Title

How Customer Demand Reactions Impact Technology Innovation and Security

Journal

ACM Transactions on Management Information Systems, 13(3)

ISSN

2158-656X

Authors

Yeo, M Lisa
Rolland, Erik
Ulmer, Jacquelyn Rees
et al.

Publication Date

2022-09-30

DOI

10.1145/3505227

Peer reviewed

How Customer Demand Reactions Impact Technology Innovation and Security

M. LISA YEO, University of California, Merced
ERIK ROLLAND, CalPoly Pomona
JACQUELYN REES ULMER, Ohio University
RAYMOND A. PATTERSON, Haskayne School of Business, University of Calgary

Innovation is a very important concern for both managers and governmental policy makers. There is an important interplay between security and technology innovation that is largely unrecognized in the literature. This research considers the case where technology innovation in the form of additional product features increases demand through greater functionality. However, the likelihood of a security breach increases with the number of product features as the features interact in unintended ways, thereby increasing the attack surface. Using a two-stage game, we demonstrate how potential demand changes (from direct risk or externalities) impact firm technology innovation strategy. The analysis shows that the type and extent of customer demand reaction has a significant impact on innovative feature development. This research identifies two potential impacts on the level of innovation that can be strategically managed - the impact of externalities on demand and industry risk - explaining how these forces alter the level of innovation in the product ecosystem. Additionally, high-security development is disincentivized, and leads to a type of competitive behavior where the opportunity window for high-security development for all firms is small.

CCS Concepts: • **Security and privacy → Economics of security and privacy;**

Additional Key Words and Phrases: Innovation, risk, game theory, direct-risk, externalities, security breach

ACM Reference format:
M. Lisa Yeo, Erik Rolland, Jacquelyn Rees Ulmer, and Raymond A. Patterson. 2022. How Customer Demand Reactions Impact Technology Innovation and Security. *ACM Trans. Manage. Inform. Syst.* 13, 3, Article 32 (April 2022), 17 pages.
https://doi.org/10.1145/3505227

1 INTRODUCTION

Innovation is a topic of great interest, and most of the discussion in the literature focuses on how an organization can increase their level of product or service innovation. This paper is not about what enables an organization to be more innovative than others, or how organizations can enhance their level of innovation. Rather, this paper uses a game-theoretic economic model to examine market forces related to security risks potentially leading to security breaches inherent in

Authors' addresses: M. Lisa Yeo, School of Engineering, University of California, Merced, 5200 N. Lake Rd., Merced, CA, 95340, US; email: lyeo2@umcermced.edu; E. Rolland, College of Business Administration, Cal Poly Pomona, 3801 West Temple Ave., Pomona, CA 91768, US; email: erolland@cpp.edu; J. Rees Ulmer, College of Business, Ohio University, 1 Ohio University Dr., Athens OH 45701, US; email: reesulmer@ohio.edu; R. A. Patterson, Haskayne School of Business, University of Calgary, 2500 University Dr. NW, Calgary, AB T2N 1N4, CA; email: raymond.patterson@ucalgary.ca.

2158-656X/2022/04-ART32
https://doi.org/10.1145/3505227

product innovation. This paper establishes our understanding of the impact of differing customer demand reactions to security breaches on feature innovation. We show that conditions under security breaches can either increase or decrease product demand and levels of product innovation in the market. The economic models presented in this paper can help firms better target innovation investments in the presence of ever-increasing security risks. Additionally, this paper establishes a baseline understanding of the influence of market risks on innovation for governmental policy makers tasked with overseeing security risks, including those around intentional or unintentional privacy breaches, without negatively impacting industry innovation.

Innovation is seen as a way to create value [10, 16]. Currently, embedding advanced technology features in products is seen as an important way to innovate. For example, Ostrovsky and Schwarz [23] imagine a future that relies on real-time decision making in an automated sensor network to track vehicle positioning and flow which, when coupled with self-driving cars, offer a real way to reduce traffic congestion. However, such an integrated system also means that every vehicle, and presumably every driver, would be completely track-able. This scenario could open the door for attackers to disrupt traffic systems and lead to injuries and even loss of life. In a less alarming, yet no less concerning scenario, individual vehicles and occupants could be tracked without permission, leading to potential privacy violations. Innovation in products, through the increase in product software features, increases the complexity of the system. This complexity creates room for unintentional errors and software defects, potentially creating software vulnerabilities in such systems. These vulnerabilities represent a portion of potential security risks for these products, along with more traditional security risks, such as malware. When attackers successfully exploit these vulnerabilities, security breaches are the result, which could result in data loss or other harm. Many countries, and most US states, have data breach notification laws, which require companies to notify victims of data breaches. These notification laws require firms to assume the expense of both recovering from the attack as well as notifying affected stakeholders. Companies might be also subject to lawsuits and other regulatory action. Regulation such as the European Union's **General Data Protection Regulation (GDPR)** has taken the approach of punishing companies that are victims of attack with heavy fines [19]. This "stick" type of regulation can reasonably be expected to further dampen service and product innovation.

Innovative change is characterized as a process of movement through three overlapping stages, which includes more than just the innovation itself: invention, the innovation itself, and diffusion [4, 18]. Within this framework, an invention is some artifact or idea that could have economic value, whereas innovation is the process by which inventions become usable. The last stage, diffusion, is the spread of capacity to use or take advantage of an innovation. Hamel [10] posits that innovation is a driver of organizational competitiveness. Indeed, innovation through technology is often viewed as a primary mechanism for newcomers to succeed despite their resource disadvantage, but innovation with technology can also be a way for incumbents to renew their success.

The more complex the project or service, the more difficult innovation becomes. Sharma et al. [26] demonstrate that supply chain innovation exhibits a diminishing return, which is consistent with the idea that the more complex something is, the less marginal impact each additional innovation will have on desired outcomes. Modularizing product design is one method that has been used to manage the impact of product complexity on innovation [27]. In terms of technology adoption in general, complexity, or perceived complexity, has long been viewed as an inhibitory factor [11, 28, 34, 35]. However, software complexity is also known to exacerbate security issues [1]. The adoption of IS security measures involves both the firm that develops the innovation and the customer who must assimilate that innovation into their activities, where higher **information system (IS)** security complexity inhibits adoption [9]. Nelson and Madnick [21] find that strong

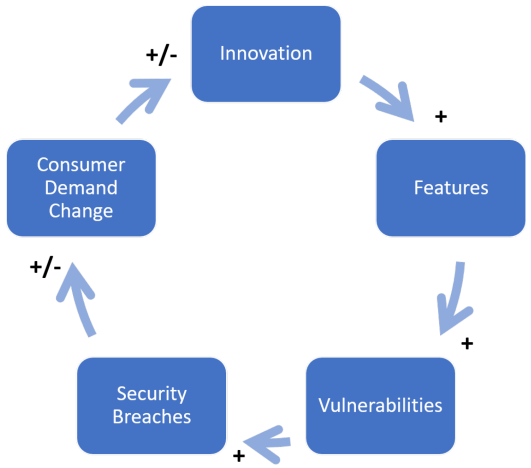


Fig. 1. The innovation - security breach cycle.

cybersecurity creates a natural tension with the value derived from innovation and excessive risk required to obtain the innovation.

