In such instances, hackers may learn something, ℓ_i, about target $i = 1,2$; where $\ell_1 < v, \ell_2 < \omega$. Hackers' payoffs are now $\ell_2 - k_2$ in the northeast and southeast cells of G_1 and $\ell_1 - k_1$ in the northwest and southwest cells of G_2. The change in hackers' payoffs potentially affects Δ_H.

Property 3‴. With a nonzero payoff for targeting ecosystems with low market share

i. If $\ell_1 > k_1$ the conditions for the Sutton Effect, $\frac{\partial \Delta_H'''}{\partial \sigma} > 0$, are less restrictive.

ii. $\frac{\partial \Delta_H'''}{\partial p} < 0 \Rightarrow$ τ and p (and their associated pure strategies) are again strategic substitutes from ecosystem 1 to hackers.

iii. $\frac{\partial \Delta_H'''}{\partial \ell_1} \lessgtr 0 \Leftrightarrow \sigma \lessgtr ½$.

Once again, with looser conditions for the Sutton Effect there is greater potential for the Wolff effect. Term ℓ_1 establishes $\ell_1 - k_1$ as the floor for targeting ecosystem 1. When this floor is positive, $\ell_1 > k_1$, hackers receive a greater marginal return for targeting ecosystem 1 (property 3‴(i)). This is reinforced when hackers believe $\sigma > ½$ (property 3‴(iii)).

9. Conclusion

This paper unifies two previously distinct frameworks: intrusion-detection and ecosystem-selection cybersecurity games, to explore how cybersecurity and market share interact in

environments characterized by network externalities. By modeling the strategic behavior of users, hackers, and defenders (ecosystems), we uncover nuanced relationships challenging conventional wisdom about cybersecurity and market dynamics.

These relationships are characterized by using monotone comparative statics. Like AI, monotone comparative statics make predictions. In addition, monotone comparative statics guide strategic responses. The characterizations point to the direction of managerial responses to changes in competitors' cybersecurity; allows managers to anticipate competitors' responses when managers change their own security; and predict both users' behavior and hackers' reactions. We link these insights to contemporary practices such as defensive opacity, defense-in-depth, and AI-enabled security operations.

Our findings reveal cybersecurity levels across competing ecosystems are strategic complements, moving in tandem rather than diverging. This interdependence implies security competition is a rapidly changing landscape where managers must be cognizant of competitors' changes in security practice. Otherwise, managers risk losing market share. As such, ecosystems converge toward similar levels of defensive intensity, shaped by mutual strategic incentives. Multifactor authentication is an example.

Paradoxically, increased defensive intensity both boosts an ecosystem's market share and attracts attacks. This underscores the limits of purely technical cybersecurity solutions and highlights the need for strategic, posture-aware cybersecurity policies recognizing economic incentives, especially in ecosystems where user participation amplifies value. For example, the result motivates further research on governance.

Strategically, managers must recognize optimal defensive intensity depends not only on internal risk assessments but also on external factors such as attacker behavior,

competitor actions, and market positioning. Increasing defensive intensity can inadvertently increase visibility to attackers, while standing still can erode user trust and market share.

In sum, the interplay between market share, user behavior, and cybersecurity reveals a complex landscape where more security is not always better, and strategic alignment across stakeholders is essential. Future research should explore how nontechnical interventions – such as user education, policy design, and behavioral incentives – complement technical defenses to augment coding solutions.

11. Appendix: proofs

Property 2: From Figure 1, $E_1[M] - E_1[N] = \sigma\{v - c_1\} - \sigma\{(1-2\tau)v\}$

$$\Delta_1 = E_1[M] - E_N[N] = \sigma\{2v\tau - c_1\}$$

Yielding $\frac{\partial \Delta_1}{\partial \tau} = 2v\sigma > 0$. Also, $\frac{\partial \Delta_1}{\partial \sigma} = 2v\sigma - c_1 > 0 \Leftrightarrow \tau > \frac{1}{2}\frac{c_1}{v}$.

