Dynamics of Shared Security in the Cloud

Nan Clement, Daniel Arce

October 31, 2023

Abstract

Cloud services exist under a shared security environment; both cloud services providers (CSPs) and users contribute to overall security. We investigate the nature of shared security in a dynamic game where users' security contributions and cloud usage figure into their CSP's vulnerability. Furthermore, CSPs' own security contribution takes into account both their users as well as competition with other CSPs. The Markov Perfect Equilibrium reveals the long-term time patterns of security of the cloud. In particular, we identify a novel form of time-path strategic complementary between usage and a CSP's Markov state of security. This implies that cloud security is an unusual form of impure public good whereby individual contributions bolstering a CSP's security endow a selective incentive (private benefit) on others, rather than only providing a selective incentive to the contributors themselves. Since this increases usage, CSP vulnerability increases over time. At the same time, the CSPs' competition with security may lead to a welfare improvement, but the lock-in effect of security on the platforms shapes the CSP's security investment and, eventually, the security results.

1 Introduction

As more businesses move into the cloud, and ransomware becomes a big-game-hunting affair, understanding the dynamic structure of cloud security is necessary for cloud services providers and their users alike. For example, Microsoft presently encourages its business users to take shelter in the cloud, building tools allowing its bread-and-butter products to be used on rival cloud services providers (CSPs) and their associated security solutions (Tilley and McMillan 2022). By contrast, Blumenthal (2011) outlines various ways the cloud might be seen as a "new platform for malice." For example, data centers provide both economies of scale and large targets for malicious actors. Indeed, cloud data breaches cost more and take longer to identify (IBM 2023). On top of this, CSP use introduces a new type of exposure to insider attacks – those with knowledge of the CSP's architecture, configuration attributes, and parameters (Cansever 2020). August, Niculescu, and Shin (2014) describe a middle ground, where Software-as-a-Service (SaaS) poses less undirected cybersecurity risk as compared to its on-site version, but more organizational-level directed cybersecurity risk.[1] Such 'diversification' may result in less overall risk. Our focus is on the CSP-user dynamics of directed risk in order to evaluate the consequences of taking shelter in the cloud.

This focus in part stems from new guidance issued by the Joint Cybersecurity Advisory (CSA) – authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) – where the importance of the cloud is now on par with enterprise environments.[2] CSA also has an accompanying analysis report (AR21-013A) for further cloud security guidance. All

[1] Undirected risk associated with on-site versions stems from malicious actors targeting many individual users in any system running the version. Directed risk stems from malicious actors targeting a particular cloud system version, thereby affecting many organizations at once.

[2] https://www.cisa.gov/news/2022/02/09/cisa-fbi-nsa-and-international-partners-issue-advisory-ransomware-trends-2021

proposed solutions require cloud users to do more to defend their services.[3] Similarly, in the online summit discussing their inaugural Cloud Risk Report (Crowdstrike 2023), Crowdstrike warns, *the cloud is the new attack surface* due to the way the cloud ends up being the platform for securing multiple forms of computing. Palo Alto Networks (2023) takes it a step further, calling the cloud the *dominant attack surface*, owing to findings in its *Unit 42 Attack Surface Threat Report* that 80 percent of medium, high or critical exposures are on assets in the cloud for the organizations analyzed.

The cloud security environment embodies *shared security* (Tianfield 2012, Almorsy, Grundy, and Müller 2016, Al-Otaibi 2021) and *joint responsibility* (Tajalizadehkhoob, Van Goethem, Korczyński, Noroozian, Böhme, Moore, Joosen, and van Eeten 2017) because both CSPs and users contribute to overall security. Throughout our paper, the term *user* refers to a firm with a service level agreement (SLA) with their CSP. Simply put, shared security and joint responsibility involve *security of the cloud*, referring to CSPs' responsibilities toward securing hardware, global infrastructure, virtual machine images within repositories, etc.; versus *security in the cloud*, referring to users' responsibilities for securing their own network, firewall configurations, etc. Misconfigurations at interfaces between user and CSP are often susceptible to exploitation, such as the 2019 Capital One breach on AWS by a former AWS employee. Another example is users leaving CSP's default passwords intact. Users must also ensure they correctly deactivate unused sites in the cloud, otherwise, the sites remain unmaintained and with out-of-date security. Data security is an area of joint responsibility for CSPs and users. In addition, the multi-tenant nature of the cloud implies an interdependent security problem for all users, and lends itself to class breaks (Arce 2020). Many, if not all, of the major CSPs are known to have had critical cross-tenant vulnerabilities, thereby violating cloud isolation (Wiz 2023). Supply chain attacks such as the Solar Winds intrusion allow malicious actors to effectively jump between tenants, as can faulty or malicious code in execution environments like Platform-as-a-Service (PaaS). Multitenancy also facilitates adversaries living off the same cloud as users because the traffic looks similar to CSPs.

We employ a dynamic game to characterize how shared security contributes to a CSP's *security umbrella*. By security umbrella we mean the way a CSP's walled garden encourages users to conduct ever more value-producing activities within the cloud because of their familiarity with operating within the walled garden, and the tools CSPs provide for doing so. An example is a CSP employing homomorphic encryption to protect users' data and allow users to process their data without a key while using various applications.

Dynamic game theory differs from the dynamics associated with repeated games, where the same stage game occurs in each period. Instead, in a given period a CSP's and its users' security contributions, along with users' usage of the CSP to create value, may lead to a different game in the subsequent period. Specifically, such choices lead to different states of security and vulnerability in the Markov sense. Given the general dynamic structure of the game under analysis, the approach does not lend itself to explicitly deriving equilibrium strategies or payoffs unless we make strong assumptions about the underlying payoffs. We do not employ such restrictions; the payoff functions in our game are additively separable but are not linear in past, current, or future states. Consequently, equilibrium strategies and payoffs are not derived; instead, we characterize them in terms of Markov Perfect Equilibrium and the associated Euler equation. In a dynamic game, strategies are linked over time and the Euler equation characterizes the evolution of CSP vulnerability given optimal dynamic behavior by CSPs and their users. The Euler equation is useful for characterizing long-term convergence and patterns in CSP vulnerability. These are timely and important issues, given the economics of the cloud are inherently dynamic.

Specifically, operating in the cloud is a decision to trade fixed costs for variable costs, where the latter are determined over time on a pay-as-you-go basis, thereby providing flexibility for on-demand variations in capacity at a granular level. Trading fixed costs mean users substantially scale back on fixed IT investments and current in-house capacity in order to avoid losses from being over or under IT capacity. Capital expenditures are replaced by operating expenses to better align costs with the dynamics of resource demands. Choosing the cloud is therefore a dynamic strategy for users because cloud usage is meant to bear fruit over time through

[3] One of the proposed solutions is, "Verify all cloud-based virtual machine instances with a public IP do not have open Remote Desktop Protocol (RDP) ports. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall."

continued reliance on cost savings in the cloud. In view of this, cloud users do not cycle between cloud and enterprise environments on a transitory basis; the economics of neither would pay off. Hence, in contrast to a one-time either/or analysis of cloud/enterprise choice, our users are in the cloud and expect to be in the cloud for the foreseeable future.

As such, if the likelihood a user persists in the cloud for the next period is nonzero for every period, then an infinite horizon model is appropriate because neither the user nor the CSP can say with certainty when their relationship will end. In addition, CSPs' profits increase when users increase usage, and users only increase usage if they are convinced about operating under the security umbrella. If usage changes over time the Markovian states of security and vulnerability change as well. Such a modeling approach is consistent with the current reality in which, in any given month, 20 percent of an organization's cloud attack surface is taken offline and replaced with new or updated services (Palo Alto Networks 2023). Again, this rules out a repeated game approach, where the states do not change by definition, in favor of a dynamic game approach, which is the modeling environment we investigate. Moreover, once committed to the cloud, a user's next-best alternative is another CSP. Over time, CSPs are therefore also in the business of keeping their users from switching to another CSP and getting users from other CSPs to switch to them, which is another dynamic facet of our model corresponding to cloud economics.

In particular, the security umbrella produces a form of lock-in different from using security and tamper-resistance to explicitly hinder users' ability to switch CSPs (e.g., Anderson 2001, Lookabaugh and Sicker 2004, Arce 2022). Such lock-in is anti-competitive (Asghari, van Eeten, and Bauer 2016, Opara-Martins, Sahandi, and Tian 2014, 2016), causing users to employ anti-lock-in strategies such as hybrid clouds, cloud management providers or brokers, and regular manual data exportation (Arce 2022). In such scenarios, the CSP works toward lock-in and users against it. By contrast, we study an environment corresponding to a CSP's and its users' contributions to shared security to create a security umbrella enhancing the value proposition for users. This is in the interest of both users and CSPs. Finally, a thriving user or CSP may become a more attractive target for malicious actors.

We derive our findings by exploiting the no-switching criterion used both in analyses of lock-in in IT (e.g., Shapiro and Varian 1998, Varian 2004) and, more recently, in platform economics. Specifically, the no-switching criterion is a means for establishing conditions necessary for non-monopolistic outcomes in platform (or two-sided) markets (e.g., Lee 2014, Arce 2020). From the two-sided markets perspective, cloud services such as infrastructure as a service (IaaS) and Software as a Service (SaaS) are examples of platforms in addition to platform as a service (PaaS). By observation, most platform markets, and certainly the market for CSP services within the cloud stack, are not monopolistic. In our model two CSPs compete by providing a security umbrella they and their users contribute to. The no-switching constraint both places economic pressure on a CSP's security provision and enables the characterization of a non-monopolistic equilibrium outcome where CSPs coexist. In invoking the no-switching criterion we do not deny users switch CSPs – they clearly do. Nevertheless, the no-switching criterion has the dual benefit of formalizing how lock-in occurs owing to user's value-added from the resulting security umbrella, and placing CSPs within a competitive structure where security is costly but economically necessary to reduce the potential for users to switch.

Our analysis yields several novel findings. First, after specifying the model itself, a user's investment in security and that of other users and its CSP are shown to be strategic substitutes. Strategic substitutes is a property of best replies indicating it is optimal for a user to decrease its security investment if other users or its CSP increase theirs. While strategic substitutes is somewhat expected, the way others' security investments directly affect a user's per-period payoff function varies according to the degree a user is locked-in under a CSP's security umbrella. Specifically, if a user is not locked-in, others' security investment increases a user's per-period payoff function (known as plain complements). However, over time a user's per-period payoff can decrease in others' security investments (known as plain substitutes) because security investments build on each other, thereby increasing the potential for a user to be locked-in under the CSP's security umbrella.

Second, future vulnerability affects a user's current-period decisions regarding its security investment and CSP usage. Specifically, without consideration of future vulnerability the components of current-period vulnerability change in terms of more current-period usage and less current-period security investment. Indeed,

our characterization of the equilibrium via an Euler equation shows current-period restraint in recognition of its implication for future vulnerability keeps the time path of cloud vulnerability from exploding. The message for managers of CSP users is decisions regarding both security and usage should account for their relationship with each other and their implications for future vulnerability.

Third, CSP usage increases with the accumulation of security. The direct implication for CSP managers is security is part of the CSP's value proposition, which is based on usage fees. A more subtle but highly consequential implication is security creates previously unidentified selective incentives (private benefits). Specifically, *any* contribution enhancing the security umbrella – a local public good for the CSP and its users – also increases usage, which is a private benefit. It therefore follows that the benefit need not stem only from a user's own contribution to security. In particular, other users' or the CSP's security investment increases a user's private benefit stemming from increased usage. As the extant literature often focuses on the publicness of cybersecurity or its associated externalities, this private benefit has largely gone unacknowledged. Cloud security is therefore an *impure public good*.

Originating with Olson's (1965) seminal treatise, *The Logic of Collection Action*, selective incentives associated with the provision of public goods are known to increase voluntary contributions. Within groups, the public benefit is often called a collective benefit and the selective incentive is a noncollective benefit. For example, lobbying by AARP (a collective benefit for all U.S. retirees) is funded by AARP member contributions, and offering private benefits to contributing members, such as discounted insurance and vacation tours, is a noncollective benefit. A non-monetary example is the "warm glow" an individual may get as a form of private psychic benefit from voluntarily contributing to a public good. The combination of public goods with selective incentives is known as impure public goods or joint products because the process of creating the public good results in both public and private benefits (Buchholz and Sandler 2021). International security alliances are among the most widely-studied examples of impure public goods. The security created for members of the alliance is the public good. The ability of domestic troops to not only defend alliance members but also conduct nonmilitary activities such as disaster relief in the homeland is a selective incentive. Similarly, the presence of selective incentives stemming from contributions to the security umbrella make the environment more conducive to collective action. Yet the resulting increasing usage due to increasing security also increases vulnerability because increasing usage raises the CSP's attractiveness to malicious actors. This distinction between security and vulnerability does not exist in the economic literature on traditional security, but it is part and parcel of cybersecurity at least since Gordon and Loeb (2002).

We analyze the shared provision of cybersecurity within a group of users and their CSP, which competes with another CSP. As such, several contributions to the economics literature on public goods result. To begin, contributions to shared security in the cloud produce the security umbrella, providing a public benefit to CSP and users alike by reducing the probability of a breach. Furthermore, users and CSPs conduct their business under the security umbrella. Such business benefits are private to each entity. Yet the resulting joint products are substantially different from the canonical economic model of selective incentives, where the private benefit is directly linked to one's own contribution and no one else's. Here, lowering the probability of a breach is the public benefit, and the private benefit – generating profit under the security umbrella – is not limited to the contributor. Hence, the private benefit is less selective in terms of accruing to the contributor only, but the analysis remains within the categories of impure public goods and joint products. This is the special nature of the benefits of cybersecurity; it is unlike other forms of product differentiation in that cybersecurity is the public good protecting both the private benefits users receive from using their CSP and the CSP's ability to generate its own private benefits by charging for the usage that creates users' benefits. AWS's stance that security is a major component of the cloud rather than an auxiliary operation (Gariba and Van Der Poll 2017) is consistent with this view.

In addition, the dynamic environment differs from the usual settings for examining impure public goods. In a single-shot setting, players do not base their actions on the past history of playing the game or consider the future implications of their actions on another iteration of the game. In a repeated-game setting the same stage game occurs in each period; hence, by definition, the players' strategies cannot change the Markovian state – the vulnerability of the CSP and its users, and the level of security – over time. By contrast, the

dynamics of our analysis allow for the Markovian state to change, making the model one of dynamic joint products (impure public goods over time). Consequently, players' strategies are both a function of the past history of play and how current decisions influence the future state of play. Private benefits (profits) earned under the security-umbrella-as-public-good change over time as well. The result is a novel form of time-path complementarity between usage and shared security measures. Together, results on the state-space dynamics of security and vulnerability in the cloud, combined with our contribution to the economic theory of public goods, imply cloud security is an atypical form of impure public good, wherein individual contributions to bolster CSP security endow a selective benefit on others, thereby increasing usage but also exacerbating CSP vulnerability over time.

We now turn from the public goods-security nexus to a fourth contribution of the paper: the welfare implications of the shared security paradigm are somewhat startling. Specifically, user lock-in is often viewed negatively. Hence, the idea that a CSP's security umbrella may lead to lock-in is concerning. Indeed, we show users can be locked-in by a less-secure more-vulnerable CSP owing to users' familiarity with the CSP's security umbrella. At the same time, however, the level of security required to lock-in users can exceed the level of security necessary to satisfy users' participation constraint. This is a welfare-improvement for users caused by the lock-in produced by the CSP's contributions to the security umbrella in order to keep users from switching. The reasoning has to do with CSP security competition resulting in strategic complements, a phenomenon we now turn to.

Thus far the contributions of the paper are stated in terms of CSP-user and user-user relationships. As we also consider CSP competition, a fifth contribution is the finding that the level of security of a CSP's competitor, and the level of security necessary for a CSP to continue existing (satisfy the no-switching constraint for its users) are strategic complements. The implication is in each period CSPs change their optimal level of security investment in the same direction. Importantly, CSP security competition is tempered; it is neither a race to the bottom, because security must satisfy the no-switching constraint, nor a war of increasing security levels, because a CSP need only partially increase its security in response to increased security by its competitor owing to user lock-in under its security umbrella.