Is there evidence in the literature that consumers change demand behaviour as the result of a cyber security breach? Wang et al. [30] find that users seek out information security-related knowledge when cyber-attacks occur, and they point out that people react similarly to both physical and cyber attacks. A logical extension is to ask whether users might act on this information and change purchasing behavior. Jeong et al. [13] perform an event study that provides evidence for the assertion that information security breaches do in fact affect the stock price in **information technology (IT)** intensive industries where a very strong competition effect was found. We assert that stock price changes should reflect investor expectations of consumer demand changes. Zafar et al. [33] found that breaches affect the financial performance of other firms that were not breached, indicating that market externalities exist when IS security breaches occur. Wang et al. [31] show that IT security investments made prior to a security breach dampen the negative stock price impact of the breach. They also showed that when the specific breach was anticipated by the attacked firm, as shown by the 10K disclosures, the stock market reaction was minimal. Thus, we find strong evidence in the literature of a relationship between IS security investments and stock prices, which imply a consumer reaction to security breaches.

Combining these concepts, we assert a relationship between innovation, product features, and vulnerabilities. That is, innovation is manifested as additional features which increase complexity. The increased complexity then leads to opportunity for security breaches as noted above. Figure 1 illustrates the innovation-security breach cycle, where an innovation is turned into product or service features which create security vulnerabilities. These vulnerabilities are exploited and the result is a security breach which impacts consumer demand.

An illustrative example of the innovation-security trade-off can be seen in the mobile phone platform ecosystems, such as Google Play and the Apple App Store. These systems are based on distinct mobile phone operating systems: Android and iOS, respectively. For the Android open operating systems platform, smartphone manufacturers and resellers may modify or extend the system to add functionality. Wu et al. [32] analyzed this common practice of vendors tailoring the Android operating system to their smartphone handsets; such modifications come at a security cost in that an average of about 86% of all preloaded apps are over-privileged. An over-privileged app over-shares with

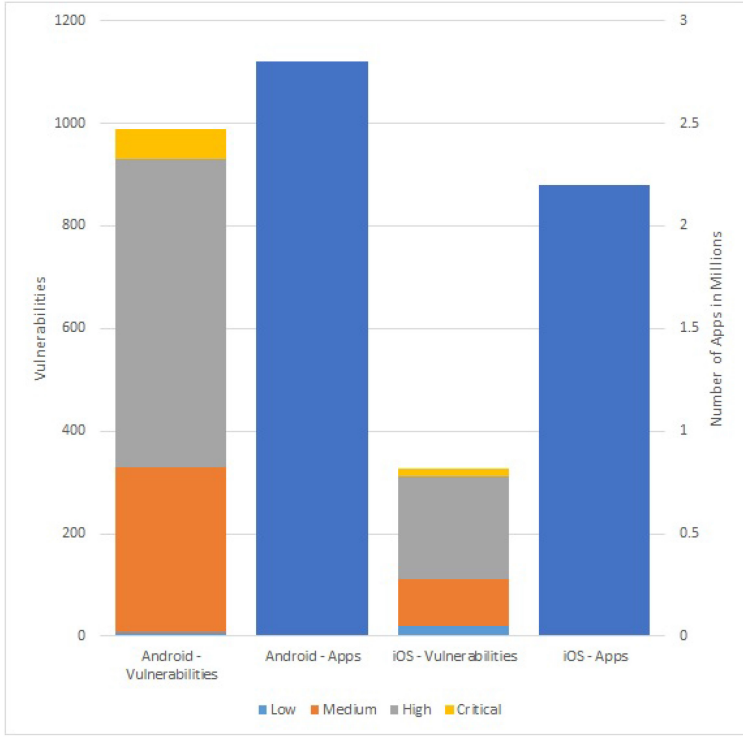


Fig. 2. Comparison of vulnerabilities discovered (May 1, 2016-Apr. 30, 2017) and total Apps available (as of Sept 30, 2017) for Android and iOS devices.

third parties, thereby violating consumer privacy expectations [24]. Foerderer [7] investigated the impact of interfirm interchange among Apple developers on complementary innovation. In addition, the majority of the vulnerabilities found (65–85%) stemmed from vendor customization, and it was found that newer smartphone models are not necessarily more secure than older models [32].

Using data from the National Vulnerability Database [22], we verify that the relative rate of vulnerability discovery is higher for Android than iOS (Figure 2). Figure 2 summarizes the vulnerabilities discovered in the 12 months ending April 30, 2017 based on the National Vulnerability Database [22]. The number of Apps in the figure are as of September 30, 2017. Unsurprisingly, we see that there are more apps available for Android devices, and thus more functionality and implicit innovation. A higher relative rate of vulnerability discovery for the system with more features (i.e., Android) would imply that the excess vulnerabilities in Android could be the result of additional interaction complexities between additional features. Our observations regarding Android versus iOS are not proof of the existence of the innovation-security tradeoff, but rather provide only circumstantial evidence.

The above observations, combined with the reality of finite development time, mean firms face important trade-offs regarding feature development, testing, and security [3, 5]. Since features offer a salient value proposition while security does not, there is an unsurprising tendency to rush products to market before they are fully tested and secured. Even when software firms offer regular updates and patching, their customers often have a difficult task of keeping systems updated in a timely manner [12]. Additionally, we could think of time-to-market relative to a competitor as yet another feature of innovation, at least in terms of how customers react to early availability. Shorter time-to-market would be expected to increase the number of vulnerabilities.

One way of creating innovation with technology is to add features to a technology product, website, or other artifact. Using the vehicle example from above, a unique innovation contributing to Tesla's success is their ability to upload "over-the-air software" with post-production innovations such as self-driving features and range expansion to older vehicles [6]. This innovation has increased the longevity and performance of Tesla's older model electric cars. Lyytinen and Rose [17] shows that technology-enabled innovation can be related to the product, service, organization and market. With the advances in platform technologies [2], rapid diffusion has been made possible, further increasing the rate of innovation at every level. Artificial intelligence tools and big data have enabled innovative insurance products where insurers can more accurately categorize risk, pricing products more appropriately, but also introducing concerns regarding security, and therefore privacy, of user data [14]. We make the assumption for the purposes of this research that there is no privacy without security. Integrated autonomous vehicles, geolocation systems, and road sensors have the ability to improve transportation [23] while introducing serious security and privacy implications.

Software vendors have been credibly accused of pushing additional features quickly to customers at the cost of decreased security in their software [25, 29]. Additionally, some features that add functionality do so at the explicit cost of privacy. The discovery of previously undisclosed collection or use of personal data in excess of what the user expects can indeed be construed as a security breach.

