Circumventing Circumvention: An Economic Analysis of the Role of Education and Enforcement*

Debabrata Dey
(ddey@uw.edu)
Foster School of Business, University of Washington, Seattle, WA 98195, USA

Abhijeet Ghoshal
(abhijeet.ghoshal@louisville.edu)
College of Business, University of Louisville, Louisville, KY 40292, USA

Atanu Lahiri
(atanu.lahiri@utdallas.edu)
Jindal School of Management, University of Texas, Dallas, TX 75080, USA

February 11, 2018

Abstract

The role of education and enforcement in ensuring compliance with a law or policy has been debated for more than a century now. Some argue in favor of stronger enforcement, while others advocate education and increased awareness. We reopen this debate in the context of security circumvention by employees, which is currently a leading cause of security and privacy breaches. Drawing from prior literature in information systems, we develop a microeconomic framework that captures employees' circumventing behavior in the face of security controls. This allows us to obtain interesting insights that have implications for how an organization should employ anti-circumvention approaches. First, education and enforcement work better in combination, and not in isolation. Second, there could be motivations to tolerate security circumvention to an extent, even when neither education nor enforcement is particularly costly. Finally, depending on the context, education and enforcement may be strategic complements or substitutes—in some situations, organizations need to invest in both simultaneously, while in others, they ought to emphasize only the cheaper of the two options.

Keywords: Security, privacy, circumvention, education, enforcement, economics of IS

1 Introduction

In recent times, with the rapid proliferation of interconnected, networked information systems (IS), security, privacy, and assurance of information technology (IT) have gained tremendous importance

*A preliminary version of this paper was presented in the Hawaii International Conference on System Sciences (HICSS), 2018. We are grateful to the review team and participants of the SITES (Strategy, Information, Technology, Economics, and Society) minitrack for their insightful comments and constructive criticisms. This work has become much more improved and refined because of their efforts. We are also grateful Don Lewis, the former Chief Technology Officer of Group Health Cooperative and the President and Founder of Strategic Intersect, for the time he has spent with us discussing some of the issues as they pertain to organizational security and privacy.

within all types of organizations (Bulgurcu et al. 2010, Ransbotham and Mitra 2009). In order to reduce the risks of security and privacy breaches, organizations have often invested heavily in IT security. For example, the global IT security market "topped $75 billion in 2015," and is expected to hit an astounding level of $170 billion by 2020 (Morgan 2016). A major share of this expenditure goes towards different types of security *controls*—controls that are supposed to reduce, or even eliminate at times, loopholes through which hackers and other unauthorized users can gain access to a system (Cavusoglu et al. 2005).

A wide variety of security controls are deployed by today's organizations, access authentication through userid and password, site blocking from organizational network, and timeout (automatic sign off) after a period of inactivity being only a few examples. A security control usually has two parts: (i) the control *technique*, and (ii) the control *specification* with which the technique is deployed. For example, userid with password is a control technique for access authentication, and the associated specification is essentially a definition of what makes certain strings of characters acceptable as userid and password. Similarly, site blocking is a security control technique, and the actual list of blocked sites is its specification. Although there are only a limited number of techniques that are employed in practice, the specification set for every technique is usually quite large, providing organizations a wide variety of choices in terms how strict they want to be in regards to a particular security control.

Ironically, despite heavy investments towards IT security, and security controls in particular, security and privacy breaches are only too common an occurrence in the networked world of today. It appears that a significant part of the problem lies not with the controls themselves, but with the human users who interact with these systems. Prior research has consistently found that, in the face of a stricter security control, users often try to bypass or work around it, essentially diluting the ability of the control to effectively thwart security attacks (e.g., Beautement et al. 2008, Bulgurcu et al. 2010, Harrison et al. 2007, Herley 2009, Koppel et al. 2015, 2008, Kothari et al. 2014, Siponen and Vance 2010). In fact, it is not just end users who are guilty of bypassing security controls; all other types of users who interact with the system—developers, testers, security experts, or even system administrators—can and do engage in activities that bypass the intended purpose of security controls (Blythe et al. 2013). Clearly, the term "user" is quite generic and the problem, quite pervasive.

Security circumvention—a situation where a user works around a security control, thereby defeating its purpose, at least partially—can take on many different forms.[1] When a user, faced with a stringent requirement for a complex password, writes it down on a sticky note to attach it to the corner of his monitor—or to the back of the keyboard for that matter—it is a case of security circumvention (Kothari et al. 2014). Similarly, when a user, faced with a list of sites that are blocked from a company network, deliberately connects to a third-party "free" virtual private network (VPN) to access those very blocked sites, it is also a case of circumvention.[2] When a doctor, facing repeated timeouts after a period of inactivity, places a Styrofoam cup on a proximity sensor to fool the system to think that it is still in use, she is actually circumventing a security control (Koppel et al. 2015). And, when a nurse on duty walks away from his station, if only for a few minutes, without signing out of the system and, hence, leaving it vulnerable, it is certainly a case of circumvention as well. As Blythe et al. (2013, p.82) put it, security circumvention occurs any time "users either fail to follow an intended protocol or workflow process, or actively take steps to defeat it."

Why do users circumvent? While it is difficult to pinpoint one single reason (Bulgurcu et al. 2010, D'Arcy et al. 2009, Kankanhalli et al. 2003), prior field work has identified several. First, the inconvenience caused by security controls or policies may often be the primary motivation—the trouble of remembering a long complex password (only with a permissible combination of different keyboard characters) or the frustration at having to repeatedly sign in to a system after periodic timeouts from inactivity are only two of many such examples (Kothari et al. 2014). Second, the urgency to engage in an activity that has been forbidden—the need, for example, to access certain sites that have been blocked—could also be very strong, which might prompt the user to circumvent by, say, connecting to a "dark" VPN (Goodchild 2010). Third, a user may also not be familiar with the repercussions of his own activities, that is, he may grossly underestimate the extent of the damage—to the organization and to him in turn—posed by his negligent actions (Bulgurcu et al. 2010). For example, an employee taking a toilet break for a couple of minutes may think that leaving the system signed in for that small time window is perhaps harmless, when, in reality, it

[1] Circumvention has also been referred to as *noncompliance* and *system abuse* in the IS literature (cf. Bulgurcu et al. 2010, D'Arcy et al. 2009, Straub and Welke 1998).

[2] Despite dire security warnings coming from industry experts against these free VPNs (Silverman 2017), as much as 20% of all VPN use today involves these free VPNs.

could pose a significant security or privacy risk. Finally, a user may not be fully conversant with the security policies and their ramifications (D'Arcy et al. 2009); such would be the case when an executive shares her password with her personal assistant without realizing that it is not only against her company's own security policies, but could also be a federal crime now (Caldwell 2016).

Intentional or not, circumvention can pose significant risks to an organization (e.g., Bulgurcu et al. 2010, Blythe et al. 2013, Bowen et al. 2006, Harrison et al. 2007, Upton and Creese 2014). Not only do such activities dilute the effectiveness of a control, they could also open doors to newer attacks that were not present before the control was put in place. Consider, for instance, an organization blocking a few sites from its internal network, perhaps because it rates those sites as potentially risky. However, if employees start connecting to third-party VPNs to reach certain sites after they have been blocked, not only do they bear the risks posed by those blocked sites, but, now, there is also a security threat from the VPN providers themselves, because, typically, these VPNs are illegitimate sites posing additional risks that were not present earlier.

Circumvention not only heightens an organization's security risks but also poses significant privacy-related risks, above and beyond the ones that are already caused by stolen data from security breaches. For example, sharing of passwords is quite common among clinicians (Koppel et al. 2015). In fact, Heckle (2011) found that clinicians often offer their logged-in sessions to the next clinician as a matter of professional courtesy. Even if such indiscriminate acts of circumvention do not result in a major security breach, they could certainly lead an unauthorized clinical staff to access private and sensitive patient information; this, in turn, would endanger a patient's right to privacy and could bring some additional legal exposure to the organization.

Given these realities, the issue of circumvention and its prevention has become a critical one for many organizations (e.g., Blythe et al. 2013, Harrison et al. 2007, Koppel et al. 2015), and this concern is shared by many practitioners. For example, Kelly (2017), a Chief Information Officer (CIO) himself, categorically identifies circumvention by internal users as the "biggest threat" towards the security of corporate data. Another CIO, Rajavel (2017), recognizes security circumvention by users as one of three most important aspects of cybersecurity today. IBM Security estimates that insider threats account for almost 75% of all security breach incidents, a large share of which comes from noncompliance by employees (Schick 2017). Similar concerns were voiced by other industry experts in our private conversations with them.