The analysis proceeds as follows. We survey closely-related research in section 2 and present our model in section 3. Section 4 focuses on the optimal path of accumulated vulnerability stemming from users' optimal CSP usage under the security umbrella. Since the path need not converge to a stationary state, we analyze the path of vulnerability in equilibrium. We further characterize user behavior along the CSP's time path of vulnerability. In so doing we provide a novel characterization of security in the cloud as a form of impure public good. In Section 5 we address whether CSP security competition can improve the situation. We present results setting the requirements on the security umbrella to function as a form of lock-in, how the security umbrella determines the non-monopolistic nature of CSP markets, and creates welfare improvements for users. Section 6 concludes with implications for managers, social planners, regulators, and potential extensions. In total, the message is not only is the cloud a joint security environment, it is a *dynamic* joint security environment.

2 Related Literature

The relationships between CSPs and their users are undeniably complex. This is further complicated by the actions of malicious actors when it comes to cloud security. Consequently, all theoretical analyses of the cloud, including ours, focus a magnifying glass on the facets of interest in order to better understand their contribution to the broader picture. This section reviews related studies our analysis builds upon in order to capture the shared security implications of ongoing competition between CSPs and continuing relationships between CSPs and their users. Furthermore, like ours, these studies of the cloud are expressed in terms of economic relationships rather than in terms of the underlying hardware and software architectures of the cloud.

For example, in August, Niculescu, and Shin (2014) the facet under magnification is the difference between the externality associated with indirect attacks on users within an organization employing patchable on-site software versus the externality associated with directed attacks on organizations subscribing to the SaaS

version. Our study complements their focus on the patching actions of on-site software users by instead examining the security interaction between CSPs and CSP users, consistent with taking shelter in the cloud. Furthermore, their game is dynamic as it is in extensive (multi-stage) form, while the time dimension is static as the game is played but once (single-shot). It is consistent with an either/or decision to use on-site software or its cloud version. By contrast, we study a game in extensive form with a time dynamic meant to capture the continuing relationship between CSP and user, consistent with cloud economics, and additionally consider the possibility users may switch CSPs. Hence, the extensive form played at any point in time varies according to the state variables determined by prior play.

In contrast to the August, Niculescu, and Shin (2014) analysis of on-site versus SaaS versioning within a monopoly setting, Zhang, Nan, and Tan (2020) consider security and customization competition between on-site software and SaaS monopolies. SaaS is less customizable than its on-site competitor and involves a usage fee. These two facets discourage usage in such a way that a high security loss environment leads to lower expected losses for SaaS users as compared a low security loss on-site environment with greater usage. The implication for the on-site vendor is, in low-loss environments, security and customization are substitute inputs, but under high-loss environments they are complementary inputs. Once again, the analysis is in terms of a single-shot extensive form game. It implies a negative security externality only, while the time dynamics under investigation in our analysis additionally allow for both the possibility of switching and for *benefits* (selective incentives) to accrue from continued operation under a CSP's security umbrella. The latter can lead to lock-in, which again is a dynamic phenomenon.

While the competitive environments of August, Niculescu, and Shin (2014) and Zhang, Nan, and Tan (2020) consider a single monopoly producing on-site and cloud versions, or an on-site monopoly competing with a cloud monopoly, two studies consider the role of cybersecurity in determining non-monopolistic outcomes. Arce (2020) subjects security to the same two-sided market disciplinary forces shaping a CSP's pricing structure and other strategies. In particular, security must satisfy (i) no-switching constraints for users, and (ii) CSP incentive compatibility constraints that are functions of the cross-platform distribution of users. Security, or lack thereof, is an influential predictor of users' switching behavior (Wilms, Stieglitz, and Mäller 2018). By comparing the level of security to keep current users from switching with the level of security needed to acquire additional users, Arce (2020) characterizes when a CSP market is imperfectly competitive versus monopolistic. The novelty is the characterization is in terms of security; i.e., a symbiosis exists between CSP market structure and security. The dynamics considered are coalitional (relating to whether users switch or not). There is no time dimension.

By contrast, Sen, Verma, and Heim (2020) consider a coupled pair of differential equations for the market share of competing software vendors. The rate of change of a vendor's market share is increasing in the adoption rate of new users 'birthed' into the market. It is decreasing in the rate of existing users switching to the competition, and increasing in the rate of users switching from the competition, with the propensity to switch given exogenously. Finally, the amount of hacking directed at the vendor restrains market share. Monopoly is possible with or without hacking, but imperfect competition is only possible under the presence of hackers. Hence, rather than viewing hackers as unilaterally bad their presence can foster competition within the software market. Here, competition means vendor coexistence or what Arce (2020) calls an interior solution to the market structure problem. In Sen, Verma, and Heim (2020) there are differences in hacker propensities to target a particular vendor but no competition in terms of costly vendor investment in cybersecurity over time. Our study includes the latter.

More-to-the-point, security-enhancing actions are not part of cloud users' strategy sets in August, Niculescu, and Shin (2014), Arce (2020), Sen, Verma, and Heim (2020), or Zhang, Nan, and Tan (2020). In the present analysis CSPs compete on the basis of security and their respective users take security-enhancing actions, as prescribed by users' and CSPs' shared responsibilities, CSA's security guidance, and Crowdstrike's and Palo Alto's Network's' characterizations of the cloud-as-attack-surface.

Table 1: Notation

	Definition
$s_{cspj,t}$	CSP j's strategy: security investment in period t
$s_{i,t}$	User i's strategy: security investment in period t
α	marginal contribution of the CSP j's security investment
k	Per unit cost from security investment for a user
K	Per unit cost from security investment for the CSP
$y_{i,t}$	User i's strategy: cloud service usage in period t
$b(y_{i,t})$	Non-security related net benefit from using $y_{i,t}$ for a user
$B(y_{i,t})$	subscription profit from user i for the CSP
$S_{j,t}$	State Variable: accumulated security investment on CSP j
$S_{i,t}$	State Variable: accumulated security investment by user i
$S_{cspj,t}$	State Variable: accumulated security investment by CSP j
$V_{j,t}$	State Variable: accumulated vulnerability on CSP j
$p(V_{j,t})$	Probability of a successful attack on user i on CSP j
$\tilde{p}(V_{j,t})$	Probability of a successful attack on CSP j
c	Per unit cost of a successful attack for a user
C	Per unit cost of a successful attack for the CSP
$v_{j,t}$	marginal vulnerability attributed to user i
$1-\delta_S$	Depreciation Speed (decay rate) of past security investment
$1-\delta_V$	Depreciation Speed (decay rate) of past vulnerability
δ	Discount factor for the optimal value function
λ	Per unit switching cost
$u_{i,t}$	User i's per period payoff in period t
$U_{i,t}$	User i's lifetime payoff at the end of period t
$\pi_{j,t}$	CSP j's per period payoff in period t
$\Pi_{j,t}$	CSP j's lifetime payoff at the end of period t

3 The Model

Our focus is on how security-enhancing actions of CSPs and their users create a security umbrella under which users determine whether they stay with their CSP or switch, and the degree they use their chosen CSP. Given users' potential to switch, CSPs compete on the basis of platform benefits and how the security umbrella facilitates continued access to such benefits. Upon choosing a CSP, users determine the extent they do business while using their CSP as a platform. Together, overall security effort and usage determine a CSP's vulnerability; i.e., its appeal to malicious actors based on the security umbrella and level of business activity occurring under it.

Table 1 lists the notation for the variables in our analysis. The model itself is presented and explained below.

3.1 Players

Two CSPs and $N(N = 2n)$ identical cloud service users exist in the market. Initially ($t = 0$), n random users are subscribers of CSP 1, and the other half are subscribers of CSP 2. A duopolistic setting facilitates a competitive environment under which CSPs realize security is not only a technical issue, but affects users' decision to stay with their incumbent CSP or switch. Security is thereby a determinant of CSPs' competitive environment (Arce 2020, Sen, Verma, and Heim 2020). This provides insights for other kinds of CSP markets (e.g., oligopoly) as well.

Table 2: Compete in Security: Security Services by Cloud Service Providers

CSP	Security Services	
Azure	Microsoft Defender for Cloud, Microsoft Sentinel, Azure Key Vault, Azure Monitor logs, Azure Dev/Test Labs, Azure Storage Service Encryption, Azure StorSimple Virtual Array, Client-Side encryption for blobs, Azure Storage shared access signatures, Azure Storage Account Keys, Azure File shares, Azure Storage Analytics, Azure SQL Firewall, Azure SQL Connection Encryption, Azure SQL Always Encrypted, Azure SQL transparent data encryption, Azure SQL Database Auditing, Virtual network rules, Azure role-based access control, Azure Active Directory, Azure Active Directory B2C, Azure Active Directory Domain Services, Azure AD Multi-Factor Authentication, Azure Backup, Azure Site Recovery, Network Security Groups, Azure VPN Gateway, Azure Application Gateway, Web application firewall, Azure Load Balancer, Azure ExpressRoute, Azure Traffic Manager, Azure Active Directory Application Proxy (Azure AD), Azure Firewall, Virtual Network service endpoints,, Azure Private Link, Azure Bastion, Azure Front Door, Azure DDoS Protection, Azure Information Protection, Microsoft Intelligent Security Graph API	
AWS	2017 Security Services	Current Security Services
	AWS Certificate Manager, Amazon Cloud Directory, AWS CloudHSM, AWS Directory Service, **AWS Artifact**, **AWS Identity and Access Management (IAM)**, **Amazon Inspector**, **AWS Key Management Service (KMS)**, **AWS Organizations**, **AWS Shield**, **AWS Web Application Firewall (WAF)**	**AWS IAM Identity Center**, **AWS Organizations**, **Amazon Inspector**, **AWS WAF**, **AWS Shield**, **AWS Artifact**, **AWS Key Management Service (KMS)**, Amazon GuardDuty, AWS IoT Device Defender, Amazon CloudWatch, Amazon Cognito , Eventbridge, AWS Security Hub, Amazon Macie, AWS Private Certificate Authority, AWS Secrets Manager, Amazon Detective, AWS Audit Manager, AWS CloudTrail
Google Cloud	2020 Security Services	Current Security Services
	Security analytics and operations, Application security	Chronicle security analytics and operations platform, Web App and API Protection (WAAP), Security Foundation, Risk and compliance as code (RCaC), Security and resilience framework, Software supply chain security, Risk Protection Program

Notes: The table lists examples of current security services on AWS, Azure, and Google Cloud from their website. Access time: July 17^{th}, 2023. The comparison of early-on security services is done by using the Wayback Machine Internet Archive.

3.2 Strategies and Timing

Figure 1 summarizes the timing of the game in each period. After the initial period, users start each subsequent period, $t > 0$, by choosing to stay with their CSP or switch. From a technical perspective, this avoids the need to invoke a fulfilled expectations equilibrium, whereby users and the CSP make decisions based on the expected number of users, with such an expectation required to be fulfilled ex-post without specifying how it comes about or the associated information structure. By contrast, our solution concept is Markov Perfect Equilibrium, whereby the state variables – security and vulnerability – determine the information structure upon which players condition their strategies. As shown below, both security and vulnerability are functions of the number of users of a CSP. Consequently, once users are allocated to their CSP (in period $t = 0$) or choose their CSP (in $t > 0$), CSPs $j \in \{1, 2\}$ choose their security investment, $s_{cspj,t}$, given their number of users. This determines the "out-of-the-box" baseline level of security, which is, of course, susceptible to zero-days and may be otherwise augmented or compromised by user behavior.

Given $s_{cspj,t}$, users follow by determining their security investment, $s_{i,t}$. Part of what goes into $s_{i,t}$ are user configurations and permissions, which are known to be prime determinants of security. Another part of $s_{i,t}$ is assessing what is meant by the CSP's out-of-the-box security each time the CSP updates. For example, in mean time before failure, when CSPs develop a new cloud service, users devote $\$s_{i,t}$'s worth of hours testing its security or paying a third-party validator to do so. Users can also test new versions of the service as released, spending $\$s_{i,t}$'s worth of hours or again pay a validator to do so. Another example is the life cycle of security architecture. Initially, CSPs invest in providing security to users, $s_{cspj,t}$. Users can then choose to re-architect their security system or purchase security services from their CSP, spending $s_{i,t}$ in total. The security services provided by Amazon Web Services, Microsoft Azure, and Google Cloud are listed in Table 2.

After these steps determine the security umbrella, users purchase $y_{i,t}$ units of cloud services based upon their configurations given the current state of security.

3.3 State Variables and Information

Our analysis revolves around two payoff-related state variables: accumulated security investment and accumulated vulnerability. The states summarize the history in previous periods and directly figure into current-period payoffs.

Given individual security investments in period t by user i of CSP j, $s_{i,t}$, and the security investment by its CSP, j, $s_{cspj,t}$, state variable *total accumulated security investment* on CSP j at the end of period t, $S_{j,t}$, is

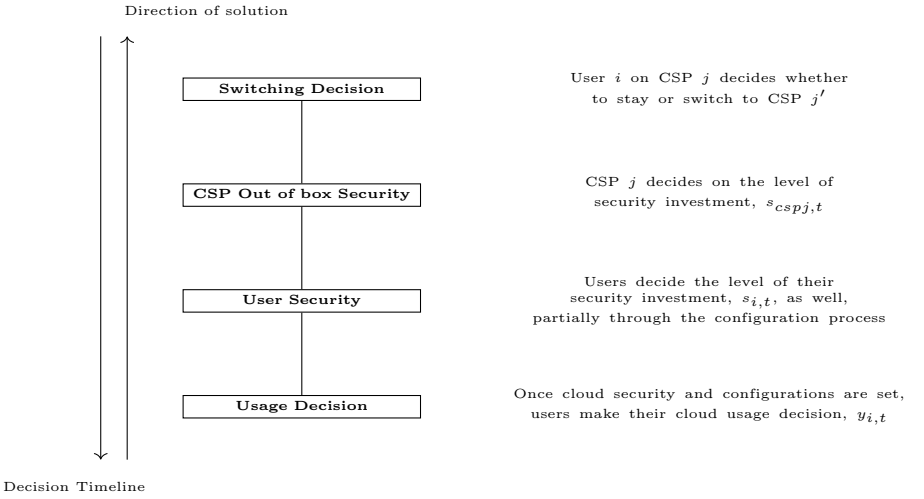


Figure 1: Timing

$$S_{j,t} = \sum_{\tau=0}^{t} \sum_{i} \delta_S^{\tau} [\alpha s_{cspj,\tau} + s_{i,\tau}] = s_{i,t} + \alpha s_{cspj,t} + \sum_{i' \neq i} s_{i',t} + \delta_S S_{j,t-1} \tag{1}$$

where $1 - \delta_S \in [0, 1]$ is the depreciation speed (decay rate) of past security investment. The term $\alpha > 0$ recognizes the CSP's security efforts can have a different marginal effect on overall security relative to users' efforts. Tianfield (2012) identifies how this relative effect can vary across IaaS, PaaS, and SaaS, causing the security responsibilities of CSP and users to differ between service layers of the cloud stack. Similarly, the MITRE ATT&CK© matrix for the cloud includes phenomena under the purview of CSPs and users that differ between layers in the cloud stack. Hence, α is not indexed by subscript j because it corresponds to the relative contribution of a CSP within a particular class of service (layer within the cloud stack), rather than across different classes of service. In equilibrium, we conduct comparative statics with respect to α.