This tunnel vision on additional features results in an increased number of vulnerabilities remaining within the source code of the consumer software. As developers have finite time to introduce features and perform testing on those new features, vendors make explicit trade-offs between functionality, ease of use, and security [3, 5]. Websites also experience this explicit innovation-security tradeoff. However, there is evidence of customer push-back when the potential downside is too great. For example, in website contexts for which users have higher privacy concerns, firms reduce their reliance on third-party providers of website functionality; Gopal et al. [8] find lower utilization of third party providers for website functionality when users experience higher privacy concerns. Thus, we observe a need for a firm to balance investments in features, the security of those features, and the customer demand reaction to both.

In this paper, we utilize analytic modeling to examine the Innovation-Security Breach Cycle. The contribution of this paper is to understand how innovation is influenced by user security concerns and adverse events such as security breaches. Under market conditions where user security concerns impact demand, higher levels of innovation observed in more competitive market segments are shown to be impacted by user security concerns manifested through differing customer demand reactions to security breaches as a mechanism that causes more or less innovation. Security concerns are shown to impact the level of innovation in services or products with embedded software technology. In doing so, we recognize differing consumer demand reactions to security violations, and we focus on how these differing reactions may impact the level of innovation in product and service design. An assumption of this paper is the law of unintended consequences [20] as it relates to complex technology-enabled product and service design: more interaction between more features create more opportunities for adverse events related to service and product safety which we consider to be security breaches. Because software technology is often the source of innovative features, we ask "How do firms balance the benefits of innovation versus their unintended consequences?"

2 MODEL

We consider the case where additional product features increase demand through greater functionality. The likelihood of a security breach increases with the number of product features as the

Table 1. Parameters and Decision Variables

Parameter	Definition
z_i	Level of investment in features for firm i, $z_i \geq 0, i = 1, 2$ (decision variable).
κ_i	Decision by firm i to be a low ($\kappa_i = 0$) or high ($\kappa_i = 1$) security developer.
Γ	Set of joint security development types. $\Gamma = \{LL, LH, HL, HH\}$
γ	A joint security development type. $\gamma \in \Gamma$
S	Set of joint firm states. $S = \{gg, gb, bg, bb\}$
s	A joint firm state. $s \in S$
P_s	Probability of state s.
$D_{i,s}$	Demand for firm i when system is in state s; note that $D_{i,gg} = q_i$
q_i	Inherent demand quantity for firm i in absence of adverse events
a	Feature attractiveness, as captured by the slope of the demand function
Λ	Base security breach arrival rate for the industry.
λ_i	Effective security breach arrival rate for firm i.
$1/\mu_i$	Expected duration of a security breach for firm i.
$\rho_i = \Lambda/\mu_i$	Composite firm-industry risk measure for a firm, i
r_i	Firm i's direct-risk elasticity of demand, or simply direct-risk. $0 \leq r_i \leq 1$
e_i	Firm i's demand changes due to externalities. $-1 \leq e_i \leq 1$
π_i	Per unit profit for firm i, excluding feature investment; $\pi_i \geq z_i$
μ, ρ, r, e, π	Symmetric versions of μ_i, ρ_i, r_i, e_i, and π_i
α	Feature cost inflation due to high-security development.
$E[\Pi_i]$	Total expected profit for firm i, or simply profit

product features interact in unintended ways, thereby increasing the possibility of unanticipated vulnerabilities. In this market, the demand for a product of firm i is impacted by the number of features and the realized risk of a security breach, such as when customers observe an IT security breach at either firm i itself or at a competing firm. Using a two-stage game, we demonstrate how potential demand changes (from risk or externalities) impact firm strategy. Our experiments illustrate that firms must balance the number of features in their product or service with the potential security risks, given the changes in customer demand when security breaches occur. We consider a symmetric duopoly with two identical profit-maximizing firms, Firm 1 and Firm 2. In the first stage, each firm decides their developer type; low security (L) or high security (H). In the second stage, each firm must decide the level of investment in product features. An increase in features leads to an increase in quantity demanded for a firm's product; H-type developers incur an additional cost for feature development, $\alpha \geq 0$, which affects the expected profit. However, additional features expose the firm to higher risk of a security breach, which in turn decreases demand for the firm's products. This risk of security breaches is mitigated for H-type developers. We use a standard economic model to establish quantity demanded for each firm under the condition that the entire system is in a 'good' state (i.e. there have been no security breaches). The parameters and decision variables are defined in Table 1.

We build our model using the following assumptions.

Assumption 1. *We consider a system of two firms where each firm makes choices regarding the features to include in their product. An increased investment in features leads to an increase in the number, or sophistication, of features offered.*

For simplicity, the decision variable in our model is feature investment, z_i, $i = 1, 2$.

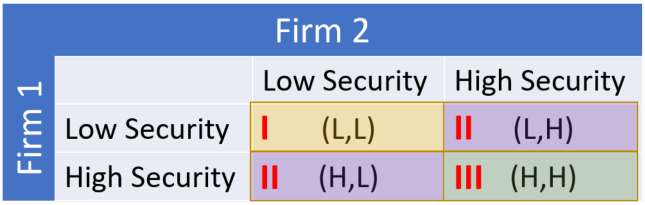


Fig. 3. Set of joint firm developer types.

Assumption 2. *Each firm decides their 'developer type', which is whether to be a low- or high-security developer.*

The decision variable, $\kappa_i \in \{0, 1\}$ captures this decision where $\kappa_i = 1$ means firm i has chosen to be a high security developer and $\kappa_i = 0$ means firm i has chosen to be a low security developer. The set of joint firm developer types is $\Gamma = \{LL, HL, LH, HH\}$. The decision to be a high-security developer impacts the cost of feature development by some amount, $\alpha \geq 0$. Thus, the cost of feature development is $(1 + \alpha\kappa_i)z_i$. The joint firm developer types are tabulated in Figure 3.

Assumption 3. *All things being equal, quantity demanded is a function of the features only; as features increase, demand also increases. To model demand we use a linear demand function.*[1]

$$q_i = 1 + az_i, \text{ where } i = 1, 2 \tag{1}$$

Assumption 4. *Once a security breach has been announced, the affected firm is defined to be in a 'bad' state. Each firm may be in either a good (g) or bad (b) state, independent of the other. The set of joint firm states is $S = \{gg, bg, gb, bb\}$ where, for example, gg represents the joint state that Firm 1 is in a good state and Firm 2 is also in a good state.*

Note that a firm returns to a "good" state when consumers "forget" the earlier security breach. We model this duration as a random variable, as explained in Assumption 5 below.

Assumption 5. *Security breaches follow a Poisson process as a series of independent attacks against the firm.*

As in Kolfal et al. [15], we consider Λ to be the base arrival rate of successful attacks for the system (or industry), although not all attacks are successful. A successful attack is one that results in a publicly known security breach that affects consumer demand. We use the terms 'successful attack' and 'security breach' interchangeably.