Essentially, there are two approaches an organization can take towards curbing circumvention (Bulgurcu et al. 2010, Guttman and Roback 1995, Kirlappos and Sasse 2014, Straub and Welke 1998, Upton and Creese 2014, Wilson and Hash 2003): On one hand, the organization can invest in *enforcement* measures, that is, towards better monitoring (auditing) of user activities and penalizing violations when detected. On the other, it can also invest in providing sufficient *education* (or training) to its employees, making them aware of the current security controls and policies, as well as the ramifications of circumventing them; such informational programs have also been called *security awareness training* in prior research (e.g., Bulgurcu et al. 2010, D'Arcy et al. 2009, Straub and Welke 1998).

To be sure, the notion of employing *education* and *enforcement* to counter noncompliance of a law or a policy is not new and is certainly not limited to the case of security circumvention. Both these approaches have often been used to curb many types of "illegal" behavior, such as tobacco sales to minors, alcoholism, drunk driving, and drug abuse (e.g., Feighery et al. 1991). Put differently, the question of whether to use enforcement or education, or both, is a fundamental one and has been debated time and again in many different contexts.[3] Interestingly, this timeless debate is yet to be settled in a satisfactory manner, either at a generic level or within a specific context. For instance, when the same debate surfaced within the context of underage tobacco use, using a controlled field experiment, Feighery et al. (1991) empirically determined both enforcement and education to be effective, though the latter to a lesser degree. However, while commenting on the relative superiority of enforcement, the authors could not but wonder "whether enforcement alone would have achieved the same outcomes" (Feighery et al. 1991, p.3171). Such ambiguity about the interdependence between these two approaches persists in the security circumvention literature as well (cf. Bulgurcu et al. 2010, D'Arcy et al. 2009, Straub and Welke 1998).

The debate is clearly far from over, and we reopen it in this essay, because the key to mitigating undesirable behavior by social agents lies not only in revisiting these fundamental dilemmas but also

[3]The late nineteenth century provides the backdrop of one such interesting example. At that time, an organization named "Anti-Saloon League" was formed in the US to start a historic fight against alcoholism, a movement that eventually led to prohibition across the US in 1920. Within this organization, though, there were two very distinct lobbies, one led by a lawyer named Wayne Wheeler who wanted to make enforcement the main focus of the league, and the other led by Ernest Cherrington who wanted to make educating citizens about the dangers of alcohol their top priority. Those were competing philosophies then—essentially, education was viewed as a substitute for enforcement—and it was thought that there would be less need for enforcement if, upon education and enlightenment, citizens on their own stayed away from alcohol.

in developing a theoretical foundation that can help us better understand the economic incentives behind such behavior. The following research questions emerge:

- How effective are these two approaches, and should one be preferred to the other? If so, under what conditions would it be preferable?
- Despite being viewed as an important concern, why is circumvention still so common today? Could there actually be an economic rationale for tolerating some circumvention?
- Do these two approaches act as substitutes or complements of each other? What factors or considerations moderate this important behavior?

When viewed within the context of security circumvention, answers to these questions are critically important to an IT manager for planning, budgeting, and developing a comprehensive organizational strategy to curb security and privacy threats posed by circumvention.

To answer these questions, we set up a simple modeling experiment using constructs borrowed from standard microeconomic models. We consider a user base that is heterogeneous in the benefits derived from, and costs incurred for, circumvention. We also consider organizational losses arising out of security loopholes as well as circumvention. A game is setup where the organization first chooses its levels of investment for both education and enforcement. Based on that, the users choose whether or not to circumvent. We solve for the equilibrium of this sequential game and perform comparative statics on the cost parameters for education and enforcement to answer our research questions.

Our answers are interesting. We find that neither approach dominates the other one throughout. We also find that neither approach is sufficient on its own, and a combination is usually the best way forward. These two results, although somewhat intuitive, provide important insights about organizational policy on circumvention. We also find that, in a significant portion of the parameter space, these two approaches to prevent circumvention complement each other, and curiously, their levels either increase or decrease together as the parameters are changed. In general, when circumvention can be reasonably controlled or fully mitigated, enforcement and education are best viewed as substitutes of each other, and the manager may shift resources from one to the other depending on their relative costs. However, when circumvention is widespread, effectively

addressing circumvention requires leveraging the complementarity between these two approaches, and a manager should then invest in both simultaneously, instead of preferring one to the other.

Our analyses also lead to some additional insights. For example, we find that, when hackers are strategic or when circumvention involves a marginal cost borne by the user, it cannot be optimal for the organization to fully eradicate circumvention. In other words, a zero-tolerance policy may have its intuitive appeal, but it may not be the ideal choice in many real-life situations.

2 Literature

Our research overlaps with the extant literature on the economics of information security. This literature has grown substantially in recent years. Of particular relevance are papers that discuss issues pertaining to investments in IT security. For example, Gordon and Loeb (2002) consider the decision to invest in security using an economic model that weighs the cost of security against the expected loss from attacks. In a subsequent empirical work, Gordon and Loeb (2006) make the point that such cost-benefit analysis is quite common in practice. Cavusoglu et al. (2008) argue that a game-theoretic approach actually leads to a more effective security investment decision when compared to such decision-theoretic approaches. This is because the attackers often strategically respond to the level of investment, which makes their activity level endogenous to the decision to invest in information security. Herath and Herath (2008) propose a real-options model to evaluate security investment decisions. Anderson and Moore (2006) and Varian (2000) look at the provision of security from the perspectives of underlying incentives, legal liability, and network externalities. Our main contribution to this literature is that we discuss how investments should be targeted—should they primarily target enforcement or should they emphasize education—in an organizational setting in which employees engage in circumvention of security controls.

The literature on security controls is also important. Lee et al. (2016) examine the role of security standards in a context where not all security controls are verifiable. Our focus is neither on verifiability nor on standards. We simply focus on the consequences of circumvention and the economic losses resulting therefrom. As mentioned already, our motivation is actually rooted in the long stream of research that highlights how users often bypass and work around security controls, in essence rendering them useless (Beautement et al. 2008, Harrison et al. 2007, Herley 2009, Koppel

et al. 2015, 2008, Kothari et al. 2014). According to Koppel et al. (2015), in many cases, these circumventions have become the norm, rather than the exception. Blythe et al. (2013) observe that users often see circumvention as a necessary means to get their job-related activities done, and not because they intend anything malicious.

Our work is also related to the stream of research in the behavioral IS literature that deals with the issue of noncompliance and system abuse. The findings are often mixed. In particular, it has been demonstrated that stronger enforcement—detection of policy violations as well as tougher sanctions on violators—is effective in improving IS security (Kankanhalli et al. 2003, Straub and Nance 1990, Straub and Welke 1998). However, Siponen and Vance (2010) argue that employees may engage in policy violations even in the presence of tough sanctions, because employees tend to engage in rationalizations that reduce the deterring effect of sanctions. Interestingly, though, educating employees about the real risks of getting caught and the severity of likely punishments turns out to be quite helpful in this regard (Straub 1990). Bulgurcu et al. (2010) and D'Arcy et al. (2009) further show that IS security policies and awareness programs are also useful in addressing intentional violations by employees. Put differently, while this stream establishes enforcement and education as two practical approaches towards circumvention, it is silent about the interplay between these two approaches, an issue we take up in this work.

Even though it does not directly consider the interdependence between education and enforcement, the above research stream provides a clear characterization of factors that affect users' attitude towards circumvention. For example, drawing from deterrence theory, D'Arcy et al. (2009), Straub (1990), and Straub and Welke (1998) argue that a user's intention to circumvent is negatively impacted by the perceived probability of detection as well as the perceived severity of sanction (if circumvention is detected). D'Arcy et al. (2009) also find that awareness training positively impacts these perceptions. Bulgurcu et al. (2010) find that a user's attitude is influenced by three factors: (i) benefit of compliance, (ii) cost of compliance, and (iii) cost of noncompliance, and argue that these costs and benefits are simply individual beliefs and may be different for different users. In our work, we borrow much of the user behavior from this literature and place it within a microeconomic framework, essentially a game-theoretic setting with strategic interactions between rational agents.

3 Model Setup

We consider a sequential game in which the organization first chooses whether or not to implement a new or a stricter security control and, if it does, the levels of education (training) and enforcement to accompany this particular control. User education, the level of which is denoted x, may include but is not limited to (Guttman and Roback 1995, Wilson and Hash 2003):

- seminars and training sessions for the control,
- repeated reminders explaining the control,
- videos and other links related to the control, and
- online tutorials and accompanying quizzes.

Essentially, any activity resulting in dissemination of information related to the control or its enforcement contributes positively towards x. In that sense, periodic notices, electronic or physical, explaining to employees the need for the control and likely penalties of circumventing it, are also parts of educating the user and contribute to x, our proxy for education level.

Likewise, y in our model is a proxy for the enforcement level; anti-circumvention enforcement measures may include, among other things (Bowen et al. 2006, Guttman and Roback 1995):

- physical inspection and monitoring,
- automated (real-time or batch) inspection and monitoring,
- analysis of users' activity logs, and
- increasing the penalty level for violations.