Taking the effect of the CSP and users' security contributions to be a function of their aggregate sum is in keeping with regarding the cloud as the attack surface. An alternative is security is determined by the minimum contribution, known as the weakest link. Yet evidence drawn from data and observations from real-world cyberattacks indicates an impressive diversity of tactics, techniques, and procedures (TTPs) on the part of cloud adversaries (Crowdstrike 2023). Examples of cloud penetration TTPs include exploiting insecure CSP default settings, user misconfigurations, containers without internal security, corporate subnets without multifactor authentication (MFA), open ports or servers to conduct a Man-in-The-Cloud attack, and abuse of cloud resources, such as occurs with coin mining. Indeed, even misconfigurations have variations such as excessive permissions, disabled logging features, and publicly accessible cloud storage buckets. Similarly, the proliferation of API calls and privileges available to control API access broadens the attack surface. A summation aggregator indicates the extent CSPs and users' address the multiplicity of security issues inherent in the cloud. It therefore follows that subsequent states of security are also derived from the (discounted) sum of past security actions.[4]

[4]Moreover, Hausken (2002) draws a parallel between weakest link and serial networks, and the cloud is not a serial network because, by design, redundancy and location independence are part of a CSP's selling points. In addition, Florêncio and Herley

Total accumulated security investment on CSP j at the end of period t, $S_{j,t}$, can also be written as the sum of CSP j's accumulated security investment, $S_{cspj,t}$, and *user's accumulated individual security investment*, $S_{i,t}$.

$$S_{j,t} = \alpha S_{cspj,t} + \sum_i S_{i,t}$$

where $S_{cspj,t} = \sum_{\tau=0}^{t} \delta_S^\tau s_{cspj,\tau}$ and $S_{i,t} = \sum_{\tau=0}^{t} \delta_S^\tau s_{i,\tau}$.

Our second state variable concerns vulnerability. A CSP's ex-ante vulnerability is a function of the security of the CSP, users' attractiveness to malicious actors, the CSP's attractiveness to malicious actors, and malicious actors' effort (Gordon and Loeb 2002, Cavusoglu, Raghunathan, and Yue 2014, Fedele and Roner 2022). Given we do not have an active malicious actor in the game, ex-ante vulnerability is mainly a measure of target attractiveness to malicious actors. A flourishing CSP with a growing number of users is more attractive ex-ante, with all their personally identifiable information, proprietary secrets, pass-codes, ransomware prospects, and business disruption opportunities at risk. It also agrees with the market share theory of malicious targeting (O'Donnell 2008, Garcia, Sun, and Shen 2014, Vasek, Wadleigh, and Moore 2015, Arce 2018, Geer, Jardine, and Leverett 2020), whereby platforms with larger relative market share receive at least their share of targeting by malicious actors. At the same time, ex-post vulnerability is also a function of CSP's and their users' security investment. Consequently, in period (stage) t, given ex-ante $V_{j,t-1}$ the ex-post marginal vulnerability attributed to user i, $v_{i,t}$, is:

$$v_{i,t} = y_{i,t} - s_{i,t},$$

Given users i of platform j, state variable *total accumulated* (ex-post) *vulnerability* on platform j at the end of period t is defined as

$$V_{j,t} = \sum_{\tau=0}^{t} \sum_i \delta_V^\tau [\underbrace{(y_{i,\tau} - s_{i,\tau})}_{v_{i,\tau}} - \alpha s_{cspj,\tau}]$$

$$V_{j,t} = \delta_V V_{j,t-1} + \sum_{i' \neq i} y_{i',t} + y_{i,t} - S_{j,t} \tag{2}$$

where $1 - \delta_V \in [0, 1]$ is the depreciation speed of past vulnerability. In contrast to our justification of cloud security as a summation-determined public good, expressing the vulnerability state variable in terms of the sum of individual user vulnerability is a simplifying assumption. Vulnerability is taken to be a function of the concentration of resources using the CSP, net of security. Nonlinearities with respect to vulnerability instead arise within users' and CSPs' payoff functions. Moreover, in many extensions of the Gordon-Loeb (2002) decision-theoretic model to a game-theoretic setting the level of vulnerability is taken as a parameter open to ex-post comparative statics analysis (Fedele and Roner 2022). By contrast, here the level of vulnerability is an endogenously-determined state variable.

Finally, in a Markov Perfect Equilibrium the state variables determine the information structure upon which players condition optimal strategies. At the beginning of state t the players know the pair $(V_{j,t-1}, S_{j,t-1})$. In addition, the number of potential state pairs, $(V_{j,t}, S_{j,t})$, is finite. This is a standard assumption necessary for existence of a Markov Perfect Equilibrium.

3.4 Cybersecurity

Beginning at least with Gordon and Loeb (2002) the probability of a successful attack is a function of ex-post vulnerability, $p(V_{j,t})$, rather than only as a function of total security effort, $p(S_{j,t})$. In expressing the

(2013) show once a single attacker versus a single defender with a weakest link is extended to the case of a population of users attacked by a population of malicious actors, as is the case in the cloud, the underlying weakest-link aggregator is converted into a summation aggregator of security effort.

probability of a successful attack in terms of vulnerability we capture the effects of its components, $s_{i,t}$, $s_{cspj,t}$, and $y_{i,t}$, on cloud security. It easily holds at the extreme, where governments having large $V_{j,t}$'s are targeted by advanced persistent threats (APTs) with the commensurate effect on $p(V_{j,t})$. At the same time, security efforts reduce vulnerability, $V_{j,t}$, and therefore the probability of a successful attack.

We define $p(V_{j,t})$ to be monotonically increasing and convex in $V_{j,t}$. The accumulated vulnerability of platform j determines every user's probability of being attacked. It is intentionally modeled in this way to capture the multi-tenant nature of cloud services, where one user's security can impact their co-tenants' security. Critical cross-tenant vulnerabilities violating cloud isolation are increasingly documented (Wiz 2023). By contrast, term $\tilde{p}(V_{j,t})$ is the probability the CSP suffers a successful attack as a function of ex-post vulnerability. It satisfies the same monotonicity and convexity assumptions as $p(V_{j,t})$.

3.5 Payoffs

A user's payoff at time t has several components: the benefit from using cloud services under the CSP's security umbrella; the probability of a successful material attack on this benefit; the cost incurred from a material impact; security investment costs; and the cost incurred from a possible platform switch:

$$u_{i,t} = p(V_{j,t})[(1-c)b(y_{i,t})] + (1-p(V_{j,t}))b(y_{i,t}) - ks_{i,t} - \lambda S_{j,t-1} \tag{3}$$

$$u_{i,t} = (1-p(V_{j,t})c)b(y_{i,t}) - ks_{i,t} - \lambda S_{j,t-1} \tag{4}$$

where function $b(y_{i,t})$ measures the net benefits arising from using $y_{i,t}$ cloud services under the security umbrella. Benefit $b(y_{i,t})$, $b' > 0, b'' < 0$ captures every non-security related aspect stemming from the cloud service (revenues gained from $y_{i,t}$, the price of $y_{i,t}$ usage, etc.). Similar benefit functions facilitating analyses of specific facets of a platform can be found in Lee (2014) and Arce (2020). Term $c \in (0,1)$ captures the percentage cost of a successful attack and k the per unit (opportunity) cost from security investment. Contingent payoff component $\lambda S_{j,t}$ is the per unit switching cost, λ, times state variable $S_{j,t}$, the accumulated security investment on the incumbent platform. It becomes part of a user's payoff only if they switch CSPs. The idea is familiarity with CSP j's security umbrella makes it costly to switch to a CSP with a different security umbrella and attendant protocols. In contrast to standard analyses where lock-in is the outcome of one actor's actions, usually the vendor, $\lambda S_{j,t}$ is jointly determined by users and their CSP through $S_{j,t}$. An alternative is Arce (2022), where users and their CSP interact to determine the marginal degree of lock-in, equivalent to λ in our model. Here instead the magnitude of lock-in is jointly determined. Finally, the expression shows security is not just another dimension of product differentiation. The security umbrella is the gateway to the benefits associated with a CSP's services, $b(y_{i,t})$. Specifically, a decrease in the probability of a successful breach owing to the actions of any user creates a selective incentive for other users in the form of $(1-p(V_{j,t})c)b(y_{i,t})$.

CSP j's per-period payoff takes a similar form:

$$\pi_{j,t} = \tilde{p}(V_{j,t})[(1-C)nB(y_{i,t})] + (1-\tilde{p}(V_{j,t}))nB(y_{i,t}) - Ks_{cspj,t} \tag{5}$$

$$\pi_{j,t} = (1-\tilde{p}(V_{j,t})C)nB(y_{i,t}) - Ks_{cspj,t} \tag{6}$$

Terms $K > 0$ measures the CSP's per-unit cost of security investment and $C \in (0,1)$ the CSP's per-unit cost of a successful attack. Function $nB(y_{i,t})$ measures the profit generated by n users' subscription to the CSP. As is the case for $b(y_{i,t})$, $nB(y_{i,t})$ summarizes all non-security aspects of providing cloud services. Given $C \in (0,1)$, CSPs always want more users.

3.6 Equilibrium

We close our model by studying the symmetric Markov Perfect Equilibrium (MPE) of the game. A player's strategy in period t is *Markov* (or state-space) if its history-dependence is only a function of the information provided by the values of the state variables at the start of period t, $(V_{j,t-1}, S_{j,t-1})$, rather than the entire specifics of the past history of play. The number of strategies for a player is therefore not greater than

the (finite) number of states, $(V_{j,t-1}, S_{j,t-1})$, rather than the number of potential histories. Moreover, the exact time sequence $\{s_{j,\tau}, s_{i,\tau}, y_{i,\tau}\}_{\tau=0}^{t-1}$ determining state (history) $(V_{j,t-1}, S_{j,t-1})$ does not matter. A Markov strategy is *stationary* if, whenever $(V_{j,t-1}, S_{j,t-1}) = (V_{j,\hat{t}-1}, S_{j,\hat{t}-1})$, $t \neq \hat{t}$, then a player takes the same strategy in state $(V_{j,t-1}, S_{j,t-1})$ as in state $(V_{j,\hat{t}-1}, S_{j,\hat{t}-1})$. That is, a player takes the same actions for the same state values independently of the time of the state. The assumption is justifiable given our game's infinite horizon. Stationary strategies are *Markov Perfect* if they are subgame perfect for the game in stage t for every t. MPE is a powerful tool for dynamic games because the state variables summarise both the history of play and the information structure.[5] Consequently, at the beginning of period t, users make strategic choices knowing the values of $V_{j,t-1}$ and $S_{j,t-1}$, and their optimal value function only depends on the resultant states.

An advantage of our approach is extensive form games and repeated games are often sensitive to the timing of actions in the (unvarying) stage game, resulting in phenomena such as first-mover advantages or Folk Theorem-based indeterminacy. If the security or economic environment is not dynamic then the equilibrium is more dependent on the decision dynamics. By contrast, in our analysis both decisions and the economic environment are dynamic, consistent with cloud economics and the continuing relationship between CSPs and their users. For example, our approach produces state-dependent actions with richer characterizations of how strategic variables affect one another. This cannot be the case in a repeated game because in a repeated game only one state occurs – the stage game. Moreover, we capture the two-way direction between security investments and cloud usage over time. As such, best replies are truly reaction functions.

3.7 Initial Characteristics

We conclude this section by characterizing the strategic relationships among users and between users and their CSP. Specifically, plain complements is a property of whether others' strategies increase a player's payoff, and strategic substitutes is a property of best replies (Eaton 2002, chap.10); that is, whether the players' strategies move in opposite directions. The following propositions characterize whether an increase in the security investments of other users or their CSP increases user i's payoff (plain complements) and if it decreases user i's security investment and the rate it changes (strategic substitutes).

In the absence of lock-in ($\lambda = 0$), users' and their CSP's security investments are plain complements for their stage t (per period) payoffs, $\frac{\partial u_{i,t}}{\partial s_{i',t}} > 0$ and $\frac{\partial u_{i,t}}{\partial s_{csp j,t}} > 0$. With finite lock-in costs, plain complements requires:

$$b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\delta_V^t > \lambda\delta_S^t$$

Proof: all proofs are in appendix.

The condition for plain complements characterizes how competition between CSPs impacts the nature of security investment. Suppose the switching cost does not bind. In that case, other users' and the CSP's efforts to enhance security provide a public good to user i. By contrast, once switching cost λ binds, such efforts may eventually be harmful if the marginal cost of their efforts in terms of lock-in, $\lambda\delta_S^t$, exceeds the marginal reduction in vulnerability they bring about, $b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\delta_V^t$. In a world where δ_V is sufficiently lower than δ_S the plain complements relationship is also broken. For example, if δ_S is large the decay speed of technology, $1-\delta_S$, is so small only past security investment matters and current-period efforts do not figure much into a user's calculus. Overall, the novel implication is others' security investments can be plain complements (increase other users' payoffs) at one point in time and plain substitutes (decrease other users' payoffs) later in the same game.

Other users' security investments are strategic substitutes for user i's security investment:

$$\frac{\partial u_{i,t}^2}{\partial s_{i,t}\partial s_{i',t}} < 0$$

[5]The game may have other non-MPE. However, if other players use stationary Markov strategies, player i's best reply is to use stationary Markov strategies as well.

Term $\partial u_{i,t}/\partial s_{i,t}$ derives a user's best reply (reaction) function. Hence, the second derivative of the term with respect to $s_{i',t}$ characterizes the user's best reply function with respect to the security strategy of another user, $i' \neq i$, and the second derivative with respect to $s_{cspj,t}$ characterizes the user's best reply function with respect to their CSP's security strategy. A negative sign means the user's best response security effort decreases in the security effort of other users, known as strategic substitutes.

Indeed, for the CSP's security investment, $\frac{\partial u^2_{i,t}}{\partial s_{i,t}\partial s_{cspj,t}}$ is also negative. The larger the CSP's responsibility for joint security for the service in question, α, the smaller is the user's best reply to the CSP's security investment. That is, strategic substitutes between CSP and users is exacerbated.

$$\frac{\partial u^2_{i,t}}{\partial s_{i,t}\partial s_{cspj,t}} = b(y_{i,t})\delta_V \frac{\partial p^2(V_{j,t})}{\partial V^2_{j,t}}(-\alpha\delta^t) < 0$$

The larger α is the more the CSP's security investment decreases the user's marginal benefit of their own security investment. While negative, users are not absolved from the joint security problem even though the cloud service they contract for may require greater security responsibility on the part of the CSP. In particular, the upper layer of cloud infrastructure (the control plane), which users are responsible for securing, has increasingly become vulnerable to attacks introduced by misconfigurations and human error (Torkura et al. 2021).

Together, Propositions 3.7 and 3.7 epitomize the joint security problem. For example, 55 percent of respondents to a Ponemon Institute survey of cloud users believe the in-house IT security leader is not responsible for ensuring their organization's safe use of cloud computing resources (Ponemon Institute 2014). To the extent such beliefs may be rational on the part of users', as indicated by Propositions 3.7 and 3.7, it is inefficient if CSPs do not follow through with the tools at their disposal to aid users. For example, AWS knew Capital One had the misconfiguration leading to their 2019 breach, but did not communicate it to Capital One or other users with similar misconfigurations.

4 Locked-In Users

We begin with a baseline model where users are locked into their CSP. In this case, $\lambda \to \infty$; therefore, users do not switch CSPs and CSPs know it.

In dynamic games the players maximize their lifetime payoffs, which are the discounted sum of their payoffs in each period, t. For user i of CSP j:

$$U_{i,j} = \sum_{t=0}^{\infty} \delta^t u_{i,t}(\cdot)$$

where $u_{i,t}(\cdot)$ is the payoff in period t, δ is the discount factor, and the horizon is infinite. An infinite horizon captures the nonzero probability CSPs and their users interact for another period.