Increasing product features also increases the opportunity for an attack to be successful. Let $\lambda_i = (1 + z_i)\Lambda$ for firm $i = 1, 2$ be the arrival rate of successful attacks (i.e. security breaches). When a firm experiences a successful attack, the effects will last for a random length of time. Event duration follows an exponential distribution with expected length $1/\mu_i$ for $i = 1, 2$. While it is possible for firms to affect the expected duration of an event, we do not model this decision. See Figure 4 for an illustration of the state diagram showing the joint firm states that create the steady state probabilities.

[1]A parabolic functional form for demand produces similar results.

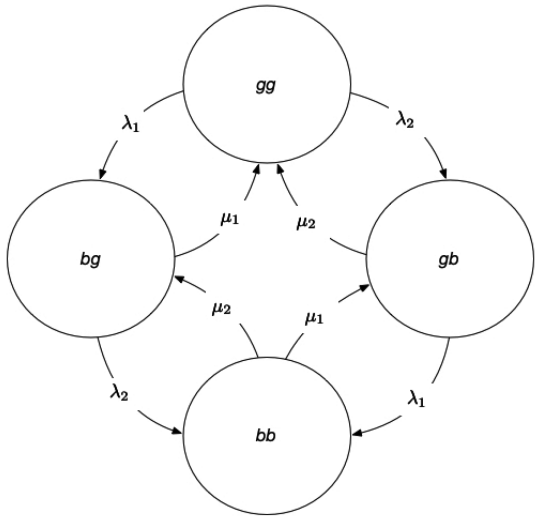


Fig. 4. State diagram.

We are now able to calculate the steady state probabilities for our model as:

$$P_{gg} = \frac{(\kappa_1+1)(\kappa_2+1)}{(\rho_1(z_1+1)+\kappa_1+1)(\rho_2(z_2+1)+\kappa_2+1)} \tag{2}$$

$$P_{bg} = \frac{\rho_1(\kappa_2+1)(z_1+1)}{(\rho_1(z_1+1)+\kappa_1+1)(\rho_2(z_2+1)+\kappa_2+1)}$$

$$P_{gb} = \frac{\rho_2(\kappa_1+1)(z_2+1)}{(\rho_1(z_1+1)+\kappa_1+1)(\rho_2(z_2+1)+\kappa_2+1)}$$

$$P_{bb} = \frac{\rho_1\rho_2(z_1+1)(z_2+1)}{(\rho_1(z_1+1)+\kappa_1+1)(\rho_2(z_2+1)+\kappa_2+1)}$$

where $\rho_i = \Lambda/\mu_i$, $i = 1, 2$. The parameter ρ_i can be thought of as a composite firm-industry risk measure, for firm i.

Assumption 6. *When a firm experiences a successful attack, then demand for that firm's product decreases. We define this percentage change in demand due to a firm's own security breach as the direct-risk elasticity of demand and model it as:*

$$r_i \in [0, 1] \tag{3}$$

As noted in the Introduction section, Jeong et al. [13] demonstrate that information security breaches impact the stock price of organizations in information technology (IT) intensive industries where there is strong competition. We assert that stock price changes should reflect investor expectations related to changes in consumer demand.

Assumption 7. *When a focal firm's competitor experiences a successful attack, then demand for the focal firm's product may increase or decrease. We define this percentage change in demand due to a competitor's security breach as the externality impacting demand and model it as:*

$$e_i \in [-1, 1], \text{ where } e_i + r_i \leq 1 \tag{4}$$

Zafar et al. [33] showed that breaches impact the financial performance of other firms that remain unbreached, indicating that market externalities exist when IS security breaches occur. For

a negative externality ($e_i < 0$) some customers will switch from the affected firm to the unbreached competitor and we call this case "Substitutes in Loss" (or "substitutes" for short). Conversely, for a positive externality ($e_i > 0$) some of the unbreached competitor's customers will also leave the market and we label this case "Complements in Loss" (or "complements" for short). We note that Assumptions 6 and 7 mirror the modeling approach in Kolfal et al. [15].

Assumption 8. *Firms are symmetric in all parameters.*

For tractibility, firms are assumed to be symmetric in all parameters. Thus, we drop the subscript i for direct-risk (r), externality (e), composite firm-industry risk measure (ρ), expected duration of a security breach ($1/\mu$), and per-unit profit (π). Thus we can model the demand equations for the set of joint firm states S as:

$$\begin{aligned} D_{1,gg} &= q_1, & D_{2,gg} &= q_2 \\ D_{1,bg} &= q_1(1-r), & D_{2,bg} &= q_2(1-e) \\ D_{1,gb} &= q_1(1-e), & D_{2,gb} &= q_2(1-r) \\ D_{1,bb} &= q_1(1-r-e), & D_{2,bb} &= q_2(1-r-e) \end{aligned} \tag{5}$$

where $q_i, i = 1, 2$ is given by (1).

3 MODEL ANALYSIS

Firms' per unit profit excluding new feature investment, π, is known and fixed. Consequently, a firm's marginal profit is taken as $\pi - (1 + \alpha\kappa_i)z_i$, which must be positive ($\pi - (1 + \alpha\kappa_i)z_i > 0$) as a participation constraint. The profit for firm i when firms are in joint state s (with probability P_s) is $D_{i,s}(\pi - (1 + \alpha\kappa_i)z_i)$. Firms maximize their expected profit, which is derived for firm i as:

$$E[\Pi_i] = \sum_{s \in S} P_s D_{i,s}(\pi - (1 + \alpha\kappa_i)z_i) = (P_{gg}D_{i,gg} + P_{bg}D_{i,bg} + P_{gb}D_{i,gb} + P_{bb}D_{i,bb})(\pi - (1 + \alpha\kappa_i)z_i), \quad \text{for } i = 1, 2 \tag{6}$$

To find optimal feature investment, we must examine the first order conditions for the expected profit. We begin by setting $\frac{\partial E[\Pi_i]}{\partial z_i} = 0$ in (7):

$$\frac{q_i M_i \rho A_i((1+\kappa_i)(1+\kappa_j) + (1-r-e)(1+z_j)\rho) + B(aM_iA_i - q_iM_i\rho - q_iA_i(1+\kappa_i\alpha))}{A_i^2 A_j} = 0 \tag{7}$$

where $i, j \in 1, 2$, $i \neq j$ and

$$\begin{aligned} M_i &= \pi - (1 + \alpha\kappa_i)z_i, \\ A_i &= 1 + \kappa_i + \rho(1 + z_i), \\ A_j &= 1 + \kappa_j + \rho(1 + z_j), \\ B &= (1+\kappa_i)(1+\kappa_j) + (1-r)(1+\kappa_j)(1+z_i)\rho + (1-e)(1+\kappa_i)(1+z_j)\rho \\ &\quad + (1-r-e)(1+z_i)(1+z_j)\rho^2 \end{aligned}$$

The solution to (7) contains three roots for each firm, although only one root provides feasible investment choices in the real domain. Based on numerical calculations, we next present a series of observations.