Given the organization's circumvention policy $\langle x, y \rangle$, that is, its choice of education and enforcement levels, our users make a decision about whether they should circumvent the security control. We traverse this time line backwards, starting with the user behavior.

3.1 User Behavior

We consider a normalized user base of mass one. We assume that users are heterogeneous and have different valuations, w, for circumventing a specific security control. A user who faces a higher

level of inconvenience from a stricter control should have a higher w. Similarly, a user with a greater urgency to engage in a prohibited activity—such as visiting a blocked site—is also likely to have a higher w. Essentially, our w is the same as the *cost of compliance*, net of *benefits of compliance* (Bulgurcu et al. 2010).

Users are also heterogeneous in the cost or expected penalty, p, they incur when engaging in circumvention; in other words, our p is akin to the *cost of noncompliance* in (Bulgurcu et al. 2010). There are many aspects that may appear as a part of this p; we list only a few below (D'Arcy et al. 2009, Herley 2009, Myyry et al. 2009):

- the expected penalty imposed on the user, that is, the probability of getting caught times the penalty on getting caught,
- the cost associated with learning the tricks to circumvent a specific control, especially when the control is not easy to bypass, and
- the moral cost in causing real harm to his or her own organization.

Therefore, a user $\langle w, p\rangle$ gets a net benefit of $v = w - p$ from circumvention, and his individual rationality (IR) would dictate him to circumvent if and only if $v > 0$. As shown in Figure 1, we assume v is uniformly distributed.[4]

Assumption 1 *The net benefit, v, is uniformly distributed over an interval $[a, b]$, that is, $\frac{v-a}{b-a}$ is uniform over $[0, 1]$.*

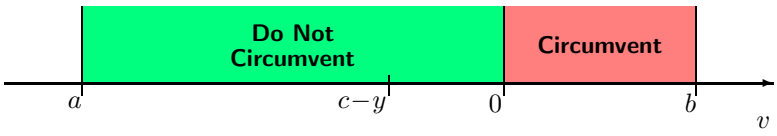


Figure 1: Users Choose to Circumvent (or Not Circumvent) Based on Their Net Benefit, v

Since users react to the organization's adopted circumvention policy $\langle x, y\rangle$, we should expect their circumvention behavior—and hence the distribution of v—to depend on both the level of

[4]Two points need further clarifications here. First, w and p always appear together as $v = w - p$ in the users' IR constraint. Therefore, the individual heterogeneities in w and p are not important, and the only thing that matters in the end is the final distribution of v. Second, our assumption of a uniform distribution is only for analytical tractability; our results are robust to other distributional forms as well.

education, x, and enforcement, y. This is easily captured by endogenizing the end points, $a(x, y)$ and $b(x, y)$, as functions of x and y. To understand the nature of these functions, we must examine the underlying mechanisms through which enforcement and educational activities manifest themselves in the user's net benefit, v. First, as mentioned earlier, typical enforcement activities involve physical and virtual monitoring and analyses of users' interactions with the system; these activities, in essence, increase the chance of detection (Bowen et al. 2006, Guttman and Roback 1995). In other words, when enforcement level increases, the probability for a user to get caught while circumventing increases. Enforcement activities could also involve imposing heftier penalties—including suspension, fine, reprimand, or even a termination of employment—when caught in the act of circumvention (Straub and Nance 1990, Walsh 2004). Since the expected penalty faced by a user is the probability of getting caught times the actual penalty when caught, all in all, stronger enforcement implies a higher expected penalty, $\frac{\partial \bar{p}}{\partial y} > 0$, and a correspondingly lower net benefit to all users. Therefore, it is reasonable to assume that the mean of v, denoted $\bar{v}$, decreases with y, that is, $\frac{\partial \bar{v}}{\partial y} = -\frac{\partial \bar{p}}{\partial y} < 0$. We assume a simple linear relationship and, accordingly, capture this mean as $\bar{v} = c - y$; see Figure 1.

Assumption 2 *The mean of the distribution is given by:*

$$\bar{v} = \frac{a(x, y) + b(x, y)}{2} = c - y, \text{ where } c \text{ is a constant.} \tag{1}$$

In contrast, the impact of education on the users' benefit is not as direct. To understand, we must recognize that a significant component of users' heterogeneity in v arises out of imperfect or partial information. Uninformed or partially informed users are likely to under- or over-estimate, among other things, the real cost borne by the organization, the difficulty in working with a new security control, or even the expected penalty imposed by an organization (D'Arcy et al. 2009, Kirlappos and Sasse 2014, Wilson and Hash 2003). Viewed differently, even if all users had the same value for v in reality, a lack of perfect information guarantees that they do not know this true value. Therefore, users with different levels of (mis-)information would have different perceptions of v, leading to a distribution around the true value (Bulgurcu et al. 2010).

Now, since security education or training activities are often designed specifically to foster user awareness and reduce such information gaps, we would expect educated users to have a better

knowledge of the real threats faced by the organization, a better understanding of the difficulties posed by a stricter security control, and a better estimation of the expected penalty imposed by the organization. All in all, we should expect educational activities to bring users closer to the mean, $\bar{v}$; so, it is logical that user awareness programs should reduce the overall variance in v, by reducing users' lack of perfect information about the true benefit. Since v follows a uniform distribution in our setup, the only way to capture this reduction in variance is to constrict the spread, $(b-a)$, and make it a decreasing function of x.

Before deciding on an appropriate functional form, we must also note that, although more information can reduce the spread, it can never remove the heterogeneity completely. This is because there is also an inherent component in users' heterogeneity that is not related to their information asymmetry—even when all users have perfect information, they are likely to exhibit some level of heterogeneity simply because of their intrinsically different preferences. This restricts us to only those functional forms that satisfy $b(x,\cdot)-a(x,\cdot)>0$ for all finite values of x. Therefore, to represent the spread of the distribution, we use the simplest functional form that conforms to all these requirements.

Assumption 3 *The spread of the distribution of v is given by:*

$$b(x,y)-a(x,y)=\frac{2\alpha}{1+x},\ \textit{where } \alpha \textit{ is a constant.} \tag{2}$$

We can now solve (1) and (2) to endogenize a and b:

$$a(x,y)=c-y-\frac{\alpha}{1+x},\ \text{ and }\ b(x,y)=c-y+\frac{\alpha}{1+x}.$$

Clearly, the density function for the net benefit, v, can be expressed as:

$$f(v)=\begin{cases}\frac{1+x}{2\alpha}, & \text{if } v\in[c-y-\frac{\alpha}{1+x},\ c-y+\frac{\alpha}{1+x}],\\ 0, & \text{otherwise.}\end{cases}$$

Since we know from users' individual rationality (IR) that every user with a $v\in(0,b]$ would engage

in circumvention, we can easily find the size of this segment as a function of x and y:

$$s(x,y) = b(x,y) \times \frac{1+x}{2\alpha} = \frac{1}{2} - \frac{(1+x)(y-c)}{2\alpha}. \tag{3}$$

Before proceeding further, we need to put some restrictions on c and α to make the model realistic. Prior research has clearly identified that the circumvention level, $s(x,y)$ in our model, decreases with both education and enforcement (Bulgurcu et al. 2010, D'Arcy et al. 2009, Kankanhalli et al. 2003, Straub 1990, Straub and Nance 1990, Straub and Welke 1998), implying that (i) $\frac{\partial s}{\partial x} < 0$ for all y and (ii) $\frac{\partial s}{\partial y} < 0$ for all x. The second restriction is automatically satisfied by s given in (3). However, the first restriction can only be satisfied if $c < 0$. Therefore, we limit our analysis to only that part of the parameter space where $c < 0$. Finally, we expect $s(0,0)$ to be positive. Otherwise, not a single user would engage in circumvention, even if the organization spends nothing on education and enforcement; the issue of circumvention then becomes moot. Hence, we only consider those parameter values for which $s(0,0) > 0$ holds, which is simply equivalent to $c + \alpha > 0$. We now state them formally.

Assumption 4 *The parameters c and α in Assumptions 2 and 3 satisfy: (i) $c<0$ and (ii) $c+\alpha>0$.*

3.2 Organization's Problem

We assume that the organization's expected loss from the loophole it is trying to plug using the new or the stricter control is L; in other words, if there were no circumvention, implementing the control is worth L to the organization. However, a portion of this saving is likely to be lost to circumvention; we expect it to be proportional to the fraction of users circumventing the control and write it as $L\mu s(x,y)$, where $\mu > 0$ is the constant of proportionality and $s(x,y)$ is as given in (3). Without loss of generality, we can normalize L to one.

Assumption 5 *The net value of the security control after circumvention is $(1 - \mu s(x,y))$, where $\mu > 0$ represents the relative magnitude of the damage caused by circumvention.*

To complete our model specification, we need to consider the costs associated with education, x, and enforcement, y. We assume a standard quadratic form for both.