From equation (1)

$$\Delta_{U_1} = s\{1 + q + (p-q)\tau\} - [q + (1-q)\tau]$$

Fulfilled expectations create implicit function

$$F(p, q, \sigma, \tau) = \sigma\{1 + q + (p-q)\tau\} - [q + (1-q)\tau]$$

By the implicit function theorem

$$\frac{dp}{dq} = -\frac{F_q}{F_p} = -\frac{(1-\tau)(\sigma-1)}{\sigma\tau} = \frac{(1-\tau)(1-\sigma)}{\sigma\tau} > 0. \blacksquare$$

Property 3: From Figure 1, $\Delta_H = E_H[1] - E_H[2] = \sigma[v - k_1 - 2vp] - (1-\sigma)[\omega - k_2 - 2\omega q]$.

$$\frac{\partial \Delta_H}{\partial \sigma} \lesseqgtr 0 \Leftrightarrow v - k_1 - 2vp \lesseqgtr -(\omega - k_2 + 2\omega q) \qquad (A1)$$

Also, $\frac{\partial \Delta_H}{\partial p} = -2\sigma v < 0. \blacksquare$

Property 4: Given $\Delta_1 = \sigma\{2v\tau - c_1\}$, $\frac{\partial \Delta_1}{\partial c_1} = -\sigma < 0$. Given $\Delta_H = \sigma[v - k_1 - 2vp] -$

$(1-\sigma)[\omega - k_2 - 2\omega q]$, $\frac{\partial \Delta_H}{\partial k_1} = -\sigma < 0. \blacksquare$

Property 1′: Given the change in payoffs, for users $\Delta_1' = E_1[M] - E_1[N]$ becomes

$$\sigma\{\tau[(2\alpha_1 - 1)v - c_1] + (1-\tau)[v - c_1]\} - \sigma\{\tau[-v] + (1-\tau)[v]\}$$

Yielding $\Delta_1' = \sigma\{2\alpha_1\tau v - c_1\}$ with $\frac{\partial \Delta_1'}{\partial \tau} = 2\alpha_1 v\sigma > 0$. Also, $\frac{\partial \Delta_1'}{\partial \sigma} > 0 \Leftrightarrow \tau > \frac{1}{2}\frac{c_1}{\alpha_1 v}$.

Finally, $\frac{\partial \Delta_1'}{\partial \alpha_1} = 2v\sigma\tau > 0. \blacksquare$

Property 3′: Given the change in payoffs, for hackers $E_H[1] - E_H[2]$ becomes

$$\sigma\{[-(2\alpha_1 - 1)v - k_1]p + [v - k_1](1 - p)\}$$
$$-(1 - \sigma)\{[-(2\alpha_2 - 1)w - k_2]q + [w - k_2](1 - q)\}$$

Yielding $\Delta'_H = = \sigma[v - k_1 - 2v\alpha_1 p + \omega - k_2 - 2\omega\alpha_2 q] - [\omega - k_2 - 2\omega\alpha_2 q]$ with

$$\frac{\partial \Delta_H}{\partial \sigma} \lessgtr 0 \Leftrightarrow (1 - \alpha_1 p)v - k_1 + (1 - \alpha_2 q)\omega - k_2 \lessgtr v\alpha_1 p + v\alpha_2 q$$

If $\alpha_1, \alpha_2 \to 1$ the original conditions for the Sutton Effect from (A1) return. They are easier to meet relative to equation (A1) under imperfect monitoring. For example, in the extreme, $\alpha_1, \alpha_2 \to 0$ yields $\frac{\partial \Delta_H}{\partial \sigma} \lessgtr 0 \Leftrightarrow v - k_1 + \omega - k_2 \lessgtr 0$. As $v > k_1, \omega > k_2, \frac{\partial \Delta_H}{\partial \sigma} > 0$. Also, $\frac{d\Delta_H}{dp} = -2v\alpha_1 < 0$. ■

Property 1′′: Given the change in payoffs, for users $E_U[1] - E_U[2]$ becomes

$$s\{p\tau + p(1 - \tau) + \rho_1(1 - p)\tau + (1 - p)(1 - \tau)\}$$
$$-\ (1 - s)\{q\tau + q(1 - \tau) + (1 - q)\tau + \rho_2(1 - q)(1 - \tau)\}$$

$$\Delta''_{U_1} = E_U[1] - E_U[2] = \ s[1 - (1 - p)(1 - \rho_1)\tau] - (1 - s)[1 - (1 - q)(1 - \rho_2)(1 - \tau)]$$

$$\frac{\partial \Delta''_{U_1}}{\partial p} = s(1 - \rho_1)\tau > 0$$

$$\frac{\partial \Delta''_{U_1}}{\partial q} = -(1 - s)(1 - \rho_2)(1 - \tau) < 0$$

$$\frac{\partial \Delta''_{U_1}}{\partial \tau} = (1 - s)(1 - q)(1 - \rho_2) - s(1 - p)(1 - \rho_1)$$

$$\Rightarrow \frac{\partial \Delta''_{U_1}}{\partial \tau} \gtrless 0 \Leftrightarrow \frac{(1 - q)(1 - \rho_2)}{(1 - p)(1 - \rho_1)} \gtrless \frac{s}{1 - s}$$

$$\frac{\partial \Delta''_{U_1}}{\partial \rho_1} = s(1 - p)\tau > 0. \blacksquare$$