In an MPE, players' payoffs are transformed into optimal value functions, which themselves are represented as only a function of the state variables summarizing the history of play:

$$U_{i,t} = U_{i,t}(V_{j,t-1}, S_{j,t-1})$$

State variables $V_{j,t-1}$ and $S_{j,t-1}$ are known at the start of period t. When users select their security investment and usage in period t they do so understanding the joint effect on their current-period payoff, $u_{i,t}(\cdot)$. In addition, users are forward-looking and realize their choices figure into determining $S_{j,t}$ and $V_{j,t}$. Given discount factor δ, users select $s_{i,t}$'s and $y_{i,t}$'s to maximize $U_{i,t}(\cdot)$ with these two effects in mind:

$$U_{i,t}(V_{j,t-1}, S_{j,t-1}) = \max_{s_{i,t}, y_{i,t}} \{u_{i,t}(\cdot) + \delta U_{i,t+1}(V_{j,t}, S_{j,t})\} \tag{7}$$

This is the familiar Bellman equation in dynamic programming expressed in terms of the user's optimal value function, $U_{i,t}(V_{j,t-1}, S_{j,t-1})$, current-period payoff, $u_{i,t}(\cdot)$, and discounted continuation value, $\delta U_{i,t+1}(V_{j,t}, S_{j,t})$.

When finding a best reply, each player holds the strategies of the other players constant, and in an MPE others' strategies are additionally unchanging in they are also stationary in equivalent states. It therefore follows equation (7) can be re-expressed in terms of the optimal value function at the given states without reference to the time period:

$$U_i(V_{j,t-1}, S_{j,t-1}) = \max_{s_{i,t}, y_{i,t}} \{u_{i,t}(\cdot) + \delta U_i(V_{j,t}, S_{j,t})\} \tag{8}$$

Consequently, finding a best reply is a dynamic programming problem for each of the players (Friedman 1976, Haurie et al. 2012). This is because when finding a best reply, player i holds the strategies of the other players constant; e.g., $\partial y_{i',t}/\partial y_{i,t} = 0 \; \forall i' \neq i$.

The solution to (8) must also be subgame perfect within period t. Figure 1 lays out our solution procedure. Usage, $y_{i,t}$, is chosen last; hence, by backward induction we solve for it first. With respect to $\delta U_i(V_{j,t}, S_{j,t})$, $V_{j,t}$ is a function of $y_{i,t}$ via state equation (2). Given the expression for $u_{i,t}(\cdot)$ in (4), the associated first-order condition is

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial y_{i,t}} = (1 - p(V_{j,t})c)\frac{\partial b}{\partial y_{i,t}} - cb\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial y_{i,t}} + \delta\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial y_{i,t}} = 0 \tag{9}$$

Setting $\partial b/\partial y_{i,t} = b'$ and substituting $\partial V_{j,t}/\partial y_{i,t} = 1$ (from equation (2)):

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial y_{i,t}} = (1 - p(V_{j,t})c)b' - cb\frac{\partial p(V_{j,t})}{\partial V_{j,t}} + \delta\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}} = 0 \tag{10}$$

where $\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}$ is unknown.

Equation (10) is the best reply function (reaction function) for $y_{i,t}$ in implicit function form. Prior to analyzing this function, unknown term $\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}$ needs to be characterized. To this end, we follow Benveniste-Scheinkman's (B-S) procedure (Benveniste and Scheinkman 1979), as operationalized in the proof of lemma 4.

A user's optimal value function decreases in total vulnerability at an increasing rate:

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}} = -\delta_V(1 - p(V_{j,t})c)b' < 0$$

$$\frac{\partial^2 U_i(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}^2} = \delta_V^2\frac{\partial p(V_{j,t})}{\partial V_{j,t}}cb' > 0$$

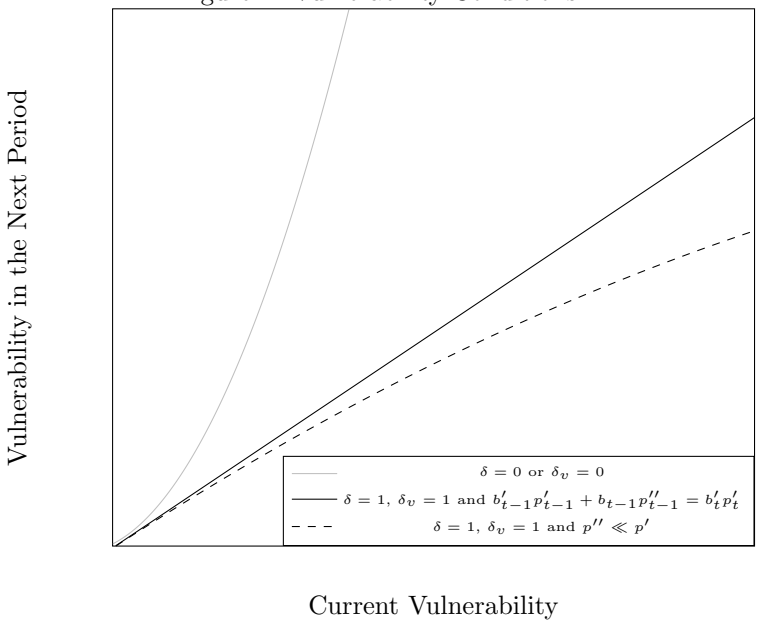
where $c \in (0, 1)$ and $b' > 0$. Updating $\frac{\partial U_i(V_{t-1}, S_{t-1})}{\partial V_{j,t-1}}$ one period yields:

$$\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}} = -\delta_V(1 - p(V_{j,t+1})c)b' < 0$$

which is the unknown term in equation (10).

By characterizing the final term in equation (10), we establish CSP users must consider both the effect of usage on the probability of a breach, the second term in equation (10), and the future effect of usage on their value function, the third term in equation (10). Both effects subtract from the benefits of current usage, as expressed by the first term in equation (10). Moreover, these effects are not constant from period-to-period. It begs the question of how these rates of change balance (or not) as reflected by the time path of vulnerability resulting from optimal usage and security; i.e., an Euler equation.

Figure 2: Vulnerability Conditions



4.1 The Euler Equation

Our model is quite general; no functional forms are specified for per-period payoffs, the probability of a breach, and so on. In such circumstances, the Euler equation assists in characterizing the associated dynamics (Josa-Fombellida and Rincón-Zapatero 2008, Dechert 1997). Here, the Euler equation shows the relationship between optimal levels of $V_{j,t}$ and $V_{j,t+1}$. In deriving the Euler equation, we characterize the optimal path of accumulated vulnerability. The path of users' behavior is addressed in the next subsection. Moreover, neither extensive form games nor repeated games generate an Euler equation as an output. The Euler equation is an advantage of the dynamic game approach.

Substituting the value for $\partial U_i/\partial V_{j,t}$ from lemma 4 into the first-order condition (reaction function) for $y_{i,t}$ in equation (10) immediately yields the Euler equation for the dynamics of accumulated vulnerability.

The Euler equation for the optimal level of accumulated vulnerability is

$$\frac{\partial U_i(V^*_{j,t-1}, S_{j,t-1})}{\partial V^*_{j,t-1}} = \delta_V \left[-bc\frac{\partial p(V^*_{j,t})}{\partial V^*_{j,t}} + \delta \frac{\partial U_i(V^*_{j,t}, S_{j,t})}{\partial V^*_{j,t}} \right] \tag{11}$$

where $\frac{\partial p(V_{j,t})}{\partial V_{j,t}} > 0$ and $\frac{\partial p^2(V_{j,t})}{\partial V^2_{j,t}} > 0$.

From lemma 4 and shifted down one period, the Euler equation can also be expressed as

$$(1 - p(V^*_{j,t-1})c)b'(y_{i,t-1}) - b(y_{i,t-1})c\frac{\partial p(V^*_{j,t-1})}{\partial V^*_{j,t-1}} = \delta\delta_V(1 - p(V^*_{j,t})c)b'(y_{i,t}) \tag{12}$$

The Euler equation lends itself to several characterizations of our model. One way to view the Euler equation is as the intertemporal relationship between the marginal costs of accumulated vulnerability in the

current and future periods (McKay, Nakamura, and Steinsson 2017). From equation (11), term $-\delta_V bc\frac{\partial p(V^*_{j,t})}{\partial V^*_{j,t}} < 0$ measures the extent current vulnerability influences optimal vulnerability by increasing the likelihood of a breach. Term $\delta\frac{\partial U_i(V^*_{j,t},S_{j,t})}{\partial V^*_{j,t}} < 0$ measures the extent future vulnerability influences optimal vulnerability. Hence, in the absence of future vulnerability considerations, current vulnerability is too high. In other words, a non-dynamic (single-shot) approach leads to excessive vulnerability in each period.

Another way to view the Euler equation is from the perspective of the interim equilibrium when users maximize their value function by choosing $y_{i,t}$. In this subgame, equation (12) characterizes the optimal path of accumulated vulnerability. On this path, given a certain level of $V^*_{j,t-1}$, the left-hand side of equation (12) is constant, and the equilibrium level of $V^*_{j,t}$ can be predicted by $V^*_{j,t-1}$, provided inverse function $p^{-1}(\cdot)$ exists.

The equilibrium path of accumulated vulnerability is

$$\frac{\partial V^*_{j,t}}{\partial V^*_{j,t-1}} = \frac{b'(y_{i,t-1})\frac{\partial p(V^*_{j,t-1})}{\partial V^*_{j,t-1}} + b(y_{i,t-1})\frac{\partial^2 p(V^*_{j,t-1})}{\partial^2 V^*_{j,t-1}}}{\delta\delta_V b'(y_{i,t})\frac{\partial p(V^*_{j,t})}{\partial V^*_{j,t}}} > 0 \tag{13}$$

Vulnerability, which increases with usage, builds upon itself. The increase in vulnerability over time justifies CSA's concern with security in the cloud. It also identifies the tradeoff inherent in taking shelter under the CSP's security umbrella. We therefore turn to the question of whether the path of accumulative vulnerability converges or not.

Specifically, the Euler equation additionally lends itself towards comparative statics of the parameters and their implications for (non-)convergence. The numerator of equation (13) comes from the first-order conditions for $V^*_{j,t-1}$ (see the proof of Proposition 4.1). Yet a user's payoff function is not linear in $V^*_{j,t-1}$, and so neither are the terms in the numerator of the equation (13). The denominator of equation (13) is a function of $V^*_{j,t}$, discounted by both δ and δ_V.

Consequently, by Proposition 4.1, convergence of the optimal path of $V^*_{j,t}$ depends on δ and δ_V. For example, in extreme cases, if $\delta = 0$ (or $\delta_V = 0$), decision-making becomes static. From Figure 2, the path of $V^*_{j,t}$ is explosive because users' and CSPs' preferences for the future (δ) do not keep vulnerability in check or their recognition of the carryover in vulnerability from one period to the next (δ_V) does not keep vulnerability in check. Managers must realize it is a consequence of an absence of concern with how vulnerability builds on itself. One way to influence managerial behavior in this direction is through the guidance provided by the aforementioned CSA document on joint security in the cloud. In the absence of managerial action, social planners must act if the market itself can not motivate the users to sufficiently contribute to the security umbrella.

By contrast, if $\delta = 1$ and $\delta_V = 1$, the optimal path is less volatile because users hold past, current, and future vulnerability in equal regard. Indeed, in this case one cannot rule out $\partial V^*_{j,t}/\partial V^*_{j,t-1} \leq 1$ and $V^*_{j,t}$ converges. Contrasting these conditions shows how important it is for CSPs and social planners to gauge users' attitudes toward the future, the past, and the resulting vulnerability.

If $\delta = 1$ and $\delta_V = 1$, equation (13) becomes

$$\frac{\partial V^*_{j,t}}{\partial V^*_{j,t-1}} = \frac{b'(y_{i,t-1})\frac{\partial p(V^*_{j,t-1})}{\partial V^*_{j,t-1}}}{b'(y_{i,t})\frac{\partial p(V^*_{j,t})}{\partial V^*_{j,t}}} + \frac{b(y_{i,t-1})\frac{\partial^2 p(V^*_{j,t-1})}{\partial^2 V^*_{j,t-1}}}{b'(y_{i,t})\frac{\partial p(V^*_{j,t})}{\partial V^*_{j,t}}} \tag{14}$$

From equation (14), the optimal path depends on the possible range of changes in functions $b(y_{i,t})$ and $p(y_{i,t})$. For example, if the numerator $b'_{t-1}p'_{t-1} + b_{t-1}p''_{t-1}$ is exactly the same as the denominator $b'_t p'_t$, then $\partial V^*_{j,t}/\partial V^*_{j,t-1} = 1$. From Figure 2, $V^*_{j,t}$ reaches a steady state. In more general cases, term $b(y_{i,t-1})$ is the net profit/benefit from using the cloud. As such, it takes the largest value in equation (14). Terms $b'(y_{i,t}) > 0$ and $b'(y_{i,t-1}) > 0$ are marginal profit, which is clearly less than total profit, $b(y_{i,t-1})$. We assume convexity in the model: $b''(\cdot) < 0$, so changes in $b'(\cdot)$ from period $t-1$ to period t will not be too big if usage is large.

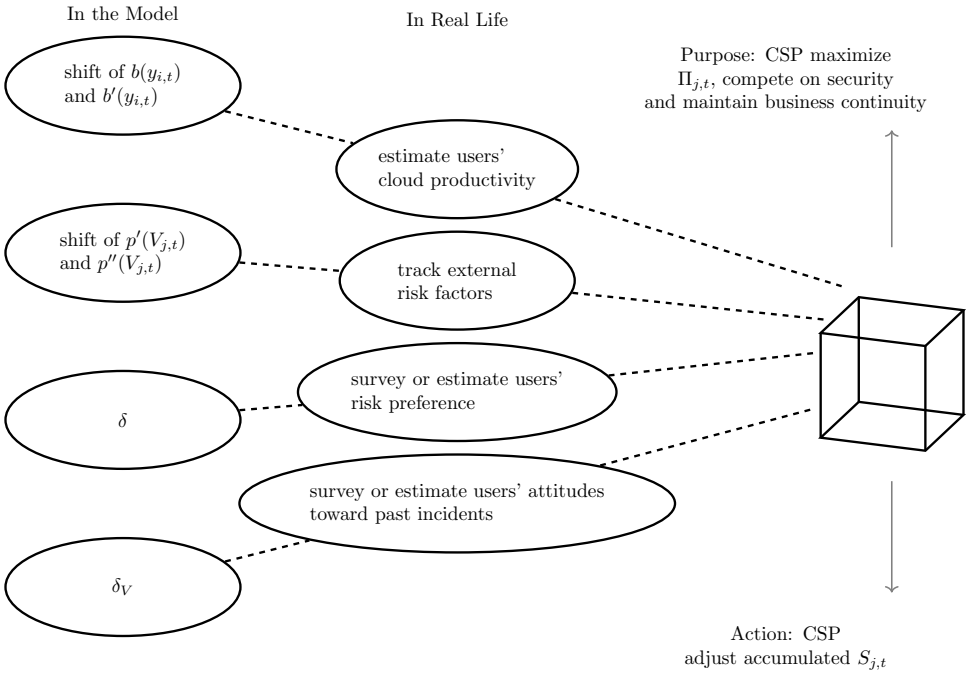


Figure 3: What Goes into the Vulnerability Prediction Box?

Notes: This figure shows how our model can serve as a manual for designing a prediction algorithm for cloud vulnerability. The external shocks that impact the users' cloud productivity and cyber risk and the changes in users' attitude towards the past and the future impact the total vulnerability results should enter the prediction algorithm, as in Proposition 4.1 where the dynamic path of total vulnerability is $\frac{\partial V^*_{j,t}}{\partial V^*_{j,t-1}} = \left[b'(y_{i,t-1}) \frac{\partial p(V^*_{j,t-1})}{\partial V^*_{j,t-1}} + b(y_{i,t-1}) \frac{\partial^2 p(V^*_{j,t-1})}{\partial^2 V^*_{j,t-1}} \right] / \delta \delta_V b'(y_{i,t}) \frac{\partial p(V^*_{j,t})}{\partial V^*_{j,t}}$.