Assumption 6 *The costs associated with education and enforcement levels x and y are $\frac{\beta x^2}{2}$ and $\frac{\gamma y^2}{2}$, respectively, where $\beta, \gamma > 0$.*

If the organization chooses to deploy the stricter control, we can combine the above and write its objective function as:

$$z = \left(1 - \mu s(x, y) - \frac{\beta x^2}{2} - \frac{\gamma y^2}{2}\right). \tag{4}$$

The organization chooses $x > 0$ and $y > 0$ to maximize z, subject to $s(x, y) \geq 0$. Of course, the organization's individual rationality (IR) would require that the optimal value, z^*, be positive—a new or a stricter security control, along with its associated education and enforcement levels, is not worth implementing if there is no net benefit from doing so, when compared to doing nothing at all.

4 Results

In equilibrium, the parameter space gets partitioned into three distinct regions:

Proposition 1 *Let*

$$g_1(\gamma) = \gamma(2\alpha(\gamma c^2+\mu)-\mu c) - \sqrt{\gamma(\gamma c^2+2\mu)(2\alpha\gamma c-\mu)^2}, \quad \textit{and} \quad g_2(\gamma) = 8\alpha^2\gamma+\mu^2-4\alpha\gamma\mu(c+\alpha).$$

Further, define:

$$h_1(\gamma) = \begin{cases} \frac{\mu^3}{2\alpha g_1(\gamma)}, & \textit{if } \gamma > \frac{\mu}{2\alpha(c+\alpha)}, \\ \infty, & \textit{otherwise,} \end{cases} \quad \textit{and} \quad h_2(\gamma) = \begin{cases} \frac{\mu^2(2-\gamma c^2-\mu)}{g_2(\gamma)}, & \textit{if } \gamma > \frac{\mu^2}{4\alpha(c\mu+\alpha(\mu-2))} \textit{ and } \mu > \frac{2\alpha}{c+\alpha}, \\ \infty, & \textit{otherwise.} \end{cases}$$

Then, the following equilibrium outcomes emerge:

- **Circumvention Region:** *When $h_1(\gamma) \leq \beta \leq h_2(\gamma)$, the organization implements the control, but some users circumvent it.*
- **No-Circumvention Region:** *When $\beta < h_1(\gamma)$, the control is implemented, and no users circumvent it.*

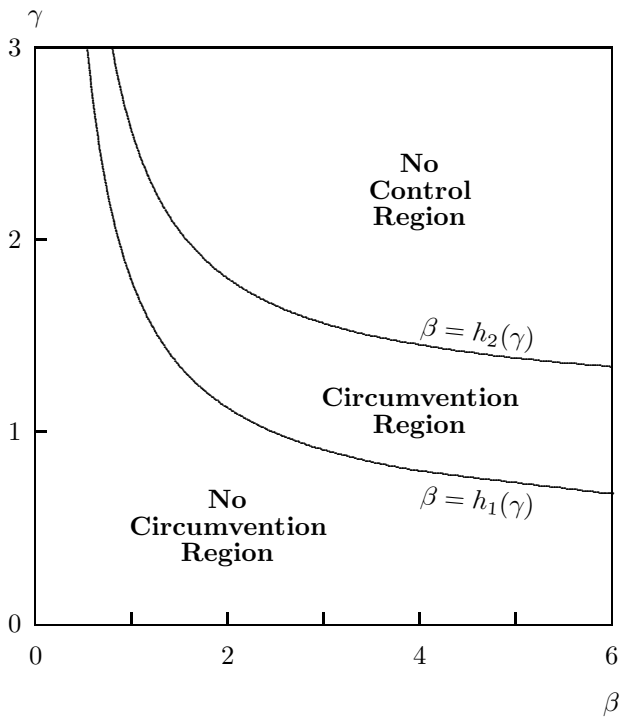


Figure 2: Relevant Partitions of the (β, γ) Space; $\alpha = 2$, $\mu = 3$, $c = -\frac{1}{3}$

- **No-Control Region:** *When $\beta > h_2(\gamma)$, the organization decides not to implement the control.*

The result in Proposition 1 is better visualized in Figure 2. As can be seen from this figure, when β is small or γ is small, or both, the organization can effectively eliminate all circumvention by users, either by providing sufficient education or by increasing the level of enforcement, or by using a combination of the two. When β and γ are both high, the organization simply cannot afford either approach and decides to not implement the control at all. In the middle, where β and γ take on moderate values, the control is adopted, along with a combination of enforcement and educational activities; circumvention is controlled to an extent, but cannot be fully eliminated. Any organization struggling with the issue of circumvention should belong to this middle region.

We now look at the organization's optimal choices of education and enforcement levels:

Proposition 2 *The optimal levels of education and enforcement can be expressed as follows:*

- **Circumvention Region ($h_1(\gamma) \leq \beta \leq h_2(\gamma)$):**

$$x^* = \frac{\mu(\mu - 2c\alpha\gamma)}{4\alpha^2\beta\gamma - \mu^2}, \quad \textit{and} \quad y^* = \frac{\mu(2\alpha\beta - c\mu)}{4\alpha^2\beta\gamma - \mu^2}.$$

- **No-Circumvention Region ($\beta < h_1(\gamma)$):** *x^* is the only real and positive solution of:*

$$\frac{\alpha\gamma(c(1+x)+\alpha)}{(1+x)^3} - x\beta = 0,$$

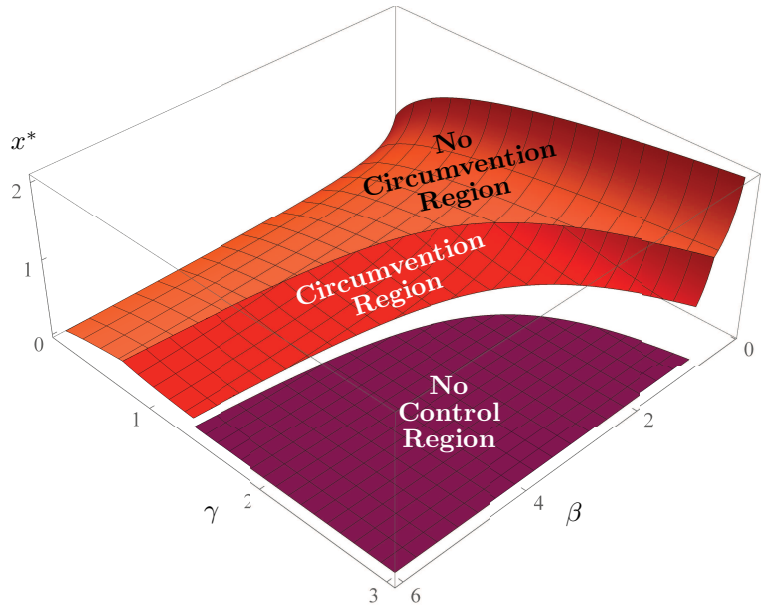
and $y^* = c + \frac{\alpha}{1+x^*}$.

- **No-Control Region ($\beta > h_2(\gamma)$):** $x^* = y^* = 0$, *trivially.*

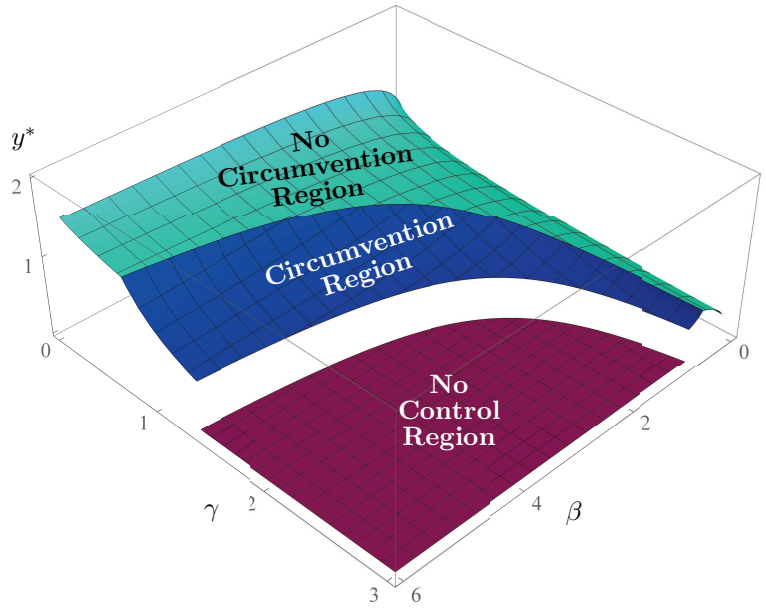
The results in Proposition 2 are presented in Figure 3. Proposition 2 and Figure 3 tell us an interesting story; they show that both the approaches, education and enforcement, work hand-in-hand against circumvention. Therefore, they are both required for dealing with circumvention, and neither approach can achieve it on its own. For any values of β and γ satisfying $\beta \leq h_2(\gamma)$, both x^* and y^* are positive, implying that it is more effective to use the two approaches in combination, rather than in isolation. In other words, neither approach dominates the other in preventing circumvention. Of course, the correct mix depends on their relative costs, as parameterized by β and γ.