3.1 Observations

While we are able to obtain closed-form analytical solutions to our model, the results are complex and thus thwart further interpretation. Thus, to better understand the firm reactions to different

		Firm 2	
		Low Security	High Security
Firm 1	Low Security	Feat. (+++,+++) Profit ($,$)	Feat. (+++,++) Profit ($,$$$)
	High Security	Feat. (++,+++) Profit ($$$,$)	Feat. (+,+) Profit ($$,$$)

Fig. 5. Relative feature investment and profit levels in the three joint development types when high security development is costless.

demand changes from externalities, we use numerical analysis to explore our model. From that analysis, we have several interesting observations.

To begin, we set the penalty for secure development, α, to zero to understand how demand reaction alone would impact feature investment. It could reasonably be expected that if secure development is more costly, then cost alone could be driving the results, so we sought to isolate this effect.

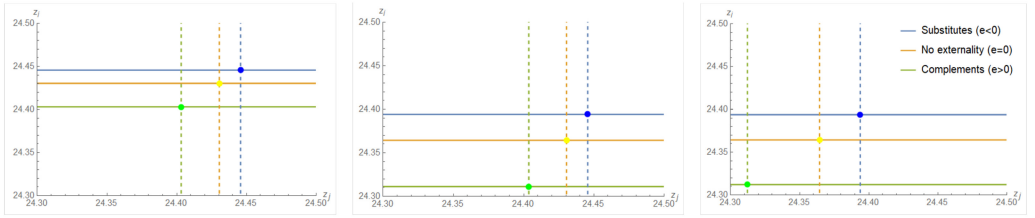
With $\alpha = 0$, we examine the three possible cases for security development types: Case 1 - both firms choose to be low-security developers (i.e. $\gamma = LL$); Case 2 - one firm chooses to be a high-security developer while the other remains a low-security developer (i.e. $\gamma = \{HL, LH\}$)[2]; and Case 3 - both firms choose to be high security developers (i.e. $\gamma = HH$). Without loss of generality, we selected firm 1 as the H-type developer in Case 2.

Observation 1. *When security is cost-less (i.e. $\alpha = 0$), all firms will choose to be high security developers.*

Firms can unilaterally increase profits by choosing to be a high security developer. That is, the expected profit for the H-type firm in joint developer type $\gamma = \{HL, LH\}$ is strictly higher than the expected profit when both firms are L-types, as illustrated in Figure 5. Thus, it is in each firm's self-interest to choose to be H-type. As a result, both will choose to be high security developers. It should be noted, however, that there is no guarantee that expected profit in the joint developer type $\gamma = HH$ will be higher than that for the single H-type developer in the joint type $\gamma = \{HL, LH\}$.

The equilibrium level of feature investment is highest when firms are substitutes in loss and lowest when they are complements in loss. As shown in the three case scenarios in Figure 6, firms will invest in the fewest features when they are complements in loss (marked by the green dot, southwest most point). That is, for positive externalities, $e > 0$, demand decreases for both firms when one firm experiences a security breach. They will invest in the most features when they are substitutes in loss (blue dot, northeast most point in Figure 6). That is, for negative externalities, $e < 0$, demand increases for the unaffected firm since customers switch from an affected firm to the competitor after a security breach occurs. This result is true not only when security is free (i.e. $\alpha = 0$), but also when high-security development is costly (i.e. $\alpha > 0$). When firms experience no externalities, $e = 0$, then the equilibrium level of feature investment is represented by the yellow dot on the imaginary line connecting (or between) the other two dots. Thus, we can conclude that the substitutes case where $e < 0$ results in an increase in feature investment compared to the neutral case where $e = 0$. In contrast, the complements case where $e > 0$ results in a decrease in feature investment compared to the neutral case where $e = 0$. Thus, externalities

[2]Without loss of generality, we will examine only when firm 1 is H-type and firm 2 is L-type as results will be symmetric.



(a) Case 1 ($\gamma = LL$) (b) Case 2 ($\gamma = HL$) (c) Case 3 ($\gamma = HH$)

Fig. 6. Optimal feature investment of each firm (z_i, z_j) by joint security development type (γ), when $\alpha = 0$.

can have opposite impacts on feature investment, depending on the type of customer demand reaction to security breaches. Substitute externalities increase feature investment, but as observed in Figure 6, the increase is relatively small. In contrast, complement externalities decrease feature investment, and as observed in Figure 6, the decrease can be relatively quite large. In other words, the downside risks of complement externalities can have a substantial dampening effect on the optimal equilibrium level of feature investment.

Features come at the cost of security. That is, any time the choice is to develop features that are more secure, there will be fewer features developed, even if security has no additional cost. Figure 6 illustrates this point; the equilibrium feature investment for the H-type firm in case 2 ($\gamma = \{HL, LH\}$) and both firms in case 3 ($\gamma = HH$) are lower than in case 1 ($\gamma = LL$). Given this assertion, Observation 1 means that fewer features are developed even when there is no cost to security.

Equilibrium expected profit is highest when firms are substitutes in loss and lowest when firms are complements in loss.[3] When firms make the same choice regarding the level of security for feature development (that is, where $\gamma \in HH, LL$), firm profits are equal. However, when one firms chooses H-type development while the other chooses L-type (i.e. $\gamma = HL$), the firm that chooses high-security development realizes higher profits than the low-security developer. In particular, we find:

$$\Pi_L^{HL} < \Pi_L^{LL} < \Pi_H^{HH} < \Pi_H^{HL}, \quad \text{when } e < 0 \tag{8}$$

$$\Pi_L^{LL} = \Pi_L^{HL} < \Pi_H^{HL} = \Pi_H^{HH}, \quad \text{when } e = 0 \tag{9}$$

$$\Pi_L^{HL} < \Pi_L^{LL} < \Pi_H^{HL} < \Pi_H^{HH}, \quad \text{when } e > 0 \tag{10}$$

where the notation Π_k^{γ} represents the expected profit of firm selecting security development type $k \in H, L$ when the joint security development is of type γ.

When the firms are complements in loss ($e > 0$), the number of features offered and the profits will be lower (even for the same number of features) than when demand is unaffected by security breaches ($e = 0$) or with substitute externalities ($e < 0$). This type of synchronized competitive situation reduces both innovation and profitability for complement externalities ($e > 0$). The relationships 8–10 show that each firm is better off when $e \geq 0$ when both firms choose H-type development.

The model so far has been examined for the case where there are no increased costs for high security development; that is, $\alpha = 0$. We find that when we consider increased costs for high security development, feature investment is decreasing in α for the high-security firm(s), as expected. Likewise, expected profits are decreasing in α for any firm choosing to be an H-type developer.

[3]This holds for a parabolic demand function also.