The large $b(y_{i,t})$ value in equation (14) is weighted by p'' and the smaller $b'(y_{i,t})$ value is weighted by p'. Moreover, breach probability $p(V_{j,t})$ is a small number with even smaller changes. Indeed, as we allow $V_{j,t}$ to take a large range of values to accommodate large-scale usage and security investments, $p(V_{j,t})$ will not be overly convex. Hence, weights p'' on $b(y_{i,t})$ and p' on $b'(y_{i,t})$ stay small for large usage values, $y_{i,t}$, and corresponding vulnerability. Thus, as illustrated in Figure 2, when $\delta = 1$, $\delta_V = 1$ and $p'' \ll p'$, it is possible that $\partial V^*_{j,t} / \partial V^*_{j,t-1} \leq 1$.

In less extreme cases, as δ_V increases, $V^*_{j,t}$'s response to $V^*_{j,t-1}$ decreases. If vulnerability depreciates slower (higher δ_V), the impact of $V^*_{j,t-1}$ on $V^*_{j,t}$ decreases. It is similar to the case for δ; if users are more forward-looking (higher δ) they use less CSP services in the current period owing to their concern for future vulnerability.

With this in mind, Figure 3 illustrates how CSP managers can track the crucial variables identified in Proposition 4.1 to design a vulnerability prediction algorithm. Specifically, the comparative statics discussed above for the factors and parameters impacting the model are listed on the far left. In the middle, corresponding real-world observations for each factor are listed. "Estimate users' cloud productivity" is important to understand $b(\cdot)$, $b'(\cdot)$ and $b''(\cdot)$. "Track external risk factors" is useful to predict $p(\cdot)$, $p'(\cdot)$ and $p''(\cdot)$ (**??**). As stated previously, p'' plays an important role in the prediction as it is the weight on the large net profit/benefit from using the cloud, $b(\cdot)$. "Survey or estimate users' risk preference" is to check whether users

are more forward-looking (higher δ). "Survey or estimate users' attitudes toward past incidents" is to know vulnerability depreciation speed, δ_V. Successful cloud security requires a combination of marginal analysis, risk analysis, and dynamic decision-making. Our results also highlight the theoretical importance of risk preferences (Hedlund 2000, Safi and Browne 2023) and cybersecurity behavior (Acquisti, Adjerid, Balebako, Brandimarte, Cranor, Komanduri, Leon, Sadeh, Schaub, Sleeper et al. 2017, Dutta and Sanyal 2023).

The purpose and subsequent actions stemming from such predictions are shown on the right of Figure 3. For CSP managers, predicting the vulnerability path helps in competing on security and maintaining business continuity. If the predicted vulnerability is not favorable, CSPs can adjust the total accumulated $S_{j,t}$. Section 5 discusses how CSPs target total accumulated $S_{j,t}$ and its impact on competition. Alternatively, CSPs or social planners can require minimum contributions for all users. Two-factor authentication is an example. This raises issues related to compliance and costly verification of compliance that are beyond the scope of our paper.

4.2 Users' Behavior on the Optimal Path

The following propositions stem from the Euler equation and characterize the dynamics of interdependent behavior of users in a shared security environment. Forward-looking users understand their investment into security affects other users' usage based on the new security level.

On the optimal path of vulnerability, $V^*_{j,t}$, equilibrium usage, $y^*_{i,t}$, increases with the size of security umbrella $S_{j,t}$:

$$\frac{\partial y^*_{i,t}}{\partial S_{j,t}} > 0$$

The safer the CSP is as a whole, the more comfortable users are with increasing their usage. Furthermore, this finding is novel because it identifies a state-based strategic complementarity between $y^*_{i,t}$ and $S_{j,t}$. Several implications follow. First, one can view security umbrella $S_{j,t}$ as an impure public good because it provides a selective (private) benefit to user i in the form of increased $y_{i,t}$ and $b(y_{i,t})$. Second, the increase in $S_{j,t}$ need not be due to an increase in $s_{i,t}$. In other words, *much of a user's security umbrella and resulting increase in usage is due to the security investments of its CSP and other users.* Finally, one cannot forget a CSP's business model relies on usage fees; hence, security adds to the CSP's value proposition by increasing $y_{i,t}$.

The impure nature of the shared security model impacts users' behavior. The next proposition further clarifies the effect, which requires the following definition of a *user's accumulated individual security investment*:

$$S_{i,t} = \sum_t \delta_S^t s_{i,t} = s_{i,t} + \delta_S S_{i,t-1}$$

A user's vulnerability increases in any other user's accumulated security investment. For all $i' \neq i$:

$$\frac{\partial v_{i,t}}{\partial S_{i',t}} > 0$$

Such increased vulnerability is of concern to users and CSPs, affecting their investment in security. The next subsection characterizes users' optimal investment in security. We examine CSPs' optimal investment in security in section 5.

4.3 Users' Optimal Value Function with Respect to Security

Having characterized vulnerability, we now turn to user security. Recall from Proposition 3.7, owing to the potential for lock-in, a user's per-period payoff can either be increasing or decreasing in other users' or their CSP's security investment; i.e., pure complements or pure substitutes. Yet in a dynamic game users maximize a value function, not per-period payoffs, and the value function from period t onward is a function of state $(V_{j,t-1}, S_{j,t-1})$. Recall lemma 4 characterizes the behavior of users' value function with respect to vulnerability

state $V_{j,t-1}$ as $\partial U_i/\partial V_{j,t-1} < 0$. The following lemma characterizes the behavior of users' value function with respect to security state $S_{j,t-1}$.

A user's optimal value function increases in accumulated security investment:

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = \delta_S k > 0$$

Lemma 4.3 establishes $\partial U_i/\partial S_{j,t-1}$ is a constant. That is, there is no time- and state-dependent Euler equation with respect to the effect of current aggregate security on future aggregate security. The dynamics of shared security arise when security interacts with usage, i.e., the Euler equation for vulnerability (equation (12)). As usage/vulnerability is predicated on security, we turn to the CSP's security decision.

5 Cybersecurity and Cloud Symbiosis

In this section we consider the case where users have the ability to switch CSPs; i.e., $\lambda \in [0, \infty)$, and characterize the $(S_{j,t-1}, \lambda)$ pairs such that users do not switch. This produces symbiotic results whereby the no-switching condition has implications for cumulative security investment, $S_{j,t}$, and cybersecurity, $p(V_{j,t})$; and the two variables lock-in users via value creation under the CSP's security umbrella, which users themselves help to create.

5.1 No-switching Condition

We examine the no-switching constraint from the perspective of CSP 1 and its users. A similar analysis holds for CSP 2 and its users. Investment in security has two effects influencing a user's choice to stay: first, it reduces the probability of a breach by reducing vulnerability, $V_{1,t}$; second, it increases switching cost, $\lambda S_{1,t}$, due to familiarity with the CSP's security umbrella. The question is: what level of CSP security investment satisfies the no-switching criterion? This is an economic factor affecting security design.

We define the no-switching constraint as follows. User i on CSP 1 chooses to stay if its optimal value on CSP 1 is greater than or equal to the optimal value generated by switching to CSP 2. Once again, the next-best alternative for users is another CSP because (i) our analysis is, effectively, ex-post to the cloud/enterprise decision analyzed by August et al. (2014) and Zhang et al. (2020), among others, and (ii) once a user is in the cloud the economics of the cloud make another CSP the logical next-best alternative.

Furthermore, instead of referring to the effect of CSP 1's investment in security, $s_{csp1,t}$, on its no-switching constraint, we can instead refer to CSP 1's choice of $S_{1,t}$. By backward induction, we solve for the $y_{i,t}$'s for CSP 1's users, and then the $s_{i,t}$'s for the same users. Given the $s_{i,t}$'s, CSP 1's choice of $s_{csp1,t}$ determines $S_{1,t}$ because it is the only degree of freedom left. It follows that, by backward induction, CSP 1 ultimately determines $S_{1,t}$. It is also the case in period $t-1$ for $s_{csp1,t-1}$ and $S_{1,t-1}$. Similar logic holds for CSP 2 with respect to $S_{2,t}$ and $S_{2,t-1}$. Moreover, a CSP's persistence in the market requires its no-switching constraint is met. Consequently, we can focus on CSP 1's choice of $S_{1,t}$ to meet its no-switching constraint instead of its choice of $s_{csp1,t}$ to maximize its optimal value function.

In period t if user i stays with CSP 1, its stage t payoff is:

$$u_{i,t}^{stay} = [1 - cp(V_{1,t})]b(y_{i,t}) - ks_{i,t},$$

then the optimal value function of a user staying with CSP 1 is:

$$U_{stay}(V_{1,t-1}, S_{1,t-1}) = [1 - cp(V_{1,t})]b(y_{i,t}) - ks_{i,t} + \delta U_{stay}(V_{1,t}, S_{1,t})$$

If switching to CSP 2, the user's stage t payoff is:

$$u_{i,t}^{switch} = [1 - cp(V_{2,t})]b(y_{i,t}) - ks_{i,t} - \lambda S_{1,t},$$

and their optimal value function is:

$$U_{switch}(V_{2,t-1}, S_{2,t-1}, S_{1,t-1}) = [1 - cp(V_{2,t})]b(y_{i,t}) - ks_{i,t} - \lambda S_{1,t-1} + \delta U_{switch}(V_{2,t}, S_{2,t})$$

As an aside, in an oligopolistic situation, we would instead take the value of $u_{i,t}^{switch}$ for a CSP j user to be the value of the solution to

$$\max_{j' \neq j}[1 - cp(V_{j',t})]b(y_{i,t}) - ks_{i,t} - \lambda S_{j,t},$$

From lemma 4.3 and the definition of U_{switch}:

$$\frac{\partial U_{stay}(V_{1,t-1}, S_{1,t-1})}{\partial S_{1,t-1}} = \delta_S k > 0$$

$$\frac{\partial U_{switch}(V_{2,t-1}, S_{2,t-1}, S_{1,t-1})}{\partial S_{1,t-1}} = -\lambda < 0$$

Hence, CSP 1 selects $S_{1,t-1}$, understanding a higher value helps to keep users from switching. However, the user ultimately makes the stay or switch decision by comparing U_{stay} and U_{switch}. By the one-deviation principle (Blackwell 1965) the no-switching condition holds in equilibrium if $U_{stay} \geq U_{switch}$. Furthermore, in a symmetric MPE if the one-deviation principle holds for user i, then no other CSP 1 user can benefit from switching. CSP 1 must at least ensure:

$$U_{stay}(V_{1,t-1}, S_{1,t-1}) = U_{switch}(V_{2,t-1}, S_{2,t-1}, S_{1,t-1})$$

CSP 1 must ensure $S_{1,t-1}$ is at least:

$$S_{1,t-1}^{\min} = \frac{1}{\lambda}\{\delta_S k(S_{2,t-1} - S_{1,t-1}^{\min}) - \delta_V b'\{[1 - p(V_{2,t})c]V_{2,t-1} - [1 - p(V_{1,t})c]V_{1,t-1}\}$$

$$+\frac{1}{2}\frac{\partial p(V_{2,t})}{\partial V_{2,t}}\delta_V^2 cb' V_{2,t-1}^2 - \frac{1}{2}\frac{\partial p(V_{1,t})}{\partial V_{1,t}}\delta_V^2 cb' V_{1,t-1}^2\}$$

Moreover, lock-in allows for cases where users will not switch even though:

$$S_{1,t-1} < S_{2,t-1}; V_{1,t-1} > V_{2,t-1}.$$

Keeping a higher level of $S_{j,t-1}$ increases users' optimal value of staying and reduces their optimal value of switching. However, Proposition 5.1 shows it is possible a user stays even when the other CSP has more accumulated security investment and less accumulated vulnerability. The user is, indeed, locked-in under their CSP's security umbrella. Furthermore, when users do not switch in equilibrium the resulting dynamics are as given in Section 3.

We now turn to a market characterization of CSP security.

$S_{1,t-1}^{min}$ and $S_{2,t-1}$ are strategic complements

$$\frac{\partial S_{1,t-1}^{min}}{\partial S_{2,t-1}} = \frac{\delta_S k}{\lambda + \delta_S k} > 0.$$

Hence, if CSP 2 increases its security, CSP 1 increases its security as well to keep users from switching. At the same time, lock-in via a security umbrella reduces the intensity of security competition and in turn reduces equilibrium $S_{j,t-1}^{min}$. To see this, without lock-in ($\lambda = 0$), $\partial S_{1,t-1}^{min}/\partial S_{2,t-1} = 1$ and CSP 1 adjusts $S_{1,t-1}^{min}$ to a change in $S_{2,t-1}$ on a 1:1 basis. By contrast, for finite $\lambda \neq 0$, $0 < \partial S_{1,t-1}^{min}/\partial S_{2,t-1} < 1$ and CSP 1 only partially adjusts to an increase in $S_{2,t-1}$. CSP security competition is neither a race to the bottom nor a war of increasing security levels. The no-switching requirements on security explain the former and partial

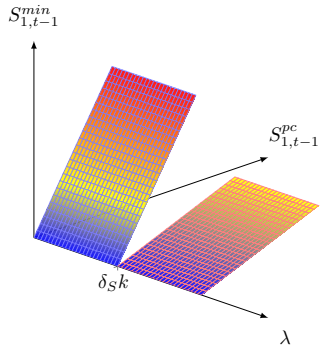


Figure 4: Platform Competition: The Lower Bound of Total Accumulated Security Investment

Notes: The figure shows the lower bound of security technology, the accumulated total security investment $S_{j,t-1}$ when CSPs compete with security. The lower bound depends on the switching cost. When the switching cost λ is lower than the marginal benefit of accumulated security for users $\delta_S k$, the non-switching condition $S^{min}_{j,t-1}$ is bigger than the participation constraint $S^{pc}_{j,t-1}$ and when the switching cost is too high, the participating users will never switch.

adjustment explains the latter. A partial reaction to the change in the security level of a rival – whether an increase or a decrease – indicates security dynamics ultimately settle within a "Goldilocks" region for CSPs.

Our final basis of comparison is when the user is locked-in (no switching is possible). In this case $\lambda \to \infty$, and, by Proposition 5.1, $S^{min}_{1,t-1} = 0$. Intuitively, if users are locked-in then the no-switching constraint is not binding. If the no-switching constraint is not binding, the user's participation constraint (PC) must instead bind. That is, security must be sufficient to induce the user to voluntarily participate. Voluntarily taking shelter in the cloud implies users are not coerced into their relationships with CSPs.

From the Taylor expansion in the proof of Proposition 5.1, when a user is locked-in:

$$U_1(V_{1,t-1}, S_{1,t-1}) = \delta_S k S_{1,t-1} - \delta_V [1 - p(V_{1,t})c] b' V_{1,t-1} + \frac{1}{2} \frac{\partial P(V_{1,t})}{\partial V_{1,t}} \delta_V^2 c b' V_{1,t-1}^2$$

The PC requires $U_{1,t-1} \geq 0$. Solving this inequality for $S_{1,t-1}$

$$S^{pc}_{1,t-1} = \frac{1}{\delta_S k} \left\{ \delta_V [1 - p(V_{1,t})c] b' V_{1,t-1} - \frac{1}{2} \frac{\partial P(V_{1,t})}{\partial V_{1,t}} \delta_V^2 c b' V_{1,t-1}^2 \right\} \tag{15}$$

The PC for users of CSP 2 similarly requires

$$S^{pc}_{2,t-1} = \frac{1}{\delta_S k} \left\{ \delta_V [1 - p(V_{2,t})c] b' V_{2,t-1} - \frac{1}{2} \frac{\partial p(V_{2,t})}{\partial V_{2,t}} \delta_V^2 c b' V_{2,t-1}^2 \right\} \tag{16}$$

In general, a user is *effectively locked-in* if the PC for their CSP is the binding constraint. This raises the interesting possibility users are effectively locked-in under finite values of switching costs, λ. Verification necessitates a comparison of $S^{min}_{j,t-1}$ versus $S^{pc}_{j,t-1}$.

The user's participation constraint is the binding constraint instead of the no-switching constraint, $S^{pc}_{j,t-1} > S^{min}_{j,t-1}$, when the marginal cost of accumulated security from lock-in, λ, exceeds the marginal benefit of accumulated security for users, $\partial U_i(S_{j,t-1}, V_{j,t-1})/\partial S_{j,t-1}$, which, by lemma 4, equals $\delta_S k$. That is, the participation constraint is the binding constraint if

$$\lambda > \delta_S k$$

In this case, the users of both CSPs are effectively locked-in.