Proposition 3 *The optimal level of education, x^*, is monotonically decreasing in β, and the optimal enforcement level, y^*, is monotonically decreasing in γ, that is, $\frac{\partial x^*}{\partial \beta} \leq 0$ and $\frac{\partial y^*}{\partial \gamma} \leq 0$. However, the relationship between x^* and γ, as well as that between y^* and β, is not monotonic. More specifically, $\frac{\partial y^*}{\partial \beta}, \frac{\partial x^*}{\partial \gamma} \geq 0$ in the no-circumvention region, but $\frac{\partial y^*}{\partial \beta}, \frac{\partial x^*}{\partial \gamma} \leq 0$ in the circumvention region.*

The results in the first part of Proposition 3 are intuitive. As the cost for education (or enforcement) goes up, we would expect to see the organization cutting down on its level; likewise, as the marginal cost goes down, we should expect the level to increase. On the other hand, when β goes up, we would expect the organization to shift resources from x to y, implying $\frac{\partial y^*}{\partial \beta} \geq 0$; likewise, we can expect $\frac{\partial x^*}{\partial \gamma} \geq 0$. However, this intuition does not hold in the circumvention region, a situation many organizations are likely to find themselves in. All these trends are clearly discernible from Figure 3 as well.



(a) Training Level, x^*



(b) Enforcement Level, y^*

Figure 3: Optimal Levels of Training and Enforcement; $\alpha = 2$, $\mu = 3$, $c = -\frac{1}{3}$

Theorem 1 *Education and enforcement complement each other in the circumvention region but act as substitutes in the no-circumvention region.*

This may come across as counterintuitive at first. Education and enforcement are both means to the same end—mitigation of circumvention. It is only natural to anticipate that they would be

substitutes of each other—when one becomes costlier, we expect it to be reduced with an accompanying increase in the level of the other. Theorem 1 formally establishes that, while this intuition remains valid in the no-circumvention region, it no longer holds in the circumvention region. In the circumvention region, these two approaches evidently complement each other, increasing or decreasing in a lockstep manner as model parameters vary.

The intuition behind this surprising result is actually found in (3), wherein $\frac{\partial s}{\partial x}$ and $\frac{\partial s}{\partial y}$ are both negative, implying that the circumvention level is decreasing in both x and y. Interestingly, the rate of decrease with respect to x is actually increasing in y, and that with respect to y increasing in x, that is, $\frac{\partial}{\partial y}\left(-\frac{\partial s}{\partial x}\right) = \frac{\partial}{\partial x}\left(-\frac{\partial s}{\partial y}\right) = \frac{1}{2\alpha} > 0$. In other words, education is more effective in mitigating circumvention and is of greater value when enforcement is stronger; similarly, enforcement is more effective and valuable when users have more information. That education and enforcement have such a reinforcing effect on each other is also consistent with practice. Enforcement is a more effective deterrent only when users are made aware of it (Bulgurcu et al. 2010), since it is their awareness that allows users to form perceptions about relative costs and benefits of noncompliance. At the same time, education is more effective only when the threat of sanctions is credible (Straub and Welke 1998). Therefore, when circumvention is rampant and a rapid decrease in its level is required, education and enforcement bolster each other's effect and act as complements. In contrast, when circumvention is already under control and the objective is to simply keep it in check, a rapid decrease in the circumvention level is no longer necessary. It is only then that education and enforcement start substituting for each other—increasing one while reducing the other commensurately becomes sufficient to hold circumvention down.

There is a more mathematical way of looking at Theorem 1. The objective function in (4) happens to be supermodular in x and y, because $\frac{\partial^2 z}{\partial x \partial y} = -\mu\frac{\partial^2 s}{\partial x \partial y} = \frac{\mu}{2\alpha} > 0$. Therefore, for the interior maximum, complementarity across strategic choices are guaranteed (cf. Sundaram 1996, ch.10). Viewed another way, the complementarity actually stems from the way x and y directly impact the circumvention level, s. Of course, this complementarity does not extend to the no-circumvention region as we do not have an interior solution there.

Before moving on, a quick note is necessary. It might be tempting to conclude that the result in Theorem 1 is closely tied to the geometry of the problem and, in particular, to the specification of s that makes z supermodular. This, however, is not necessarily true. The main insight—the two

anti-circumvention approaches are best viewed as strategic complements in the face of widespread circumvention, and as strategic substitutes when circumvention is reigned in—happens to be a lot more fundamental than the geometry or the specification of s itself. In fact, it is not necessary that both the circumvention and no-circumvention regions exist in equilibrium for this important insight to remain applicable. We discuss this next.

5 Circumvention and Strategic "Hacker"

A discussion of an organization's strategic choices in the face of security risks from circumvention would be largely incomplete without an analysis of the strategic dimension of hackers' opportunistic behavior. Indeed, absent such strategic behavior, circumvention poses little security or privacy risks to an organization. For, an incident involving circumvention can turn into a real threat only when someone—a *hacker* in the absence of a better term—is actively looking for such an incident while searching for an opportunity to *hack* into the system and breach its security control. It is only reasonable that such hackers would act in a strategic manner, implying that they would weigh their efforts against the potential benefit or, as it is often called, the *payload*.

Prior research has argued that hackers' payload is essentially (proportional to) the damage they can cause through the hack (cf. Dey et al. 2012, Png and Wang 2009). We too adopt this as our account of a hacker's strategic behavior and denote the payload as $\mu(e)s$, which, according to Assumption 5, is also the organization's loss due to circumvention. The only difference is that $\mu(e)$, the relative magnitude of the damage caused by circumvention, is no longer a constant; it now depends on e, the effort level exerted by the hackers. In practice, we would expect $\mu(e)$ to be an increasing function of e, satisfying the boundary condition of $\mu(0) = 0$. We consider a simple linear form: $\mu(e) = \mu e$, wherein $\mu > 0$ once again becomes a constant for notational brevity.

The time line of this sequential game is as follows: the organization first chooses $\langle x, y \rangle$; each user then decides whether or not to circumvent, which determines $s(x, y)$; finally, the hackers choose their effort level, e. We assume that a hacker's cost or disutility for an effort level e is $\frac{\eta e^2}{2}$, $\eta > 0$, leading to the hacker's optimization problem: $\max_e \left(\mu e s - \frac{\eta e^2}{2}\right)$, which has a simple solution of $e^* = \frac{\mu s}{\eta}$. Therefore, the damage caused by strategic hackers becomes $\frac{(\mu s)^2}{\eta}$. Our earlier Assumption 5 must then be replaced by the following result:

Lemma 1 *The net value of the security control after circumvention is* $\left(1 - \frac{(\mu s(x,y))^2}{\eta}\right)$*, where* $\mu, \eta > 0$ *and* $s(x, y)$ *is as in (3).*

Therefore, if the organization decides to deploy the control, its objective function now becomes:

$$z = \left(1 - \frac{(\mu s(x, y))^2}{\eta} - \frac{\beta x^2}{2} - \frac{\gamma y^2}{2}\right).$$

Once again, the organization chooses $x > 0$ and $y > 0$ to maximize this new z, subject to $s(x, y) \geq 0$. As before, the organization's individual rationality (IR) would require that the optimal value, z^* is positive. It turns out that, unlike before, the organization's decision problem now has a valid interior solution for the entire (β, γ) space except, of course, at very high values of β and γ where the organization adopts the no-control strategy and collects a pay-off of zero. In other words, we have:

Theorem 2 *When hackers are strategic, the no-circumvention region disappears. As long as a control is adopted, there are always some users who circumvent it.*

Theorem 2 seems surprising. Now that hackers are acting strategically and looking to exploit employees' circumventing behavior more opportunistically, one would expect the organization to become extra cautious about the possible threats that circumvention poses; it would then seem logical that the organization clamps down on circumvention more forcefully in an effort to curb it further. However, what we find in Theorem 2 is exactly the opposite—when hackers are strategic, the organization actually relents, allowing some level of circumvention to persist.

Although counterintuitive, Theorem 2 can be explained in the following manner. When circumvention reduces, so does the hackers' incentives to exploit it. Therefore, when circumvention is low enough, and hackers are sufficiently discouraged, further reduction in circumvention has little marginal impact on the organization's benefits and does not pay for itself. It is only when $\gamma = 0$ or $\beta = 0$ that the organization finds it worthwhile to fully eradicate circumvention by choosing (x^*, y^*) so as to make $s(x^*, y^*) = 0$; however, this boundary solution also happens to be an interior solution now.