Property 3′′′: Given the change in payoffs, for hackers $\Delta_H'''= E_H[1] - E_H[2]$

$$= \sigma\{[-v - k_1]p + [v - k_1](1 - p) + \ell_1 - k_1\}$$

$$- (1 - \sigma)\{[-\omega - k_2]q + [\omega - k_2](1 - q) + \ell_1 - k_1\}$$

$$\Delta_H'''= \sigma\{[1 - 2p]v - k_1 + [1 - 2q]\omega - k_2 + 2(\ell_1 - k_1)\} - \{[1 - 2q]\omega - k_2 + \ell_1 - k_1\}$$

$$\frac{\partial \Delta_H'''}{\partial \sigma} \gtreqless 0 \Leftrightarrow (1 - p)v - k_1 + (1 - q)\omega - k_2 + 2(\ell_1 - k_1) \gtreqless vp + vq$$

The $2(\ell_1 - k_1)$ term is not in equation (A1). If $\ell_1 > k_1$ the constraint for the Sutton Effect slackens relative to (A1). Also, $\frac{\partial \Delta_H'''}{\partial p} = -2v\sigma < 0$ and $\frac{\partial \Delta_H'''}{\partial \ell_1} = 2\sigma - 1$. ■

12. References

Agrawal, A., Gans, J., and Goldfarb, A. 2018 *Prediction Machines*. *The Simple Economics of Artificial Intelligence*. Boston: Harvard Business Review Press.

Alan, N.S., Karagozoglu, A.K., and Zhou, K. 2021 Firm-level cybersecurity risk and idiosyncratic volatility. *Journal of Portfolio Management*, 47(9), 110-140.

Andreozzi, L. 2004. Rewarding policemen increases crime. Another surprising result from the inspection game. *Public Choice*, 121(1), 69-86.

Arce, D. 2018. Malware and market share. *Journal of Cybersecurity*, 4, 1-6.

Arce, D. 2020. Cybersecurity and platform competition in the cloud. *Computers & Security*, 93, 1-8.

August, T., Niculescu, M.F., and Shin, H. 2014. Cloud implications on software network structure and security risks. *Information Systems Research*, 25(3), 489-510.

Aumann, R.J. 1987. Correlated equilibrium as an expression of Bayesian rationality. *Econometrica*, 55, 1-18.

Bakos, Y. and Katsamakas, E. 2008. Design and ownership of two-sided networks: Implications for Internet platforms. *Journal of Management Information Systems*, 25(2), 171-202.

Berghel, H. Malware month. 2003. *Communications of the ACM*, 46(12), 15-19.

Barua, A., Kriebel, C.H., and Mukhopadhyay, T. 1991. An economic analysis of strategic information technology investments. *MIS Quarterly*, 15(3), 313-331.

Bulow, J., Geanakoplos, J., and Klemperer, P. 1985. Multimarket oligopoly: Strategic substitutes and complements. *Journal of Political Economy*, 93(3), 488-511.

Chanbe, J.-W., Jarachandran, K., Ramirez, C.A., and Tintera, A. 2024. On the anatomy of

cyberattacks. *Economics Letters*, *238*, 111676.

Chen, L. and Leneutre, J. 2009. A game theoretical framework on intrusion detection in heterogenous networks. *IEEE Transactions on Information Forensics and Security*, 4(2), 165-178.

Clement, N. and Arce, D. 2025. Dynamics of shared security in the cloud. *Information Systems Research*, 36(2), 916-943.

Collins, B., Xu, S., and Brown, P.N. 2025. Game-theoretic cybersecurity: The good, the bad, and the ugly. *arXiv*.

Cornell, B. and Roll, R. 1981. Strategies for pairwise competition in markets and organizations. *Bell Journal of Economics*, 12(1), 201-213.

Courtney, R.J. Jr. 1982. A systematic approach to data security. *Computers & Security*, 1(2), 99-112.

Coniglio, S., Gatti, N., and Marchesi, A. 2020. Computing pessimistic Stackelberg equilibrium with multiple followers: The mixed-pure case. *Algorithmica*, 82(5), 1189-1238.

Echenique, F. 2003. Mixed equilibria in games of strategic complementarities. *Economic Theory*, 22(1), 33-44

Florakis, C., Louce, C., Michaely, R., and Weber, M. 2023. Cybersecurity risk. *Review of Financial Studies*, 36, 351-407.