Note first that lock-in is no longer akin to $\lambda \to \infty$. The requirement instead becomes $\lambda > \delta_S k$. Figure 4 shows two different sets of linear relationships between the no-switching constraint $S^{min}_{j,t-1}$ and the participation constraint $S^{pc}_{j,t-1}$, one for when switching cost λ is above the threshold and one for λ below it. If switching cost λ is high the binding constraint is the participation constraint $S^{pc}_{j,t-1}$. As shown in Figure 4, the no-switching constraint is smaller than the participation constraint when λ is higher than the threshold; thus, the plane is less steep. In this case, the participation constraint is enough to lock in users because the no-switching constraint is smaller than the participation constraint in a flatter plane.

By contrast, if switching cost λ is instead lower than the marginal benefit of accumulated security for users, $\delta_S k$, the no-switching constraints are instead the binding constraints. The plane is steeper in Figure 4 because the no-switching constraint supersedes the participation constraint. It implies (i) users' PCs are not binding, which is a welfare improvement as users are no longer held to their reservation utilities; (ii) the no-switching constraints are the mechanism for establishing non-monopolistic platform competition (Lee 2014, Arce 2020, 2022), and (iii) if $S_{j,t-1} < S^{min}_{j,t-1}$ whereas $S_{j',t-1} \geq S^{min}_{j',t-1}$, the result is a monopoly outcome in favor of CSP j'. *Cybersecurity is a driver of non-monopolistic outcomes in CSP markets.*

By extension, for heterogeneous users, the relevant economic variable is the marginal benefit of cumulative security of the marginal user (i.e., the user whose no-switching constraint is binding for the CSP). Furthermore, CSPs can do this by bolstering their security umbrella in two possible ways: increasing their own security investment and/or their users' security investment. Examples capturing both possibilities include offering blockchains and homomorphic encryption to users. This suggests a hastening from subscription-based CSPs that turn users' fixed costs into variable ones towards CSPs offering advantages under their security umbrella.

5.2 CSPs and the Path of Vulnerability

In the end, the combination of usage and security determines vulnerability. Furthermore, as shown in our analysis of the Euler equation for vulnerability, users' consideration of the future impact of usage on vulnerability or lack thereof determines whether the path of vulnerability stays within a sustainable range or instead explodes. The implications for CSPs are as follows.

Given discount factor δ, the CSPs's value function is

$$\Pi_{j,t}(V_{j,t-1}, S_{j,t-1}) = \max_{s_{cspj,t}} \{\pi_{j,t}(\cdot) + \delta \Pi_{j,t+1}(V_{j,t}, S_{j,t})\} \tag{17}$$

This is the CSP's Bellman equation expressed in terms of the optimal value function, $\Pi_{j,t}(V_{j,t-1}, S_{j,t-1})$, current-period payoff, $\pi_{j,t} = (1-\tilde{p}(V_{j,t})C)nB(y_{i,t}) - Ks_{cspj,t}$, and discounted continuation value, $\delta\Pi_{j,t+1}(V_{j,t}, S_{j,t})$.

CSP profits decrease in vulnerability at a constant rate equal to the discounted value of the cost/benefit ratio of CSP security.

$$\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t-1}} = -\delta_V \frac{K}{\alpha} \tag{18}$$

Table 3 illustrates the impact of different levels of the marginal contribution of CSP security investment, α. The value of α impacts users' usage, users' security contribution, and CSP's security investment. Column 2 shows users' marginal benefit from the CSPs' investment increases in α. Column 3 shows users' inclination to contribute to the security umbrella decreases in α. Column 4 shows CSPs' lifetime payoff is less sensitive to vulnerability as α increases. Overall, in an environment where CSPs' marginal security contribution is higher than the users', $\alpha > 1$, both usage and vulnerability are higher.

Furthermore, as the only way a CSP can directly decrease vulnerability is by increasing security, *CSPs are in the business of providing security.* Indeed, the proof of the proposition shows a CSP's security investment only impacts its optimal value function by reducing total vulnerability. Hence, in no way can security be considered auxiliary to the CSP's core value proposition. This can be seen in that the greater a CSP's relative weight in providing shared security for the service in question, α, the less vulnerability reduces CSP profits.

Table 3: The Impact of Marginal CSP Security Contribution

α Value	$\frac{\partial u_{i,t}}{\partial s_{cspj,t}} > 0$	$\frac{\partial u^2_{i,t}}{\partial s_{i,t}\partial s_{cspj,t}} < 0$	$\frac{\partial \Pi_j}{\partial V_{j,t-1}} < 0$	Influences
$\alpha = 2$	$2b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}[\delta_V^t]$	$-2b(y_{i,t})\frac{\partial p^2(V_{j,t})}{\partial V^2_{j,t}}\delta_V^t$	$-\delta_V \frac{K}{2}$	Users are more inclined to increase usage and less inclined to contribute to the security umbrella. CSPs are less inclined to invest in security. Vulnerability increases.
$\alpha = 1$	$b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}[\delta_V^t]$	$-b(y_{i,t})\frac{\partial p^2(V_{j,t})}{\partial V^2_{j,t}}\delta_V^t$	$-\delta_V K$	The outcome on vulnerability is neutral because there is no relative difference between the marginal impact of CPS versus user contributions to the security umbrella .
$\alpha = 0.5$	$0.5b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}[\delta_V^t]$	$-0.5b(y_{i,t})\frac{\partial p^2(V_{j,t})}{\partial V^2_{j,t}}\delta_V^t$	$-2\delta_V K$	Users are less inclined to increase usage and more inclined to contribute to the security umbrella. The platform is more motivated to invest in security. Vulnerability decreases.

Note: CSPs can have amplified marginal effect on security investment from advanced security measures and promptly respond to emerging threats that lead to an $\alpha > 1$, and $\alpha < 1$ can be because CSPs' investment accelerates homogeneity that leads to correlated failure (Chen, Kataria, and Krishnan 2011). The second column shows the users' marginal benefit from CSP's investment at different α. The third column is the marginal change in the user's best reply with respect to CSP's investment. The fourth column is the constant marginal cost of vulnerability for the platform.

CSPs therefore face a tradeoff in that increased usage both increases revenues and increases vulnerability. However, unlike $\frac{\partial U_j(V_{j,t-1},S_{j,t-1})}{\partial V_{j,t-1}}$ for users, which is a function of both $V_{j,t-1}$ and $V_{j,t}$, thereby leading to an Euler equation, there is no carryover from one period to the next for $\frac{\partial \Pi_j(V_{j,t-1},S_{j,t-1})}{\partial V_{j,t-1}}$. From Proposition (4.1), vulnerability increases and builds upon itself through usage. It is of particular concern if users' path of vulnerability is explosive. Indeed, it is ultimately indicative of a potential fallacy of composition stemming from users taking shelter within the cloud. The fallacy can occur because (i) aggregate vulnerability increases over time because the cloud itself becomes the attack surface, (ii) CSPs' dynamic value function is decreasing in aggregate vulnerability, and (iii) users' dynamic value function is decreasing in aggregate vulnerability. There is a difference between individual user benefits from taking shelter in the cloud and their aggregate implications. Ultimately, cloud security depends on whether users and cloud managers have the foresight to understand the cloud is a dynamic shared security environment.

6 Conclusion

We address the growing importance of security in cloud computing services via a dynamic game of shared security in the cloud. Our analysis characterizes the optimal dynamic path of accumulated vulnerability of cloud services providers (CSPs), and CSP users' dynamic behavior (cloud usage and security investments) on this path. The results include theoretical contributions to the literature on the competitive impact of information security and extend the public good nature of cybersecurity to joint products (impure public goods). Not only does security competition affect CSP and CSP users' security investment decisions, it also changes usage decisions in lieu of their dynamic impact on CSP vulnerability. Consequently, a less-secure CSP can lock in users by providing the means for creating value under their security umbrella. The dynamics imply cloud security is an atypical form of impure public good, encouraging greater adoption and intensifying vulnerability unless CSP managers and users' managers account for the future impact of their actions.

In addition, we show how CSP security competition to keep users from switching facilitates non-monopolistic

CSP markets. For example, as shown in Table 2, AWS offers Amazon S3 Server-Side Encryption, which automatically encrypts data stored in Amazon S3, and AWS Key Management Service (KMS), and is optimized to work only with other AWS services. Google Cloud as well offers Cloud Storage Server-Side Encryption, which automatically encrypts data stored in Google Cloud Storage and Google Cloud KMS, and is designed to work seamlessly only with other Google Cloud services. The degree of switching costs resulting from lock-in also determines whether other users' security investments increase or decrease a user's payoff. Hence, dynamic and competitive considerations modify what is meant by shared security and joint responsibility in the cloud.

Our results have significant management and policy implications. The practical motivation for this study is to characterize how cloud providers compete on security and navigate the changing security environment. Cloud providers view information security from two perspectives: as a competitive advantage and an operational objective. For competition, we derive the lower bound on security investment to keep users from switching as a function of a dynamic constraint involving a CSP's past and future security investments and users' past and future usage and security decisions. From the operational perspective, cloud providers are encountering increasing security expectations and responsibilities. We provide a map for CSPs to assess and monitor their overall vulnerability. For example, providers can use surveys and experiments to understand users' risk preferences better and tailor their security offerings accordingly. When choosing a CSP managers should adopt a long-term view and consider the future possibility of switching to a different provider.

We also find CSPs will not engage in a war of increasing security levels to attract users. Nor will security competition manifest itself as a race to the bottom, a characterization that should be of interest to regulators. It is worth noting that when CSPs use security to keep users from switching, a welfare improvement results in that users are not held to reservation levels of utility. Furthermore, social planners aiming to encourage competition can view no-switching levels of security as a means for producing non-monopolistic outcomes in cloud services.

Future research directions include accommodating heterogeneous users and security standardization within a dynamic shared security environment. In terms of heterogeneity, according to Flexera's 2023 State of Cloud Report (**?**), there is an increase in the demand for cloud services across various types of organizations, including individuals, small businesses, large corporations, government agencies, non-profit organizations, and educational institutions. With respect to standardization, AWS, Palo Alto Networks, IBM, and other notable companies announced the Open Cybersecurity Schema Framework (OCSF) during the August 2022 Blackhat conference. The initiative represents a significant milestone in the advancement of cybersecurity standardization, as it aims to address the issue of tool incompatibility among security vendors. Both heterogeneity and standardization will affect impureness of the public good resulting from enhancements to the security umbrella.

A final direction is cloud security governance, such as designing mechanisms to encourage a cooperative result to improve cloud security and ensure vulnerability converges to a steady state. Our dynamic equilibrium results highlight the importance of incorporating risk preferences and cybersecurity behavior for such designs.

7 Proofs for Section 2

7.1 Proof of Proposition 3.7

Proposition 3.7 Recall

$$u_{i,t} = (1 - p(V_{j,t})c)b(y_{i,t}) - ks_{i,t} - \lambda S_{j,t-1}$$

Taking the first derivative with respect to other users' investment decision,

$$\frac{\partial u_{i,t}}{\partial s_{i',t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial s_{i',t}} - \lambda\frac{\partial S_{j,t}}{\partial s_{i',t}}$$

In a symmetric MPE equations (1) and (2) become

$$V_{j,t} = \sum_t \delta_V^t[(n-1)(y_{i',t} - s_{i',t}) + (y_{i,t} - s_{i,t}) - \alpha s_{cspj,t}]$$

$$S_{j,t} = \sum_t \delta_S^t[\alpha s_{cspj,t} + (n-1)s_{i',t} + s_{i,t}]$$

First, without switching costs ($\lambda = 0$) the first-order derivative is

$$\frac{\partial u_{i,t}}{\partial s_{i',t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial s_{i',t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}[-(n-1)\delta_V^t] > 0$$

Without switching costs, users' security investments are plain complements.

With switching costs, plain complements requires

$$\frac{\partial u_{i,t}}{\partial s_{i',t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial s_{i',t}} - \lambda\frac{\partial S_{j,t}}{\partial s_{i',t}} > 0$$

Appealing again to the expressions for $V_{j,t}$ and $S_{j,t}$ in a symmetric MPE, it becomes

$$b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\delta_V^t > \lambda\delta_S^t$$

Without switching costs, a CSP's security investment is a plain complement for users,

$$\frac{\partial u_{i,t}}{\partial s_{cspj,t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial s_{cspj,t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}[-\alpha\delta_V^t] > 0$$

With switching costs, plain complements requires

$$\frac{\partial u_{i,t}}{\partial s_{cspj,t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial s_{cspj,t}} - \lambda\frac{\partial S_{j,t}}{\partial s_{cspj,t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}[-\alpha\delta_V^t] - \lambda\frac{\partial S_{j,t}}{\partial s_{cspj,t}} > 0$$

Given $\frac{\partial S_{j,t}}{\partial s_{cspj,t}} = \delta_S^t\alpha$, this reduces to

$$b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\delta_V^t > \lambda\delta_S^t$$

The condition is the same as for other user's security investments.

7.2 Proof of Proposition 3.7

Proposition 3.7 From the proof of Proposition 3.7

$$\frac{\partial u_{i,t}}{\partial s_{i',t}} = b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}(\delta_V(n-1)) - \lambda\delta_S^t(n-1)$$

The cross derivative is

$$\frac{\partial u_{i,t}^2}{\partial s_{i,t}\partial s_{i',t}} = \frac{\partial u_{i,t}^2}{\partial s_{i',t}\partial s_{i,t}} = -b(y_{i,t})\delta_V\frac{\partial p^2(V_{j,t})}{\partial V_{j,t}^2}(\delta_V(n-1)) < 0$$

7.3 Proof of Proposition 3.7

Proposition 3.7 The first derivative is

$$\frac{\partial u_{i,t}}{\partial s_{i,t}} = -b(y_{i,t})\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial s_{i,t}} - \lambda\frac{\partial S_{j,t}}{\partial s_{i,t}}$$

The cross derivative is

$$\frac{\partial u_{i,t}^2}{\partial s_{i,t}\partial s_{cspj,t}} = b(y_{i,t})\delta_V\frac{\partial p^2(V_{j,t})}{\partial V_{j,t}^2}(-\alpha\delta^t) < 0$$

8 Proofs for Section 4

8.1 Proof of Lemma 4

Lemma 4 Following the argument in B-S, differentiating Bellman equation (8) with respect to state $V_{j,t-1}$

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}} = -cb\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial V_{j,t-1}} + \delta\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial V_{j,t-1}}$$

Given $\partial V_{j,t}/\partial V_{j,t-1} = \delta_V$,

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}} = \delta_V\left\{-cb\frac{\partial p(V_{j,t})}{\partial V_{j,t}} + \delta\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\right\}$$

Solving the best reply for $y_{i,t}$ in (10) for $\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}$ and substituting into the above equation

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}} = -\delta_V(1 - p(V_{j,t})c)b' < 0$$

8.2 Proof of Proposition 4.1

Proposition 4.1 From lemma 4, $(1 - p(V_{j,t})c)b' = -\frac{1}{\delta_V}\frac{\partial U_i(V_{t-1}, S_{t-1})}{\partial V_{j,t-1}}$. Substituting this into the first term on the right-hand side of (10) and solving for $\frac{\partial U_i(V_{t-1}, S_{t-1})}{\partial V_{j,t-1}}$ results in the Euler equation.