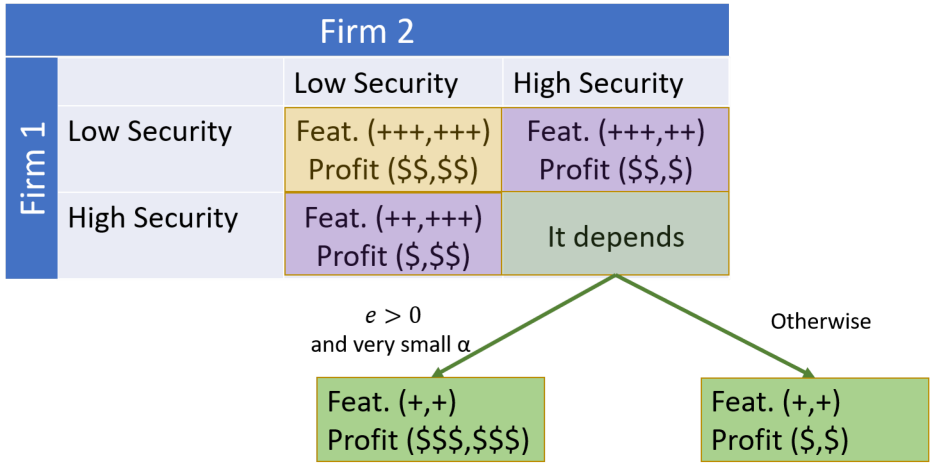


Fig. 7. Relative feature investment and profit levels in the three joint development types when high security development is costly.

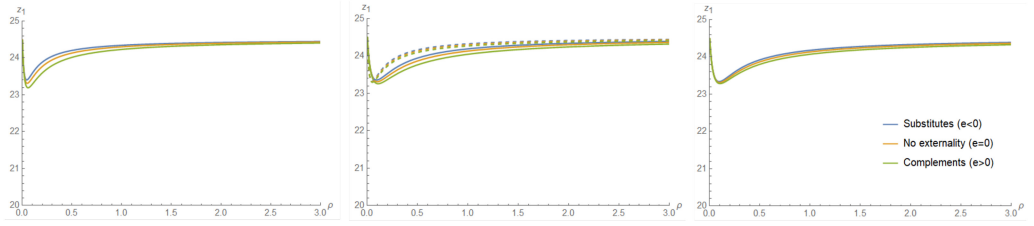
A low security development firm incurs no additional costs, thus it is unaffected by changes in α. Typically, we would assert that there must be some cost to high security.[4] Thus, in reality $\alpha > 0$, and it will not logically be equal to zero in most situations. However, we have examined this rather unrealistic case to see what it would suggest. Next, we consider positive cost for security, $\alpha > 0$, to create perhaps more realistic insights. In this case, we show that adding even a small cost will cause the equilibrium in the model to settle at a point where low security investment for both firms is optimal, resulting in fewer features and lower security.

Observation 2. *With even a small increase in cost to develop secure features, both firms will select low security development.*

Unlike the case where high security development is free ($\alpha = 0$), introducing a penalty for secure development leads to both fewer features and lower profits in all cases for H-type developers, except under very specific conditions (see Figure 7). When firms are complements in loss and the cost for secure development is very small (e.g. $\alpha \leq 0.01$), then it is possible that profits in the case $\gamma = HH$ are higher than in the other joint development cases. However, unlike the situation where $\alpha = 0$, firms will not unilaterally choose to be H-type developers; some form of coordination is required to achieve the HH joint state. Thus, a prisoner's dilemma exists for these very specific conditions.

Observation 3. *When in substitutes or no externality cases (i.e. $e \leq 0$), the higher cost H-type development (i.e. $\alpha > 0$) dominates the decision of the firm; profits are never better for H-type development when $\alpha > 0$. However, in the complements case ($e > 0$), if the added cost of H-type development is sufficiently small, then a prisoner's dilemma emerges. Neither firm can do better by unilaterally choosing to be an H-type developer although, if both firms cooperated and jointly choose to be H-type developers they will both be better off. That is, for the complements case, expected profit may be highest*

[4]Improved development methods may incorporate better security leading to fewer bugs and overall faster development. However, there is a cost to migrating to these development methods (e.g., retraining existing employees, managing process changes, investing in more advanced tools and equipment, etc.). While such increased investments may be temporary, training new employees in the process will likely represent an ongoing commitment.



(a) Case 1 ($\gamma = LL$)

(b) Case 2 ($\gamma = HL$)
Firm 1: Solid lines
Firm 2: Dotted lines

(c) Case 3 ($\gamma = HH$)

Fig. 8. Sensitivity of optimal feature investment to changes in the riskiness of the environment parameter ρ.

when the joint developer type is $\gamma = HH$, provided the added cost of H-type development is sufficiently small.

3.2 Parameter Sensitivity

We next examine how key parameters impact optimal feature investment, z_i^*, and expected profit, $E[\Pi_i^*]$, through a combination of partial derivatives and numerical analysis.

The parameter a can be thought of as representing the attractiveness of features. Its direct effect is to alter the slope of the inherent demand given by (1). Unsurprisingly, numerical analysis shows that both feature investment and expected profit are increasing in a:

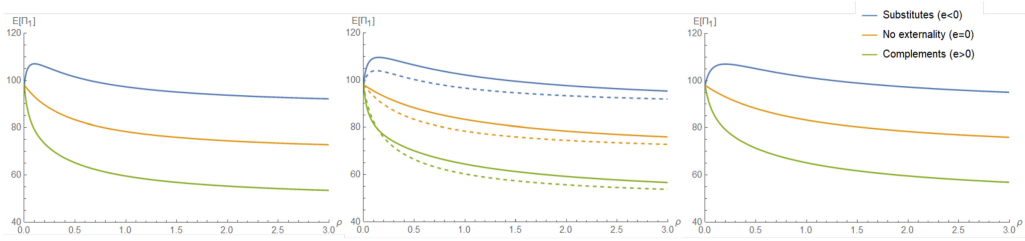
$$\frac{\partial z_i}{\partial a} > 0 \qquad \frac{\partial E[\Pi_i]}{\partial a} > 0 \tag{11}$$

The riskiness of the industry, ρ, has an interesting effect on the optimal feature investment curve. As illustrated in Figure 8, when ρ makes small increases above zero, we see a sharp decrease in the optimal feature investment. However, as ρ continues to increase, the decline in the optimal feature investment will reach a minimum and then slowly rise as ρ continues to increase. Overall, the substitutes case has the highest feature development. This pattern holds for all cases of security decisions and is similar to that found in Kolfal et al. [15] where it was shown that security spending increased initially then fell as ρ increased. In our model, reducing feature spending reduces the attack surface which is effectively the same as increasing security spending in Kolfal et al. [15].

Further, Figure 9 illustrates that for the complements and no externality cases, ($e \geq 0$), expected profits are decreasing. However, in the substitutes case ($e < 0$), expected profits initially increase until a threshold value, ρ_T is reached, then profits decrease. The result for the substitutes case ($e < 0$) is in contrast to the result found in Lemma 2 of Kolfal et al. [15], since the increasing investment in features impacts the per unit profit margin. In Kolfal et al. [15], per unit margins were improved by reducing security spending for riskier environments.

To some extent, ρ can be managed. For example, the control that Apple exerts over its product ecosystem and app developers through its app store can be interpreted as an example of a successful attempt to reduce its ρ. The model clearly predicts that decreasing ρ from high levels will increase firm profits, with only a small effect on feature investment. Feature investment is lowest, though, for riskiness near zero.