Theorem 2 provides practical insights for organizations as well. It clearly shows that it is not really necessary for an organization to try to eradicate circumvention completely. As long as it is

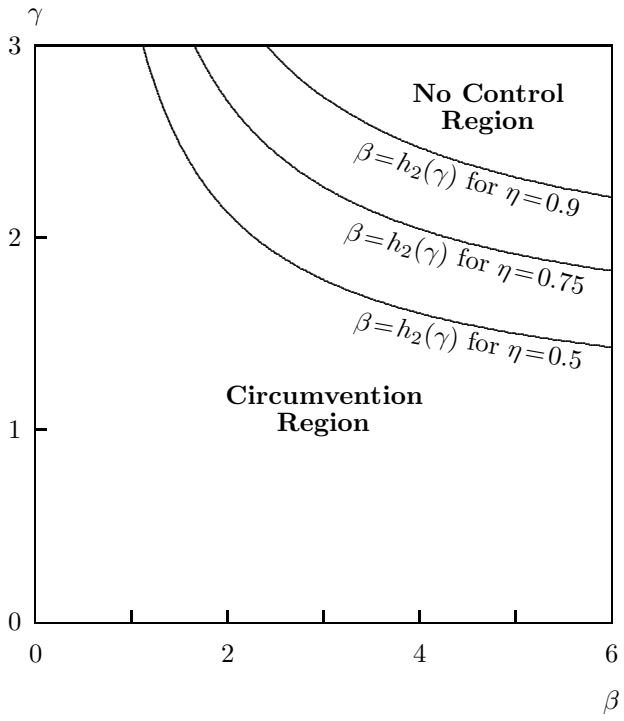


Figure 4: Circumvention and No-Control Regions in the (β, γ) Space; $\alpha = 2$, $\mu = 3$, $c = -\frac{1}{3}$

under control, that is, as long as it is at a reasonably low level, circumvention has little chance to attract strategic hackers widely. Therefore, there is little need for an organization to get carried away in its anti-circumvention efforts, even when such efforts are not that costly. Since we expect hackers to be strategic in practice, this insight is quite relevant for IT managers grappling with the issue of circumvention while setting an appropriate budget for education and enforcement.

Theorem 2 tells us that only two equilibrium regions—circumvention and no-control—are possible in this revised setup. The boundary between the two regions, still denoted by $\beta = h_2(\gamma)$, can be found by equating the interior z^* to zero. Figure 4 clearly shows these two regions, along with the boundary between them for three different values of η. It is clear from the plots that the circumvention region expands, and the no-control region shrinks, as η increases. This is along the expected lines. As η increases, hackers' effort becomes costlier, so they cut down on their hacking efforts to breach the security. Thus, facing a lower level of threat from circumvention, the organization prefers to tolerate some circumvention and deploys the control over a larger portion of the parameter space.

Proposition 4 *When hackers behave strategically, if the organization chooses to deploy the control, its optimal choices for education and enforcement levels are x^* and y^*, where $y^* = \frac{\mu^2(1+x^*)(c(1+x^*)+\alpha)}{2\alpha^2\gamma\eta+\mu^2(1+x^*)^2}$, $x^* = r^* - 1$, and r^* is the unique real root of the following fifth-order polynomial equation:*

$$4\alpha^4\beta\gamma^2\eta^2(r-1) + 2\alpha^2\gamma\eta\mu^2\left(2\beta r^2(r-1) + \gamma c(cr+\alpha)\right) + \mu^4 r\left(\beta r^3(r-1) - \alpha\gamma(cr+\alpha)\right) = 0.$$

Proposition 4 echoes the result in Proposition 2 that education and enforcement are both required to effectively deal with circumvention; clearly, neither approach can do it on its own. Now, how should an organization view education and enforcement, as substitutes or as complements? Since the circumvention region has completely subsumed the no-circumvention region now—and since the specification of s remains exactly as before—it might be tempting to conclude that education and enforcement would now always complement each other. Such a rush towards a conclusion, though, would not be prudent, because our earlier result in Theorem 1 that education and enforcement are complements in the entire circumvention region no longer holds. The next theorem states this more formally:

Theorem 3 *When hackers behave strategically, education and enforcement could act as substitutes or as complements in the circumvention region. More specifically, let $\beta = h_3(\gamma)$ be the unique positive solution of:*

$$\alpha + 2(1 + x^*)(c - y^*) = 0.$$

Then, for all (β, γ) values satisfying $\beta > h_3(\gamma)$, education and enforcement act as complements; for the remaining portion of the circumvention region, they are substitutes.

Theorem 3 is perhaps better viewed in the form of Figure 5, where the boundary, $\beta = h_3(\gamma)$, is plotted for three different values of η. Theorem 3 and Figure 5 reaffirm the fact that, for a significant portion of the parameter space—for $\beta > h_3(\gamma)$ to be precise—education and enforcement complement each other in curbing circumvention. It is only when either of them becomes really cheap, and circumvention can hence be reigned in, that we see them become substitute to each other. Viewed another way, for moderate values of β and γ, as either one decreases, the optimal levels of education and enforcement start increasing simultaneously. However, when, β (or, γ) becomes very small, education (or, enforcement) becomes very cheap and the organization starts

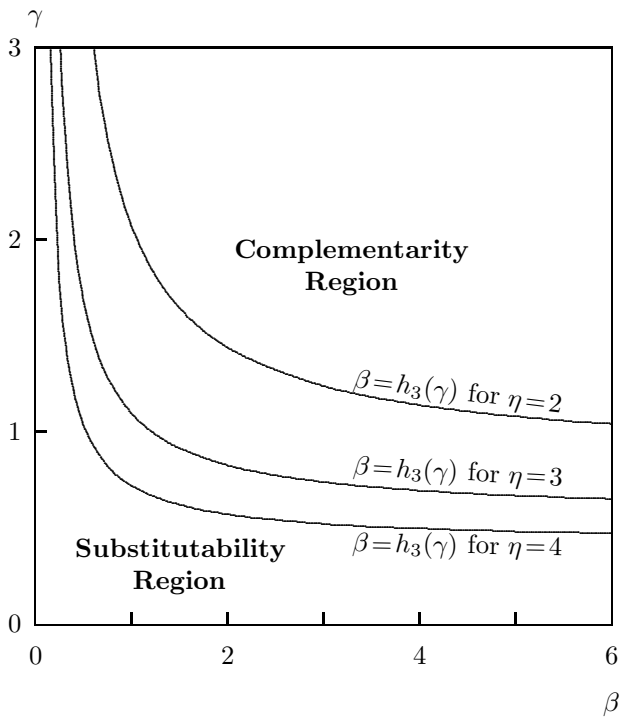
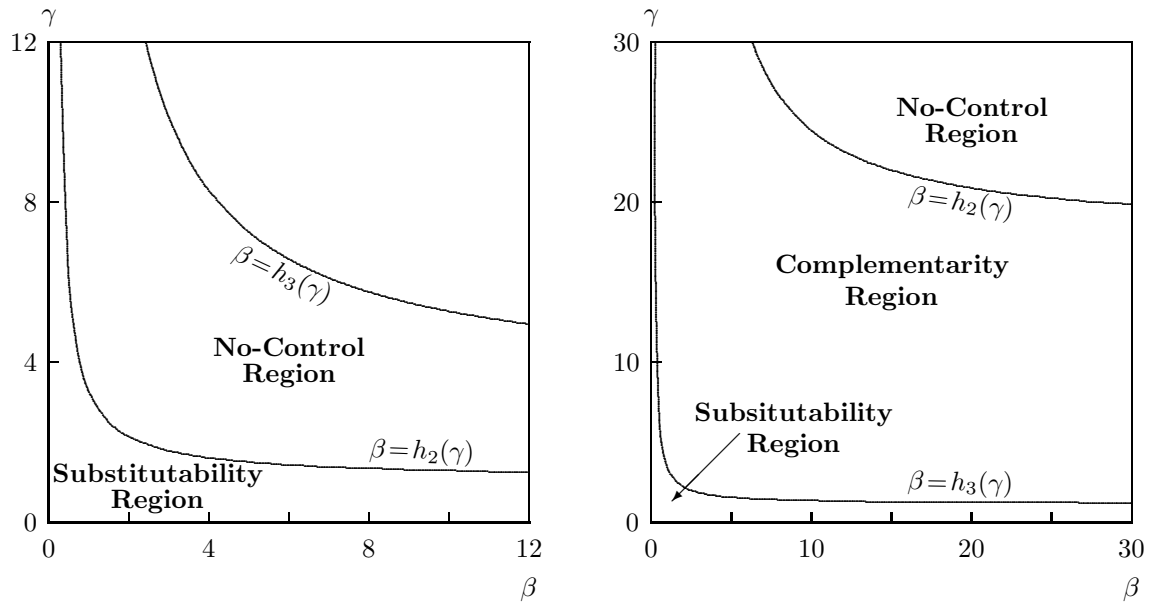


Figure 5: Complementarity versus Substitutability; $\alpha = 2$, $\mu = 3$, $c = -\frac{1}{3}$

increasing x (or, y) to such a high level that it now starts substituting for y (or, x).