8.3 Proof of Proposition 4.1

Proposition 4.1 Totally differentiating equation (12) with respect to $V_{j,t}^*$:

$$\left[-cb'\frac{\partial p(V_{j,t-1}^*)}{\partial V_{j,t-1}^*} - cb\frac{\partial^2 p(V_{j,t-1}^*)}{\partial^2 V_{j,t-1}^*}\right]\frac{\partial V_{j,t-1}^*}{\partial V_{j,t}^*} = -\delta\delta_V cb'\left[\frac{\partial p(V_{j,t}^*)}{\partial V_{j,t}^*}\right]\frac{\partial V_{j,t}^*}{\partial V_{j,t}^*}$$

Given $\frac{\partial p(V_{j,t})}{\partial V_{j,t}} > 0$, $\frac{\partial p^2(V_{j,t})}{\partial V_{j,t}^2} > 0$, and rearranging terms

$$\frac{\partial V_{j,t}^*}{\partial V_{j,t-1}^*} = \frac{cb'\frac{\partial p(V_{j,t-1}^*)}{\partial V_{j,t-1}^*} + cb\frac{\partial^2 p(V_{j,t-1}^*)}{\partial^2 V_{j,t-1}^*}}{\delta\delta_V cb'\frac{\partial p(V_{j,t}^*)}{\partial V_{j,t}^*}} > 0 \tag{19}$$

All terms in the numerator and the denominator of equation (19) are positive. Hence, $\partial V_{j,t}^*/\partial V_{j,t-1}^* > 0$. This and a positive second derivative of $p(\cdot)$ implies the $\partial p(V_{j,t}^*)/\partial V_{j,t}^*$ in the denominator becomes larger. It is, therefore, possible the denominator is greater than the first term in the numerator. Hence, whether $\partial V_{j,t}^*/\partial V_{j,t-1}^* > 1$ depends on δ, δ_V, and the second term in the numerator.

8.4 Proof of Proposition 4.2

Proposition 4.2 From equations (12), the Euler equation of optimal $V^*_{j,t-1}$ and $V^*_{j,t}$ is:

$$[1 - p(V^*_{j,t-1})c]b'(y_{i,t-1}) - b(y_{i,t-1})\frac{\partial p(V^*_{j,t-1})}{\partial V^*_{j,t-1}} = \delta\delta_V[1 - p(V^*_{j,t})c]b'(y_{i,t})$$

Substituting in the components of $V^*_{j,t}$ as a function of $V^*_{j,t-1}$, $S_{j,t}$ and $y_{i,t}$, (with $y_{i',t} = y_{i,t}$ in a symmetric MPE):

$$[1 - p(V^*_{j,t-1})c]b'(y_{i,t-1}) - b(y_{i,t-1})\frac{\partial p(V^*_{j,t-1})}{\partial V^*_{j,t-1}} = \delta\delta_V[1 - p(\delta_V V^*_{j,t-1} + ny_{i,t} - S_{j,t})c]b'(y_{i,t}) \tag{20}$$

For any given value of the left-hand side of equation (20), if $S_{j,t}$ increases, $y_{i,t}$ must commensurately increase, holding all other variables constant:

$$\frac{\partial y_{i,t}}{\partial S_{j,t}} > 0$$

8.5 Proof of Proposition 4.2

Proposition 4.2

From Proposition 4.2,

$$\frac{\partial y_{i,t}}{\partial S_{j,t}} > 0$$

where $S_{j,t} \equiv nS_{i,t} + \alpha S_{cspj,t} = S_{i,t} + (n-1)S_{i',t} + \alpha S_{cspj,t}$.
Suppose the increase in $S_{j,t}$ is solely from other users. If $S_{i',t}$, $i' \neq i$ increases but $S_{i,t}$ is constant ($\Rightarrow s_{i,t} = 0$) and $S_{cspj,t}$ is constant ($\Rightarrow s_{cspj,t} = 0$) , then $v_{i,t} = y_{i,t} - s_{i,t}$ must increase because $y_{i,t}$ increases in $S_{j,t}$.

8.6 Proof of Lemma 4.3

Lemma 4.3 The rationale for this lemma and its proof is as follows. By backward induction, given the optimal $y_{i,t}$'s, from Bellman equation (8),

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial s_{i,t}} = -cb\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{i,t}}\frac{\partial S_{i,t}}{\partial s_{i,t}} - k + \delta\left[\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial S_{j,t}}\frac{\partial S_{i,t}}{\partial s_{i,t}} + \frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{i,t}}\frac{\partial S_{i,t}}{\partial s_{i,t}}\right] = 0$$

Substituting in $\frac{\partial V_{j,t}}{\partial S_{i,t}} = -1$ and $\frac{\partial S_{j,t}}{\partial s_{i,t}} = 1$:

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial s_{i,t}} = cb\frac{\partial p(V_{j,t})}{\partial V_{j,t}} - k + \delta\left[\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\right] = 0 \tag{21}$$

where $\partial U_i(V_{j,t}, S_{j,t})/\partial S_{j,t}$ is unknown. Hence, the need for the lemma.

Once again, characterizing the implicit best reply function for $s_{i,t}$ in (21) requires analyzing the Bellman equation (8) using the B-S procedure with respect to state $S_{j,t}$. Given the optimal $s_{i,t}$ from (21), differentiating Bellman equation (8) with respect to state $S_{j,t-1}$:

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = -bc\frac{\partial p(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}} - \frac{k}{n}\left(\frac{\partial S_{j,t}}{\partial S_{j,t-1}} - \delta_S\right)$$

$$+\delta\left(\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}} + \frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}}\right)$$

As $\frac{\partial S_{j,t}}{\partial S_{j,t-1}} = \delta_S$, and $\frac{\partial V_{j,t}}{\partial S_{j,t}} = -1$:

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = \delta_S bc \frac{\partial p(V_{j,t})}{\partial V_{j,t}} + \delta_S \delta \left(\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}} \right)$$

Substituting the value for $\frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial U_i(V_{j,t}, S_{j,t})}{\partial V_{j,t}}$ derived from the implicit best reply function for $s_{i,t}$ in (21) yields:

$$\frac{\partial U_i(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = \delta_S k$$

Thus proving the lemma. Upon iterating one period, it is the unknown term in first-order condition (21).

9 Proofs for Section 5

9.1 Proof of Proposition 5.1

Proposition 5.1 Given an infinite horizon, the characterizations in lemmas 1 and 2 continue to hold for all $i \in \{stay, switch\}$, where j is the relevant host CSP $j \in \{1, 2\}$:

$$\frac{\partial U_i}{\partial V_{j,t-1}} = -\delta_V [1 - p(V_{j,t})c] b', \frac{\partial^2 U_i}{\partial V_{j,t-1}^2} = \frac{\partial p(V_{j,t})}{\partial V_{j,t}} \delta_V^2 cb'$$

$$\frac{\partial U_i}{\partial S_{j,t-1}} = \delta_s k \Rightarrow \frac{\partial^2 U_i}{\partial S_{j,t-1}^2} = 0, \frac{\partial U_i}{\partial S_{j,t-1} \partial V_{j,t-1}} = 0$$

In addition, from lemma 5.1: $\frac{\partial U_{switch}}{\partial S_{1,t-1}} = -\lambda \Rightarrow \frac{\partial^2 U_{switch}}{\partial S_{1,t-1}^2} = 0$.

As U_{stay} is a function of $V_{1,t-1}, S_{1,t-1}$, and U_{switch} is a function of $V_{2,t-1}, S_{2,t-1}$ and $S_{1,t-1}$, we employ the partial derivatives expressed above in order to generate a second-order Taylor series as approximations of U_{stay} and U_{switch}. Such a quadratic approximation is appropriate because two of the second-order partials above equal zero, as does the cross-partial. Higher-order partial derivatives are equal to zero as well. Furthermore, a Taylor expansion is around zero, and $U_{stay}(0,0) = 0$, $U_{switch}(0,0,0) = 0$. It follows that the Taylor expansions are

$$U_{stay}(V_{1,t-1}, S_{1,t-1}) = \delta_s k S_{1,t-1} - \delta_V [1 - p(V_{1,t})c] b' V_{1,t-1} + \frac{1}{2} \frac{\partial p(V_{1,t})}{\partial V_{1,t}} \delta_V^2 cb' V_{1,t-1}^2 + \zeta_{stay}$$

$$U_{switch}(V_{2,t-1}, S_{2,t-1}, S_{1,t-1}) = -\lambda S_{1,t-1} + \delta_s k S_{2,t-1} - \delta_V [1 - p(V_{2,t})c] b' V_{2,t-1}$$
$$+ \frac{1}{2} \frac{\partial p(V_{2,t})}{\partial V_{2,t}} \delta_V^2 cb' V_{2,t-1}^2 + \zeta_{switch}$$

where ζ_{stay} and ζ_{switch} represent the residuals. From here on we ignore the residuals and focus on the quadratic approximations.

CSP 1 only needs to make a sufficient security investment such that the no-switching constraint is binding. Call this $S_{1,t}^{min}$ such that $U_{stay} = U_{switch}$. That is,

$$\delta_S k S_{1,t-1}^{min} - \delta_V [1 - p(V_{1,t})c] b' V_{1,t-1} + \frac{1}{2} \frac{\partial p(V_{1,t})}{\partial V_{1,t}} \delta_V^2 cb' V_{1,t-1}^2$$

$$= -\lambda S_{1,t-1}^{min} + \delta_S k S_{2,t-1} - \delta_V [1 - p(V_{2,t})c] b' V_{2,t-1} + \frac{1}{2} \frac{\partial p(V_{2,t})}{\partial V_{2,t}} \delta_V^2 cb' V_{2,t-1}^2$$

$$S_{1,t-1}^{\min} = \frac{1}{\lambda} \{ \delta_S k (S_{2,t-1} - S_{1,t-1}^{\min}) - \delta_V b' \{ [1 - p(V_{2,t})c] V_{2,t-1} - [1 - p(V_{1,t})c] V_{1,t-1} \}$$

$$+\frac{1}{2}\frac{\partial p(V_{2,t})}{\partial V_{2,t}}\delta_V^2 cb' V_{2,t-1}^2 - \frac{1}{2}\frac{\partial p(V_{1,t})}{\partial V_{1,t}}\delta_V^2 cb' V_{1,t-1}^2\}$$

this is the expression for $S_{1,t-1}^{min}$ given in Proposition 5.1.

We now turn to the claim that the no-switching condition can hold even when $S_{1,t-1} < S_{2,t-1}$ and $V_{1,t-1} > V_{2,t-1}$. Pulling all $S_{1,t-1}^{min}$ terms to the left-hand side of the above equality:

$$\left(1+\frac{1}{\lambda}\delta_S k\right) S_{1,t-1}^{\min} = \frac{1}{\lambda}\delta_S k S_{2,t-1} - \frac{1}{\lambda}\{\delta_V b'\{[1-p(V_{2,t})c]V_{2,t-1} - [1-p(V_{1,t})c]V_{1,t-1}\}$$
$$+\frac{1}{2\lambda}\frac{\partial p(V_{2,t})}{\partial V_{2,t}}\delta_V^2 cb' V_{2,t-1}^2 - \frac{1}{2\lambda}\frac{\partial p(V_{1,t})}{\partial V_{1,t}}\delta_V^2 cb' V_{1,t-1}^2 \tag{22}$$

Since $p'(V_{j,t}) > 0$ and $p''(V_{j,t}) > 0$ and we assume $V_{2,t-1} < V_{1,t-1}$:

$$\Omega = \frac{1}{2\lambda}\frac{\partial p(V_{2,t})}{\partial V_{2,t}}\delta_V^2 cb' V_{2,t-1}^2 - \frac{1}{2\lambda}\frac{\partial p(V_{1,t})}{\partial V_{1,t}}\delta_V^2 cb' V_{1,t-1}^2 < 0$$

If we assume $1 - p'(V_{j,t})\delta_V c < 0$,[6]

$$\Psi = -\frac{1}{\lambda}\{\delta_V b'\{[1-p(V_{2,t})c]V_{2,t-1} - [1-p(V_{1,t})c]V_{1,t-1}\} < 0$$

Then the above expression for $S_{1,t-1}^{min}$ in (25) can be written as:

$$\left(1+\frac{1}{\lambda}\delta_S k\right) S_{1,t-1}^{\min} = \frac{1}{\lambda}\delta_S k S_{2,t-1} + \underbrace{[\Psi+\Omega]}_{(-)} \tag{23}$$

For this to hold it must be the case that $S_{1,t-1}^{\min} < S_{2,t-1}$

9.2 Proof of Proposition 5.1

$$\left(1+\frac{1}{\lambda}\delta_S k\right) S_{1,t-1}^{\min} = \frac{1}{\lambda}\delta_S k S_{2,t-1} - \frac{1}{\lambda}\delta_V b'\{[1-p(V_{2,t})c]V_{2,t-1} - [1-p(V_{1,t})c]V_{1,t-1}\}$$
$$+\frac{1}{2\lambda}\frac{\partial p(V_{2,t})}{\partial V_{2,t}}\delta_V^2 cb' V_{2,t-1}^2 - \frac{1}{2\lambda}\frac{\partial p(V_{1,t})}{\partial V_{1,t}}\delta_V^2 cb' V_{1,t-1}^2 \tag{24}$$

$$S_{1,t-1}^{\min} = \frac{1}{(\lambda+\delta_S k)}\{\delta_S k S_{2,t-1} - \delta_V b'\{[1-p(V_{2,t})c]V_{2,t-1} - [1-p(V_{1,t})c]V_{1,t-1}\}$$
$$+\frac{1}{2}\frac{\partial p(V_{2,t})}{\partial V_{2,t}}\delta_V^2 cb' V_{2,t-1}^2 - \frac{1}{2}\frac{\partial p(V_{1,t})}{\partial V_{1,t}}\delta_V^2 cb' V_{1,t-1}^2\} \tag{25}$$

9.3 Proof of Proposition 5.1

The no-switching condition in equation (25) can be written as a function of participation constraints (15) and (16),

$$\left(1+\frac{1}{\lambda}\delta_S k\right) S_{1,t-1}^{\min} = \frac{1}{\lambda}\delta_S k S_{2,t-1}^{pc} + \frac{1}{\lambda}\delta_S k S_{1,t-1}^{pc} \tag{26}$$

[6] Recall $\delta_V, c \in (0,1)$.

By symmetry, if users of CSP 1's participation constraint is met, it is met for users of CSP 2 as well. It follows that $S^{pc}_{2,t-1} = S^{pc}_{1,t-1}$. Substituting into equation (26):

$$\left(1 + \frac{1}{\lambda}\delta_S k\right) S^{\min}_{1,t-1} = \frac{2}{\lambda}\delta_S k S^{pc}_{1,t-1}$$

We can see $S^{\min}_{1,t-1} < S^{pc}_{1,t-1}$ if:

$$1 + \frac{1}{\lambda}\delta_S k > \frac{2}{\lambda}\delta_S k$$

which is:

$$\lambda > \delta_S k$$

The left hand is the per-unit marginal cost of accumulated security for users because of the lock-in effect. The right hand is the depreciation speed of security investment times the per-unit cost of security investment for users. And from lemma 1, it is the marginal benefit of accumulated security for users.

10 Proof of Proposition 5.2

By backward induction, given the optimal $y_{i,t}$ and optimal $s_{i,t}$:

$$\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial s_{cspj,t}} = -CnB\frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{cspj,t}}\frac{\partial S_{cspj,t}}{\partial s_{cspj,t}} - K$$

$$+\delta\left[\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial s_{cspj,t}} + \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{cspj,t}}\frac{\partial S_{cspj,t}}{\partial s_{cspj,t}}\right] = 0$$

Substituting in $\frac{\partial V_{j,t}}{\partial S_{cspj,t}} = -\alpha$, $\frac{\partial S_{j,t}}{\partial s_{cspj,t}} = \alpha$, and $\frac{\partial S_{cspj,t}}{\partial s_{cspj,t}} = 1$:

$$\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial s_{cspj,t}} = CnB\alpha\frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} - K + \delta\alpha\left[\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\right] = 0 \tag{27}$$

where $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}}$ and $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}}$ are unknowns.