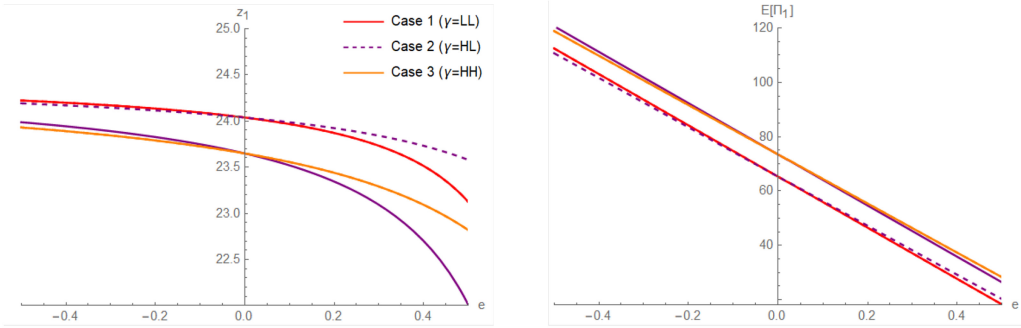
Optimal feature investment and expected profit are decreasing in direct-risk elasticity of demand, as well as in demand externalities. We show Figure 10 for only one value of direct risk, $r = .5$, as this provides the widest range of possible values for demand changes due to externalities, given the constraints in Assumptions 6 and 7. Recall, also, that firms are considered substitutes



(a) Case 1 ($\gamma = LL$) (b) Case 2 ($\gamma = HL$) (c) Case 3 ($\gamma = LL$)

Firm 1: Solid lines
Firm 2: Dotted lines

Fig. 9. Sensitivity of expected profits to changes in the riskiness of the environment parameter ρ.



(a) Feature Investment
Firm 1: Solid lines
Firm 2: Dotted lines

(b) Expected Profit
Firm 1: Solid lines
Firm 2: Dotted lines

Fig. 10. Sensitivity of optimal feature investment and expected profit to changes in the externality parameter e. Note that in Cases 1 and 3 the Firm 1 and Firm 2 curves are identical.

in loss when $e < 0$ and complements in loss when $e > 0$. Thus, this sensitivity analysis confirms the observation that feature investment is higher for substitutes than complements. Feature investments increase for substitute externalities and decrease for complement externalities. The slope of investment changes due to externalities is steeper for complements externalities than for substitute externalities, as shown in Figure 10. In other words, the downside risks of complement externalities can have a substantial dampening effect on the optimal equilibrium level of feature investment.

Examination of Figure 10 reveals an interesting insight. Notice the difference in the way the feature investment lines behave versus the way the expected profit lines behave as e increases from left to right. The feature investment curves asymptotically on the left side when $e < 0$, and expected profit does not. This illustrates that profit is not just about the number of features that you create; profits and features are clearly correlated, although in a non-linear manner. Expected profits, in contrast to feature investment, are linearly decreasing in e, and e is driving both feature investment and profits.

4 DISCUSSION AND CONCLUSIONS

In this paper, we propose a model to evaluate the trade-off between innovation and the risk that is inherently brought on by that innovation. Innovation may cause unanticipated risk for the

customer, such as the potential for security breaches caused by unforeseen exposures created through the product ecosystem. The change in demand from the externalities that a firm faces has a substantial impact on the level of innovation that they offer to the customer. This causes a firm to offer either more or fewer innovations than in an environment with no externalities. Different innovation levels are driven by how customers react to the risk imposed on them by the product ecosystem.

We have explored conditions where firms make trade-offs between offering additional features to an IT-related product or service and the marginal decrease in security. The game theoretic economic model presented in this paper illustrates that investment in feature development and subsequent profits are substantially impacted by the demand changes due to externalities for adverse events such as security breaches. The impact of externalities for the product are divided into two distinct categories. The first is complements-in-loss, whereby adverse events experienced by customers at a competing firm decrease the firm's demand. It is shown that innovation and profits are reduced when the direction of demand reaction to a security breach at one firm is synchronized across firms. In contrast, when demand reaction to a security breach at one firm inversely impacts the other firm, then innovation through additional features (and profits) are higher.

Efforts to control the risk associated with the product ecosystem, such as Apple's tight control over their app store or a website's exclusion of third-party functionality providers, will result in lower industry risk. The model illustrates that as the industry risk is reduced from high levels, the equilibrium level of innovation will decrease. Thus, tightly controlled product ecosystems such as Apple's are expected to dampen innovation somewhat, but this negative impact on demand and profits could easily be offset if the firm is able to desynchronize risks vis-a-vis its competitors while reducing the risks for its customers. In contrast, the Android app store has fewer controls over app developers. The equilibrium level of innovation is higher when the industry risk is higher, as are the realized security breaches arising from the product ecosystem. The stronger control exerted by Apple over their platform environment, seems to have some benefits as far as security is concerned, but product ecosystem innovation as measured by the number of apps is also lower. Our model identifies two potential impacts on the level of innovation that can be strategically managed. The first cause is the level and direction of externalities due to security incidents on demand. The second cause is lower industry risk. Our model explains the impacts of both of these forces which alter the level of innovation in the product ecosystem.

There are many factors and variable values that remain somewhat abstract in this paper. The root causes of market conditions where user security concerns impact demand remain largely unspecified. The line of questioning would be "What does or does not causes those conditions?" This paper does not explicitly deal with the root causes of differences in market conditions, as this is outside our scope and is an avenue for future research.

This research has shown that high-security development is disincentivized, and leads to a type of competitive behavior where the opportunity window for high-security development for all firms is small. This, in turn, leads to innovations where high security is not the focus. Thus, the results indicate that industry security standards or governmental policy intervention are likely required to facilitate high-security solutions. Without such intervention, we would expect to observe the situation that we currently witness, which is a world in which high-security innovations are the exception.

REFERENCES

[1] Mamdouh Alenezi and Mohammad Zarour. 2020. On the relationship between software complexity and security. *International Journal of Software Engineering & Applications (IJSEA)* 11 (2020), 51–60. Issue 1. http://arxiv.org/abs/2002.07135.