Finally, it is clear from Figure 5 that, as η decreases, the complementarity region shrinks and the substitutability region expands. Evidently, as η decreases, the hackers step up their efforts, resulting in a higher expected damage to the organization. Facing a higher level of damage due to circumvention, the organization is then compelled to make $s(x, y)$ even smaller, so that the strategic hackers are discouraged even further. And, as we already know, when $s(x, y)$ is small, the substitution effect between x and y takes over, leading to an expansion of the substitutability region. In fact, for a sufficiently small value of η, the h_3 boundary in Figure 5 may actually overtake h_2 in Figure 4, making the complementarity region completely disappear. Such a situation is depicted in panel (a) of Figure 6, where h_3 is above h_2 and the complementarity region disappears. The other situation—moderate or high values of η where the complementarity region persists—is shown in panel (b) of Figure 6.



(a) $\eta = 0.5$ (b) $\eta = 1.5$

Figure 6: Partitions of the (β, γ) Space; $\alpha = 2$, $\mu = 3$, $c = -\frac{1}{3}$

6 Non-Zero Marginal Cost of Circumvention

An implicit assumption in our modeling setup is that a user faces no marginal cost per act of circumvention. Therefore, they either circumvent fully or they do not circumvent at all, depending on whether their v is positive or negative, and all users engage in essentially the same level of circumvention. Although a zero marginal cost may make sense for certain controls, it might be too restrictive in certain others. For example, a user trying to access blocked sites may have to take the pain of connecting to a third party VPN every time he accesses such a site. This per-connection cost may reduce the frequency with which he engages in this task. To capture this, we model user v's level of circumvention as l and set his cost of circumvention to $\frac{\chi l^2}{2}$, where $\chi > 0$ is a cost parameter.[5] Since a user gets a net benefit that increases with l, we set it at lv.

[5]One could argue that a user experiences only a fixed marginal cost for circumvention, making the total cost linear, and not quadratic. It turns out that, in the case of a linear circumvention cost, all our original results in Section 4 hold as stated. To see this more clearly, consider user v's circumvention cost to be χl, making his net utility $l(v - \chi)$. Therefore, the user would circumvent if and only if $\chi < v \leq b$. The level of circumvention can then be written as:

$$s = (b - \chi) \times \frac{1 + x}{2\alpha} = \frac{1}{2} - \frac{(1 + x)(y - c + \chi)}{2\alpha}.$$

Comparing this with (3), it is easy to see that, now, we simply get back our original formulation with c being replaced by $(c - \chi)$.

Then, the user's net utility becomes $\left(lv - \frac{\chi l^2}{2}\right)$, the concavity of which ensures that the user desires circumvention only up to a point. Maximizing this utility, we can find the user's optimal level of circumvention as: $l^*(v) = \frac{v}{\chi}$, which can be integrated over all circumventing users $v \in (0, b]$ to find the total level of circumvention as:

$$\frac{1+x}{2\alpha}\int_0^b l^*(v)dv = \frac{\alpha(s(x,y))^2}{\chi(1+x)},$$

where $s(x, y)$ is as in (3). Assumption 5 should then be replaced by:

Lemma 2 *The net value of the security control after circumvention is* $\left(1 - \mu\frac{\alpha(s(x,y))^2}{\chi(1+x)}\right)$, *where* $\mu, \chi > 0$.

Therefore, if the organization chooses to deploy the stricter control, its objective function now becomes:

$$z = \left(1 - \frac{\alpha\mu(s(x,y))^2}{\chi(1+x)} - \frac{\beta x^2}{2} - \frac{\gamma y^2}{2}\right).$$

Interestingly, this decision problem, too, has a valid interior solution for the entire (β, γ) space, except at very high values of β and γ where the organization adopts the no-control strategy.

Theorem 4 *When users face a non-zero marginal cost for circumvention, the no-circumvention region disappears, and, if a control is adopted, there are always some users who circumvent it.*

Theorem 4 clearly tells us that, just as in the case of strategic hackers, it is not necessary to eradicate circumvention fully when users face a marginal cost to circumvent. If the net benefit v can be restricted to a small enough level, the marginal cost would force the users to reduce their circumvention activities to an extent that circumvention loses its teeth in causing harm to the organization. This way, circumvention becomes a lot more tolerable to the organization.

Theorem 4 also indicates that, once again, only two equilibrium regions—circumvention and no-control—are possible. The boundary between the two regions can be found by simply equating the interior z^* to zero. It can be shown that this boundary shifts upwards with an increasing χ, thereby shrinking the no-control region. As χ increases, users cut down on their circumvention activities. Thus, facing a lower level of circumvention, the organization deploys the control over a larger portion of the parameter space.

Proposition 5 *When users face a non-zero marginal cost for circumvention, the organization's optimal choices for education and enforcement levels when deploying a control are given by x^* and y^*, where $y^* = \frac{\mu(c(1+x^*)+\alpha)}{2\alpha\gamma\chi+\mu(1+x^*)}$, $x^* = r^* - 1$, and r^* is the unique real root of the following fifth-order polynomial equation:*

$$\frac{\gamma\mu^2(cr+\alpha)^2}{r(2\alpha\gamma\chi+\mu r)^2} - \frac{\gamma\mu(cr+\alpha)(cr-\alpha)}{r^2(2\alpha\gamma\chi+\mu r)} - 2\beta(r-1) = 0.$$

Proposition 5 echoes Propositions 2 and 4 that education and enforcement are both required to effectively deal with circumvention and that neither approach can do it on its own.

Theorem 5 *When users face a non-zero marginal cost for circumvention, education and enforcement act as substitutes in the entire circumvention region.*

Theorem 5 shows that, even though the disappearance of the non-circumvention region now is quite similar to what happens in the case of strategic hackers, the case of non-zero marginal cost is clearly different. Unlike our earlier results, in this case, the complementarity region vanishes completely. The broader takeaway is that, although x and y reinforce each other in reducing s, they are not necessarily strategic complements. It is the context that ultimately decides the actual nature of their interplay.

7 Other Considerations

We set up a parsimonious model to examine the role of education and enforcement in curbing circumvention. In so doing, we made certain simplifying assumptions about the context. In this section, we relax a couple of those assumptions and check robustness of our findings. Additional details about these extensions are provided in the appendix.

7.1 Spillover Effects of Education and Enforcement

So far, we have assumed that education and enforcement impact the distribution of v in a very distinct and isolated manner—education impacts only the variance and enforcement only the mean of the distribution. However, it is possible that there is some indirect effect of enforcement on the variance and of education on the mean. For example, when enforcement leads to sanctioning

an employee, his co-workers might observe it and become more aware of organizational policies; this could result in a reduction of the variance of v. Likewise, when an employee is made aware of the potential fallouts of circumvention and ensuing business implications, his moral cost for circumvention may increase, making circumvention appear costlier to the employee. In other words, there could be spillover effects of education on the mean of v and of enforcement on its variance. To investigate such a possibility, we now set:

$$\bar{v} = \frac{a(x,y) + b(x,y)}{2} = c - \delta x - y, \quad \text{and} \quad b(x,y) - a(x,y) = \frac{2\alpha}{1 + x + \epsilon y},$$

where $\delta, \epsilon > 0$ are the spillover parameters. In that case, the circumvention level becomes:

$$s(x,y) = \frac{1}{2} - \frac{(1 + x + \epsilon y)(y + \delta x - c)}{2\alpha}.$$

Substituting this $s(x,y)$ into the organization's objective function and maximizing the latter, we find that the (β, γ)-space again gets partitioned into three regions: (i) no-circumvention region, (ii) circumvention region, and (iii) no-control region. Furthermore, irrespective of the values of δ and ϵ, education and enforcement complement each other in the circumvention region and are substitutes in the no-circumvention region.

7.2 Network Effect

It is also possible that users' circumventing behavior exhibits some positive network effect. This is because those who circumvent may influence others, with tips, tricks, and encouragement. Besides, when co-workers get away with noncompliance of security policies, it may encourage others to try it as well. In a fulfilled expectations equilibrium, we can find the fraction of circumventing users, $s(x,y)$, from the following equation:

$$s(x,y) = \frac{1 + x}{2\alpha}\left(\frac{\alpha}{1 + x} + c - y + \nu s(x,y)\right),$$

where $\nu > 0$ is the network effect parameter. When solved, the above results in:

$$s(x,y) = \frac{1}{2} - \frac{(1 + x)(y - c - \frac{\nu}{2})}{2\alpha - \nu(1 + x)}.$$

Once again, this $s(x, y)$ can be substituted into the organization's objective function. Solving the organization's decision problem, we find that, similar to Proposition 1, the (β, γ)-space gets partitioned into three regions. Also, similar to Theorem 1, we can show that education and enforcement are complements in the circumvention region and substitutes in the no-circumvention region.