Fudenberg, D. and Tirole, T. 1992. *Game Theory*. Cambridge: MA: MIT Press.

Gandal, N. 1994. Hedonic price indices for spreadsheets and an empirical test for network externalities. *RAND Journal of Economics*, 25(1), 160-170.

Gandal, N., Moore, T., Riordan, M., and Barnir, N. 2023. Empirically Validating the Effect of Security Precautions on Cyber Incidents. *Computers & Security*, 133, 103380.

Garcia, A., Sun, Y., and Shen, J. 2014. Dynamic platform competition with malicious users. *Dynamic Games and Applications*, 4(3), 290-308.

Geer, D., Bace, R., Gutmann, P., Metzger, P., et al. 2007. Cyber insecurity: The cost of monopoly. totse.com.

Geer, D., Jardine, E., and Leverett, É. 2020. On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 5(1), 9-29.

Gianini, G., Damiani, E., Mayer, T.R., et al. 2013. Many-player inspection games in networked environments. *7th IEEE International Conference on Digital Ecosystems and Technologies – DEST*. Menlo Park, CA: IEEE, pp.1-6.

Hardin, G. The tragedy of the commons. 1968. *Science*, 162(3865), 1243-1248.

Howard, R. 2023. *Cybersecurity First Principles*. Wiley: Hoboken, NJ.

Huang, L. and Zhu, Q. 2023. A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security*, 98, 1-15.

Jacquemin, A. 1987. *The New Industrial Organization*. *Market Forces and Strategic Behavior*. Cambridge, MA: MIT University Press.

Jegers, M. and Van Hove, L. 2020. Malware and market share: A comment on Arce. *Journal of Cybersecurity*, 6(1), tyaa024.

Jiang, H., Khanna, N., Yabg, Q., and Zhou, J. The cyber risk premium. 2024. *Management Science*, 70(12), 8791-8817.

Kiennert, C., Ismail, Z., Debar, H., and Leneutre, J. 2018. A survey on game-theoretic approaches for intrusion detection and response optimization. *ACM Computing Surveys*, 51(5), article 90.

Kreps, D.M. 1977. A note on "fulfilled expectations equilibria." *Journal of Economic Theory*.

14(1), 32-43.

Leverett, É., Jardine, E., Burns, E., et al. 2020. Averages don't characterise the heavy tails of ransoms. *2020 APWG Symposium on Electronic Crime Research* (eCrime). Boston: IEEE, 1-20.

Liu, C. and Babar, M.A. 2026. Corporate cybersecurity risk and data breaches: A systematic review of the empirical research. *Australian Journal of Management*, 51(1), 62-92.

Liu, Y., Comanciu, C., and Man, H. 2006. A Bayesian game approach for intrusion detection in wireless ad hoc networks. *Proceedings from the 2006 Workshop on Game Theory for Communications Networks – GamesNets* '06, New York: ACM, 4 – es.

Lohn. A.J. 2026. Defending against intelligent attackers at large scales. *arXiv*: 2504.18577v1.

Merton, R.K. 1936. The unanticipated consequences of purposeful social action. *American Sociological Review*, 1(6), 894-904.

Metcalfe, R.M. 1995. Metcalfe's Law: A network becomes more valuable as it reaches more users. *InfoWorld*, 40(17), 53.

Metcalfe, R.M. 2013. Metcalfe's Law after 40 years of Ethernet. *IEEE Computer*, 46(12), 26-31.

Milgrom, P. and Roberts, R. 1990. Rationalizability, learning, and equilibrium in games with strategic complementarities. *Econometrica*, 58(6), 1255-1277.

Nash, J. 1950. *Non-Cooperative Games*. Dissertation, Department of Mathematics, Princeton University. In Kuhn, H.W. and Sylvia Nasar, S. (eds.) 2002. *The Essential John Nash*. Princeton University Press: Princeton, pp.53-84.

O'Donnell, A. 2008. When malware attacks (anything but Windows). *IEEE Security & Privacy*, May/June, 68-70.

Ostrom, E. 1990. *Governing the Commons*. NY: Cambridge University Press.

Otrok, H., Zhu, B., Yahyaoui, H., and Bhattacharya, P. 2009. An intrusion detection game

theoretical model. *Information Security Journal: A Global Perspective*, 19(5), 199-212.

Png. I.L. and Wang, Q-H. 2009. Information security: facilitating user precautions vis-à-vis enforcement against attackers. *Journal of Management Information Systems*, 26(2), 97-121.