At the optimum the term in brackets takes the value

$$\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}} = \frac{K}{\delta\alpha} - \frac{CnB}{\delta}\frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} \tag{28}$$

While it is asserted $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}}$ is an unknown, in actuality $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}} = 0$ because, as we argue in the text, by the process of backward induction, once the CSP selects it's $s_{cspj,t}$ there are no degrees of freedom left for determining $S_{j,t}$. Selecting $s_{cspj,t}$ is equivalent to selecting $S_{j,t}$ and, at the optimum, $\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial s_{cspj,t}} = 0$. For purposes of completeness, we prove $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}} = 0$. Once this is established, equation (28) is used to solve for $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}}$ along the optimal path.

Employing the B-S procedure by differentiating (17) with respect to state $S_{j,t-1}$:

$$\frac{\partial \Pi_i(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = -CnB\frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}} - K\frac{\partial s_{cspj,t}}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}}$$

$$+\delta\left[\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}} + \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}}\frac{\partial V_{j,t}}{\partial S_{j,t}}\frac{\partial S_{j,t}}{\partial S_{j,t-1}}\right]$$

Directly differentiating, $\frac{\partial S_{j,t}}{\partial S_{j,t-1}} = \delta_S$, $\frac{\partial V_{j,t}}{\partial S_{j,t}} = -1$ and $\frac{\partial S_{j,t}}{\partial s_{cspj,t}} = \alpha$, which is a constant. Hence, by the inverse function rule for partial differentiation, $\frac{\partial s_{cspj,t}}{\partial S_{j,t}} = \frac{1}{\alpha}$. The above equation becomes

$$\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = \delta_S CnB \frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} - \frac{\delta_S}{\alpha} K + \delta_S \delta \left[\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}} \right]$$

Substituting in the value, $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}} - \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}} = \frac{K}{\delta\alpha} - \frac{CnB}{\delta} \frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}}$, from equation (28),

$$\frac{\partial \Pi_i(V_{j,t-1}, S_{j,t-1})}{\partial S_{j,t-1}} = 0$$

That is, our intuition with respect to $\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial s_{cspj,t}}$ and $\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial S_{j,t}}$ at the optimum holds. A CSP's security investment only impacts its optimal value function by reducing total vulnerability. Substituting this value into equation (28),

$$\frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}} = \frac{1}{\delta} \left[CnB \frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} - \frac{K}{\alpha} \right] \tag{29}$$

Returning again to the B-S procedure,

$$\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}} = -CnB \frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} \frac{\partial V_{j,t}}{\partial V_{j,t-1}} + \delta \frac{\partial \Pi_j(V_{j,t}, S_{j,t})}{\partial V_{j,t}} \frac{\partial V_{j,t}}{\partial V_{j,t-1}}$$

Substituting in $\frac{\partial V_{j,t}}{\partial V_{j,t-1}} = \delta_V$ and the value from equation (29),

$$\frac{\partial \Pi_j(V_{j,t-1}, S_{j,t-1})}{\partial V_{j,t-1}} = -CnB \frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} \delta_V + \delta \frac{1}{\delta} CnB \frac{\partial \tilde{p}(V_{j,t})}{\partial V_{j,t}} \delta_V - \frac{1}{\delta} \frac{K}{\alpha} \delta_V \delta = -\delta_V \frac{K}{a}$$

References

Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Leon PG, Sadeh N, Schaub F, Sleeper M, et al. (2017) Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50(3):1–41.

Al-Otaibi YD (2021) A shared two-way cybersecurity model for enhancing cloud service sharing for distributed user applications. *ACM Transactions on Internet Technology (TOIT)* 22(2):1–17.

Almorsy M, Grundy J, Müller I (2016) An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107* .

Anderson R (2001) *Security engineering: a guide to building dependable distributed systems* (John Wiley & Sons).

Arce DG (2018) Malware and market share. *Journal of Cybersecurity* 4(1), ISSN 2057-2085 2057-2093, URL `http://dx.doi.org/10.1093/cybsec/tyy010`.

Arce DG (2020) Cybersecurity and platform competition in the cloud. *Computers & Security* 93, ISSN 01674048, URL `http://dx.doi.org/10.1016/j.cose.2020.101774`.

Arce DG (2022) Security-induced lock-in in the cloud. *Business & Information Systems Engineering* 64(4):501–513.

Asghari H, van Eeten M, Bauer JM (2016) Economics of cybersecurity. *Handbook on the Economics of the Internet* (Edward Elgar Publishing).

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

Benveniste LM, Scheinkman JA (1979) On the differentiability of the value function in dynamic models of economics. *Econometrica: Journal of the Econometric Society* 727–732.

Blackwell D (1965) Discounted dynamic programming. *The Annals of Mathematical Statistics* 36(1):226–235.

Blumenthal MS (2011) Is security lost in the clouds? *Communications and Strategies* (81):69–86.

Buchholz W, Sandler T (2021) Global public goods: a survey. *Journal of Economic Literature* 59(2):488–545.

Cansever D (2020) Security games with insider threats. *International Conference on Decision and Game Theory for Security*, 502–505 (Springer).

Cavusoglu H, Raghunathan S, Yue WT (2014) Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems* 25(2):281–304, ISSN 0742-1222 1557-928X, URL `http://dx.doi.org/10.2753/mis0742-1222250211`.

Chen Py, Kataria G, Krishnan R (2011) Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly* 35(2):397–422, URL `http://dx.doi.org/https://aisel.aisnet.org/misq/vol35/iss2/9/`.

Crowdstrike (2023) 2023 cloud risk report. Technical report, Crowdstrike.

Dechert WD (1997) Non cooperative dynamic games: a control theoretic approach. *Unpublished. Available on request to the author* .

Dutta A, Sanyal P (2023) Examining the effects of virtual work on cybersecurity behavior .

Eaton B (2002) *Applied Microeconomic Theory: Selected Essays of B. Curtis Eaton* (Edward Elgar), ISBN 978-1-85898-650-0, URL `https://books.google.com/books?id=0UfgwAEACAAJ`.

Fedele A, Roner C (2022) Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys* 36(1):157–187.

Florêncio D, Herley C (2013) Where do all the attacks go? *Economics of information security and privacy III*, 13–33 (Springer).

Friedman JW (1976) *Oligopoly and the Theory of Games*, volume 8 (North-Holland).

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

Gariba ZP, Van Der Poll JA (2017) Security failure trends of cloud computing. *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, 247–256 (IEEE).

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

Gordon LA, Loeb MP (2002) The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)* 5(4):438–457.

Haurie A, Krawczyk JB, Zaccour G (2012) *Games and dynamic games*, volume 1 (World Scientific Publishing Company).

Hausken K (2002) Probabilistic risk analysis and game theory. *Risk Analysis* 22(1):17–27.

Hedlund J (2000) Risky business: safety regulations, risk compensation, and individual behavior. *Injury prevention* 6(2):82–89.

IBM (2023) Cost of a data breach. Technical report, IBM Security.

Josa-Fombellida R, Rincón-Zapatero JP (2008) Markov perfect nash equilibrium in stochastic differential games as solution of a generalized euler equations system .

Lee RS (2014) Competing platforms. *Journal of Economics & Management Strategy* 23(3):507–526.

Lookabaugh T, Sicker DC (2004) Security and lock-in. *Economics of information security*, 225–246 (Springer).

McKay A, Nakamura E, Steinsson J (2017) The discounted euler equation: A note. *Economica* 84(336):820–831.

O'Donnell AJ (2008) When malware attacks (anything but windows). *IEEE Security & Privacy* 6(3):68–70.

Olson's M (1965) *The Logic of Collective Action: Public Goods and the Theory of Groups*, volume 124 (Harvard University Press).

Opara-Martins J, Sahandi R, Tian F (2014) Critical review of vendor lock-in and its impact on adoption of cloud computing. *International Conference on Information Society (i-Society 2014)*, 92–97 (IEEE).

Opara-Martins J, Sahandi R, Tian F (2016) Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing* 5(1):1–18.

Palo Alto Networks (2023) Unit 42 attack surface threat report. Technical report, $\text{Palo}_A lto_N etworks$.

Ponemon Institute (2014) Data breach: The cloud multiplier effect. Technical report, Ponemon Institute.

Safi R, Browne GJ (2023) Detecting cybersecurity threats: The role of the recency and risk compensating effects. *Information Systems Frontiers* 25(3):1277–1292.

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

Shapiro C, Varian HR (1998) *Information rules: A strategic guide to the network economy* (Harvard Business Press).

Tajalizadehkhoob S, Van Goethem T, Korczyński M, Noroozian A, Böhme R, Moore T, Joosen W, van Eeten M (2017) Herding vulnerable cats: a statistical approach to disentangle joint responsibility for web security in shared hosting. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 553–567.

Tianfield H (2012) Security issues in cloud computing. *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 1082–1089 (IEEE).

Tilley A, McMillan R (2022) Microsoft's new security chief says it is time to take shelter in the cloud. *Wall Street Journal* B1.

Torkura KA, Sukmana MI, Cheng F, Meinel C (2021) Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security* 102:102124.

Varian HR (2004) Competition and market power. *The Economics of Information Technology: An Introduction* 1–47.

Vasek M, Wadleigh J, Moore T (2015) Hacking is not random: a case-control study of webserver-compromise risk. *IEEE Transactions on Dependable and Secure Computing* 13(2):206–219.

Wilms K, Stieglitz S, Mäller B (2018) Feeling safe on a fluffy cloud: How cloud security and commitment affect users switching intention. *Proceedings of the Thirty Ninth Conference on Information Systems*.

Wiz (2023) 2023 state of the cloud. Technical report, Wiz.

Zhang Z, Nan G, Tan Y (2020) Cloud services vs. on-premises software: Competition under security risk and product customization. *Information Systems Research* 31(3):848–864.

References

Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Leon PG, Sadeh N, Schaub F, Sleeper M, et al. (2017) Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50(3):1–41.

Al-Otaibi YD (2021) A shared two-way cybersecurity model for enhancing cloud service sharing for distributed user applications. *ACM Transactions on Internet Technology (TOIT)* 22(2):1–17.

Almorsy M, Grundy J, Müller I (2016) An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107* .

Anderson R (2001) *Security engineering: a guide to building dependable distributed systems* (John Wiley & Sons).

Arce DG (2018) Malware and market share. *Journal of Cybersecurity* 4(1), ISSN 2057-2085 2057-2093, URL `http://dx.doi.org/10.1093/cybsec/tyy010`.

Arce DG (2020) Cybersecurity and platform competition in the cloud. *Computers & Security* 93, ISSN 01674048, URL `http://dx.doi.org/10.1016/j.cose.2020.101774`.

Arce DG (2022) Security-induced lock-in in the cloud. *Business & Information Systems Engineering* 64(4):501–513.

Asghari H, van Eeten M, Bauer JM (2016) Economics of cybersecurity. *Handbook on the Economics of the Internet* (Edward Elgar Publishing).

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

Benveniste LM, Scheinkman JA (1979) On the differentiability of the value function in dynamic models of economics. *Econometrica: Journal of the Econometric Society* 727–732.

Blackwell D (1965) Discounted dynamic programming. *The Annals of Mathematical Statistics* 36(1):226–235.

Blumenthal MS (2011) Is security lost in the clouds? *Communications and Strategies* (81):69–86.

Buchholz W, Sandler T (2021) Global public goods: a survey. *Journal of Economic Literature* 59(2):488–545.

Cansever D (2020) Security games with insider threats. *International Conference on Decision and Game Theory for Security*, 502–505 (Springer).

Cavusoglu H, Raghunathan S, Yue WT (2014) Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems* 25(2):281–304, ISSN 0742-1222 1557-928X, URL `http://dx.doi.org/10.2753/mis0742-1222250211`.

Chen Py, Kataria G, Krishnan R (2011) Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly* 35(2):397–422, URL `http://dx.doi.org/https://aisel.aisnet.org/misq/vol35/iss2/9/`.

Crowdstrike (2023) 2023 cloud risk report. Technical report, Crowdstrike.

Dechert WD (1997) Non cooperative dynamic games: a control theoretic approach. *Unpublished. Available on request to the author* .

Dutta A, Sanyal P (2023) Examining the effects of virtual work on cybersecurity behavior .

Eaton B (2002) *Applied Microeconomic Theory: Selected Essays of B. Curtis Eaton* (Edward Elgar), ISBN 978-1-85898-650-0, URL `https://books.google.com/books?id=0UfgwAEACAAJ`.

Fedele A, Roner C (2022) Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys* 36(1):157–187.

Florêncio D, Herley C (2013) Where do all the attacks go? *Economics of information security and privacy III*, 13–33 (Springer).

Friedman JW (1976) *Oligopoly and the Theory of Games*, volume 8 (North-Holland).

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

Gariba ZP, Van Der Poll JA (2017) Security failure trends of cloud computing. *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, 247–256 (IEEE).

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

Gordon LA, Loeb MP (2002) The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)* 5(4):438–457.

Haurie A, Krawczyk JB, Zaccour G (2012) *Games and dynamic games*, volume 1 (World Scientific Publishing Company).

Hausken K (2002) Probabilistic risk analysis and game theory. *Risk Analysis* 22(1):17–27.

Hedlund J (2000) Risky business: safety regulations, risk compensation, and individual behavior. *Injury prevention* 6(2):82–89.

IBM (2023) Cost of a data breach. Technical report, IBM Security.

Josa-Fombellida R, Rincón-Zapatero JP (2008) Markov perfect nash equilibrium in stochastic differential games as solution of a generalized euler equations system .

Lee RS (2014) Competing platforms. *Journal of Economics & Management Strategy* 23(3):507–526.

Lookabaugh T, Sicker DC (2004) Security and lock-in. *Economics of information security*, 225–246 (Springer).

McKay A, Nakamura E, Steinsson J (2017) The discounted euler equation: A note. *Economica* 84(336):820–831.

O'Donnell AJ (2008) When malware attacks (anything but windows). *IEEE Security & Privacy* 6(3):68–70.

Olson's M (1965) *The Logic of Collective Action: Public Goods and the Theory of Groups*, volume 124 (Harvard University Press).

Opara-Martins J, Sahandi R, Tian F (2014) Critical review of vendor lock-in and its impact on adoption of cloud computing. *International Conference on Information Society (i-Society 2014)*, 92–97 (IEEE).

Opara-Martins J, Sahandi R, Tian F (2016) Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing* 5(1):1–18.

Palo Alto Networks (2023) Unit 42 attack surface threat report. Technical report, $\text{Palo}_{A}lto_{N}etworks$.

Ponemon Institute (2014) Data breach: The cloud multiplier effect. Technical report, Ponemon Institute.

Safi R, Browne GJ (2023) Detecting cybersecurity threats: The role of the recency and risk compensating effects. *Information Systems Frontiers* 25(3):1277–1292.

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

Shapiro C, Varian HR (1998) *Information rules: A strategic guide to the network economy* (Harvard Business Press).

Tajalizadehkhoob S, Van Goethem T, Korczyński M, Noroozian A, Böhme R, Moore T, Joosen W, van Eeten M (2017) Herding vulnerable cats: a statistical approach to disentangle joint responsibility for web security in shared hosting. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 553–567.

Tianfield H (2012) Security issues in cloud computing. *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 1082–1089 (IEEE).

Tilley A, McMillan R (2022) Microsoft's new security chief says it is time to take shelter in the cloud. *Wall Street Journal* B1.

Torkura KA, Sukmana MI, Cheng F, Meinel C (2021) Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security* 102:102124.

Varian HR (2004) Competition and market power. *The Economics of Information Technology: An Introduction* 1–47.

Vasek M, Wadleigh J, Moore T (2015) Hacking is not random: a case-control study of webserver-compromise risk. *IEEE Transactions on Dependable and Secure Computing* 13(2):206–219.

Wilms K, Stieglitz S, Mäller B (2018) Feeling safe on a fluffy cloud: How cloud security and commitment affect users switching intention. *Proceedings of the Thirty Ninth Conference on Information Systems.*

Wiz (2023) 2023 state of the cloud. Technical report, Wiz.

Zhang Z, Nan G, Tan Y (2020) Cloud services vs. on-premises software: Competition under security risk and product customization. *Information Systems Research* 31(3):848–864.