[2] H. K. Bhargava. 2014. Platform technologies and network goods: Insights on product launch and management. *Information Technology and Management* 15, 3 (2014), 199–209.
[3] Christina Braz, Ahmed Seffah, and David M'Raihi. 2007. Designing a trade-off between usability and security: A metrics based-model. In *Human-Computer Interaction – INTERACT 2007*, Cécilia Baranauskas, Philippe Palanque, Julio Abascal, and Simone Diniz Junqueira Barbosa (Eds.). Springer Berlin, 114–126.
[4] Giovanni Dosi. 1988. The nature of the innovative process. In *Technical Change and Economic Theory*, Giovanni Dosi, Christopher Freeman, Richard Nelson, Gerald Silverberg, and Luc Soete (Eds.). Pinter Publishers, New York, 221–238.
[5] Golnaz Elahi and Eric Yu. 2009. Modeling and analysis of security trade-offs - A goal oriented approach. *Data & Knowledge Engineering* 68 (2009), 579–598. Issue 7. https://doi.org/10.1016/j.datak.2009.02.004
[6] Dacia J. Ferris. 2019. Tales from a Tesla Model S with 450,000 miles: Battery life, durability, and more. (2019). https://www.teslarati.com/tesla-model-s-quality-durability-on-display-in-450k-mile-car-still-going-strong/. Accessed: 2021-02-12.
[7] Jens Foerderer. 2020. Interfirm exchange and innovation in platform ecosystems: Evidence from Apple's worldwide developers conference. *Management Science* 66, 10 (2020), 4359–4919. https://doi.org/10.1287/mnsc.2019.3425
[8] Ram Gopal, Hooman Hidaji, Raymond Patterson, Erik Rolland, and Dmitry Zhdanov. 2018. How much to share with third parties? User privacy concerns and website dilemmas. *MIS Quarterly* 42 (2018), 143–164. Issue 1.
[9] Mumtaz Abdul Hameed and Nalin Arachchilage. 2020. A conceptual model for the organizational adoption of information system security innovations. In *Security, Privacy, and Forensics Issues in Big Data*, Ramesh C. Joshi and Brij B. Gupta (Eds.). IGI Global, Hershey, PA, 317–339. https://doi.org/10.4018/978-1-5225-9742-1.ch014
[10] Gary Hamel. 1998. Strategy innovation and the quest for value. *Sloan Management Review* 39, 2 (1998), 7–14.
[11] Tejaswini C. Herath, Hemantha S. B. Herath, and John D'Arcy. 2020. Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 51, 2 (2020), 12–35. https://doi.org/10.1145/3400043.3400046
[12] John M. Holt. 2017. The Problem with Patching. (2017). https://www.securityinfowatch.com/cybersecurity/information-security/article/12365412/the-problem-with-patching. Accessed: 2021-02-12.
[13] Christina Y. Jeong, Sang-Yong Tom Lee, and Jee-Hae Lim. 2019. Information security breaches and IT security investments: Impacts on competitors. *Information & Management* 56, 5 (2019), 681–695. https://doi.org/10.1016/j.im.2018.11.003
[14] Benno Keller. 2018. *Big Data and Insurance: Implications for Innovation, Competition and Privacy*. Technical Report. The Geneva Association.
[15] Bora Kolfal, Raymond A. Patterson, and M. Lisa Yeo. 2013. Market impact on IT security spending. *Decision Sciences* 44 (2013), 517–556. Issue 3. https://doi.org/10.1111/deci.12023
[16] K. Laudon. 1985. Environmental and institutional models of system development: A national criminal history system. *Commun. ACM* 28 (1985), 728–740.
[17] Kalle Lyytinen and Gregory M. Rose. 2003. The disruptive nature of information technology innovations: The case of internet computing in systems development organizations. *MIS Quarterly* 27, 4 (2003), 557–596.
[18] E. Mansfield. 1968. *Industrial Research and Technical Innovation*. W. W. Norton, New York.
[19] Bernard Marr. 2018. GDPR: The biggest data breaches and the shocking fines (that would have been). (2018). https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/. Accessed: 2021-02-04.
[20] Robert K. Merton. 1936. The unanticipated consequences of purposive social action. *American Sociological Review* 1, 6 (1936), 894–904. http://www.jstor.org/stable/2084615.
[21] Natasha Nelson and Stuart Madnick. 2017. Trade-offs between Digital Innovation and Cyber-security. (2017), 32 pages.
[22] NIST. 2017. National Vulnerability Database. (2017). https://nvd.nist.gov/. Accessed: 2021-01-25.
[23] Michael Ostrovsky and Michael Schwarz. 2018. *Carpooling and the Economics of Self-Driving Cars*. Working Paper 24349. National Bureau of Economic Research. https://doi.org/10.3386/w24349
[24] Anjanette Raymond, Jonathan Schubauer, and Dhruv Madappa. 2019. After over-privileged permissions: Using technology and design to create legal compliance. *J. Bus. & Tech. L.* 15, 1 (2019), 67–106. https://digitalcommons.law.umaryland.edu/jbtl/vol15/iss1/3.
[25] David Rice. 2008. *Geekonomics: The Real Cost of Insecure Software*. Pearson Education, Inc., Boston, MA.
[26] Amalesh Sharma, Surya Pathak, Sourav B. Borah, and Anirban Adhikary. 2020. Is it too complex? The curious case of supply network complexity and focal firm innovation. *Journal of Operations Management* 66, 7 (2020), 839–865. https://doi.org/10.1002/joom.1067 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/joom.1067.
[27] Yaowu Sun and Qi Zhong. 2020. How modularity influences product innovation: The mediating role of module suppliers' relationship-specific investments. *Management Decision* 58, 12 (2020), 2743–2761. https://doi.org/10.1108/MD-06-2019-0837 Publisher: Emerald Publishing Limited.

[28] L. G. Tornatzky and K. J. Klein. 1982. Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management* EM-29, 1 (1982), 28–45. https://doi.org/10.1109/TEM.1982.6447463 Conference Name: IEEE Transactions on Engineering Management.

[29] Jaikumar Vijayan. 2008. Microsoft Can't Claim Victory in Security Battle. (June 2008). http://www.computerworld.com/article/2551257/security0/microsoft-can-t-claim-victory-in-security-battle.html.

[30] Jingguo Wang, Nan Xiao, and H. Raghav Rao. 2010. Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures. *ACM Trans. Manage. Inf. Syst.* 1 (2010), 1–23. https://doi.org/10.1145/1877725.1877728

[31] Tawei Wang, Karthik N. Kannan, and Jackie Rees Ulmer. 2013. The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24, 2 (2013), 201–218. https://doi.org/10.1287/isre.1120.0437 arXiv:https://doi.org/10.1287/isre.1120.0437

[32] Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, and Xuxian Jiang. 2013. The impact of vendor customizations on Android security. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS'13)*. ACM, New York, NY, USA, 623–634. https://doi.org/10.1145/2508859.2516728

[33] Humayun Zafar, Myung Ko, and Kweku-Muata Osei-Bryson. 2012. Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal (IRMJ)* 25, 1 (2012), 21–37. https://doi.org/10.4018/irmj.2012010102 Publisher: IGI Global.

[34] Kevin Zhu, Shutao Dong, Sean Xin Xu, and Kenneth L. Kraemer. 2006. Innovation diffusion in global contexts: Determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems* 15, 6 (2006), 601–616. https://doi.org/10.1057/palgrave.ejis.3000650 Publisher: Taylor & Francis _eprint: https://doi.org/10.1057/palgrave.ejis.3000650.

[35] Kevin Zhu, Kenneth Kraemer, and Sean Xu. 2006. The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. *Management Science* 52 (2006), 1557–1576. https://doi.org/10.1287/mnsc.1050.0487

Received March 2021; revised October 2021; accepted December 2021