Rass, S. and Zhu, Q. 2016. GADAPT: A sequential game-theoretic framework for designing defense-in-depth strategies against advanced persistent threats. In Zhu, Q. et al. (eds.) *GameSec* 2016, *LCNS* 9996. Springer International, pp.314-326.

Rohlfs, J. 1974. A theory of interdependent demand for a communication service. *Bell Journal of Economics and Management Science*, 5(1), 16-37.

Rosenthal, C. and Jones, C. 2020. *Chaos Engineering*. *System Resiliency in Practice*. Boston: O'Reily.

Roy, S. and Sabarwal, T. 2012. Characterizing stability properties in games with strategic substitutes. *Games and Economic Behavior*, 75(1), 337-353.

Sen, R. and Borle, S. 2016. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems* 32(2), 314-341.

Sen, R., Verma, A., and Heim, G. R. 2020. Impact of cyberattacks by malicious hackers on the competition in software markets. *Journal of Management Information Systems*, 37(1), 191-216.

Shapiro, S.J. 2023. *Fancy Bear Goes Phishing*. *The Dark History of the Information Age, in Five Extraordinary Hacks*. NY: Farrar, Strauss, and Giroux.

Vasek, M., Wadleigh, J., and Moore, T. 2016. Hacking is not random: A case-control study of webserver-compromise risk. *IEEE Transactions on Dependable and Secure Computing*, 13,(2), 206-219.

Walters, M. 2023. The history of Microsoft Patch Tuesday, https://www.action1.com/blog/history-of-microsoft-patch-tuesday/

Wolff, J. 2016. Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, 33(2), 597-620.

Table1: Ecosystem, Hacker, and User Endogeneity

Game	Hackers	Target/Ecosystem	Users
Intrusion Detection (Inspection)	Endogenous attack probability.	Endogenous probability of intrusion detection.	Selection of ecosystem is outside of scope.
Ecosystem Selection & Defense	Proportion attacking an ecosystem is endogenous	Exogenous probability of intrusion detection.	Proportion selecting an ecosystem is endogenous.
Current	Proportion attacking an ecosystem is endogenous	Endogenous probability of intrusion detection.	Proportion selecting an ecosystem is endogenous.

Table 2: Variables in the Model

Symbol	Definition
$v > 0$	Ecosystem 1's value at stake if breached.
M	Ecosystem 1 monitors for intrusions.
N	Ecosystem 1 does not monitor for intrusions.
$p \in [0,1]$	Probability ecosystem 1 monitors for intrusions. [$1 - p \equiv$ probability ecosystem 1 does not monitor.]
$s \in [0,1]$	Ecosystem (ecosystem) 1's market share of users.
$\omega > 0$	Ecosystem 2's value at stake if breached.
m	Ecosystem 2 monitors for intrusions.
n	Ecosystem 2 does not monitor for intrusions.
$q \in [0,1]$	Probability ecosystem 2 monitors for intrusions. [$1 - q \equiv$ probability ecosystem 2 does not monitor.]
$1 - s$	Ecosystem (ecosystem) 2's market share of users.
$c_i > 0$	Ecosystem i's cost of monitoring for intrusions, i= 1,2.
$\tau \in [0,1]$	Proportion of hacker population attacking (targeting) 1.
$1 - \tau$	Proportion of hacker population attacking (targeting) 2.
$k_i > 0$	Hackers' cost of attacking ecosystem i = 1,2.
$\sigma \in [0,1]$	Proportion of user population selecting ecosystem 1.
$1 - \sigma$	Proportion of user population selecting ecosystem 2.
Δ_i	Relative payoff difference function for player/population $i \in$ {ecosystem 1, ecosystem 2, users, hackers}

Figure 1: Intrusion Detection with Ecosystem Selection

G_1		
Users select 1 σ	**Hackers attack 1** τ	**Hackers attack 2** $1-\tau$
Ecosystem 1 monitors (*M*) p	$v-c_1, -v-k_1, s$	$v-c_1, 0, s$
Ecosystem 1 does not monitor (*N*) $1-p$	$-v, v-k_1, 0$	$v, 0, s$

G_2		
Users select 2 $1-\sigma$	**Hackers attack 1** τ	**Hackers attack 2** $1-\tau$
Ecosystem 2 monitors (*m*) q	$\omega-c_2, 0, 1-s$	$\omega-c_2, -\omega-k_2, 1-s$
Ecosystem 2 does not monitor (*n*) $1-q$	$\omega, 0, 1-s$	$-\omega, \omega-k_2, 0$

Note: Payoffs listed in the order ecosystem (ecosystem 1 in G_1 and ecosystem 2 in G_2), hackers, users.