8 Managerial Implications

Security and assurance of IT have already taken the center-stage in an organization's IT policy and investment decisions. And, the issue of circumvention has simply added fuel to that fire. Typically, the failure to secure technology using technology has made organizations throw more money at acquiring even more technology (McGowan 2016). Our work shows that such a unidimensional approach to security might be pointless, and the time has come to recognize that the users of IT systems are often "the weakest link in information security" (Bulgurcu et al. 2010, p.523).

What implementable insights do we find? First, in Proposition 1, we see that there is a significant portion of the parameter space in which it may be optimal for the organization to tolerate some level of circumvention. This certainly explains the situation observed in many organizations today. Facing higher costs for education and enforcement, organizations often recognize the futility in trying to eradicate circumvention fully. Later, in Theorems 2 and 4, we show that there could be additional motivations for tolerating circumvention. Very interestingly, there could be incentives to allow some level of circumvention to persist even when education and enforcement are not costly. In particular, we show in Theorem 2 that, when hackers are strategic and specifically target vulnerable organizations, tolerating some circumvention—that is, allowing some level of vulnerability—is in fact optimal. This surprising result is a reminder that properly analyzing strategic interactions between different stakeholders and making right investment decisions in the context of IT security are perhaps best accomplished using game-theoretic concepts (Cavusoglu et al. 2008). The strategic interaction of interest here is the one between an organization and hackers targeting it strategically. Recognizing that strategic hackers would scale down on their hacking efforts as circumvention wanes, the organization may no longer feel the pressure to eradicate circumvention fully. As long as the circumvention level can be controlled and kept sufficiently small, the declining threat from hackers allows the organization to tolerate circumvention to an extent. The implication is clear.

There is no need for the organization to get carried away in its anti-circumvention measures, and, for an IT manager, some moderation is recommended when dealing with the issue. This same sentiment is echoed even when we extend our analysis to the case where users experience a marginal circumvention cost. As shown in Theorem 4, there as well, the no-circumvention region disappears completely. Overall, our research suggests that a zero-tolerance policy may not be appropriate in the context of circumvention. Although addressing the issue is important and keeping it in control should be a priority, overzealous enforcement efforts could easily be futile.

Second, in Proposition 2 and later in Propositions 4 and 5, we learn that neither approach to curb circumvention dominates the other, and they work best in combination, not in isolation. It is certainly important to raise the awareness level about security policies, their necessity and the intended purpose, and the ramifications of circumventing them. However, organizations need not immediately and fully shift their focus away from enforcement activities and adopt education as the only anti-circumvention strategy. The role of education—creating awareness among users from different walks—has long been recognized (Bowen et al. 2006, D'Arcy et al. 2009, Guttman and Roback 1995, Wilson and Hash 2003). Likewise, the role of enforcement in deterring noncompliance has also received considerable support (Straub and Nance 1990, Kankanhalli et al. 2003). Therefore, our result essentially echoes those from prior research that circumvention is best addressed when both the approaches are used in a judicious mix. Of course, this work, based on a positive modeling experiment, does not shed much light on what a judicious mix should constitute, but it does highlight some of its characteristics.

The most notable of the above characteristics—the non-monotonicity of x^* with respect to γ or, equivalently, the non-monotonicity of y^* with respect to β, in Proposition 3—is quite counterintuitive. And, it has a clear, actionable implication. It tells us that the strategy an organization might undertake in the face of circumvention can suddenly change once circumvention is eradicated. The implication for a manager is as follows. When dealing with widespread user circumvention, the organization must invest in both education and enforcement. As the investment in enforcement is stepped up, the manager must also increase the investment in education to reap the full deterring effect of enforcement. However, once the organization has achieved the desired level of mitigation of user circumvention, the manager may relent in one of the two approaches; instead of pressing on both fronts, the manager should now emphasize the cheaper of the two while substituting away

from the more expensive one. Thus, an organization's education and enforcement policies, along with its broader security policies, need to evolve over time.

As discussed above, when strategic hackers are considered, the no-circumvention region disappears, as it is then never optimal to fully eradicate circumvention. However, the insight that education and enforcement are best viewed as complements in the face of widespread circumvention, but as substitutes of each other after circumvention has been effectively dealt with, remains applicable; see Theorem 3. In fact, this insight is quite robust and continues to hold even when issues such as network effect are considered. Only in instances in which circumvention involves a marginal cost borne by the user, does the problem get somewhat intuitive, with education and enforcement becoming substitutes of each other across the entire parameter space. Overall, the message seems quite clear. In many practical situations, facing severe threats from circumvention, the manager should divide organizational resources between enforcement and education. However, once circumvention dips to a sufficiently low level, the two approaches no longer complement each other; each then becomes a substitute for the other. So, investing more in both in lockstep no longer makes a good economic sense, and not recognizing this subtle point could lead the manager to allocate resources inefficiently.

For easy side-by-side comparison, we now summarize the results from the basic and all the extended model setups in Table 1. This table clearly highlights two of the main takeaways from

Table 1: A Summary of Results

	Model Setting				**Model Results**			
Model No.	Strategic Hackers?	Marginal Cost?	Spill-over Effect?	Network Effect?	Circum-vention?	No Circum-vention?	Substi-tutes?	Comple-ments?
1	No	No	No	No	Yes	Yes	Yes	Yes
2	Yes	No	No	No	Yes	No	Yes	Yes
3	No	Yes	No	No	Yes	No	Yes	Yes
4	No	No	Yes	No	Yes	Yes	Yes	Yes
5	No	No	No	Yes	Yes	Yes	Yes	No

this exercise. First, there are situations under which the organization is better off tolerating some circumvention and not eradicating it fully. Second, as anti-circumvention policies, education and enforcement may act as strategic complements, or as strategic substitutes, depending on the actual context.

9 Conclusion

Deliberate circumvention by its employees can pose significant security risks to an organization. Our work shows that investing in enforcement activities alone to mitigate such behavior could be futile, especially if it is not accompanied by proper education to increase the level of awareness among users. It has long been recognized that technology for the sake of technology does not work, and creating awareness among users is an important direction towards effective security control (Blythe et al. 2013, Bowen et al. 2006, D'Arcy et al. 2009). In recent times as well, there has been a growing recognition among industry professionals of the key role played by user awareness and training. Our results seem to echo this sentiment by highlighting the need to have appropriate educational programs.

Although set up to investigate security circumvention by employees, it is difficult to ignore the broader connotations of our work in a more general context. Indeed, as mentioned in the introduction, the use of education and enforcement to counter noncompliance of a law or policy is widespread, and the debate surrounding their relative efficacy has been a fundamental one. While prior research has done a good job of looking at different aspects of this issue empirically, not much attention has been placed on studying the joint economic impact of the two approaches in a holistic manner. Our microeconomic framework can provide a template for such an investigation. Of course, the model details would be somewhat different from one context to another, and the results may also vary to an extent. However, we expect that the key insights from our exercise—(i) the presence of noncompliance to some degree, (ii) the need to deploy education and enforcement together, and (iii) the presence of some complementarity between them at high levels of noncompliance and substitutability at low levels—to survive in many other real-world contexts.

Our basic model setup makes certain simplifying assumptions. For example, we assume that the impacts of the two approaches, education and enforcement, on the distribution of users' net benefit are very distinct. One impacts the mean, while the other, the variance. This abstraction is a simplification as, in reality, they both can influence the mean and variance at the same time. Our extended analysis shows that, even if these second-order spillover effects are accounted for, our earlier insights carry over. Similarly, our basic model does not consider the network effect that might arise from circumventing users influencing other users to join the bandwagon. Our extended

analysis again finds that the results remain qualitatively quite similar when such network effects are taken into account.

There are a few limitations of this work. For example, we do not consider any budget constraints in dealing with circumvention while, in practice, organizations often contend with limited budget available for investing in education and enforcement. Also, in our setup, a user's circumventing behavior is considered to be dependent only on the education and enforcement levels. However, in reality, such behavior is likely to be more dynamic. As users learn new tricks and gets more information, it is quite possible that their behavior would change—some users may migrate from the circumventing segment to the non-circumventing one and vice versa. As long as the two migrating groups are about the same size, the expected level of circumvention would remain the same, so our analysis would continue to hold. If these two groups evolve differently, however, our results may over- or under-estimate this level. Without a rigorous analysis, it is difficult to speculate how that might impact our results in a dynamic fashion. Despite these limitations, the purpose of this work would be amply served if it has succeeded in drawing attention to the need for educating users in the interconnected business environment of today. Perhaps, McGowan (2016) is correct when she concludes, "Institutions cannot hesitate in the goal to educate their employees."

References

Anderson, R., T. Moore. 2006. The economics of information security. *Science* **314**(5799) 610–613.

Beautement, A., M.A. Sasse, M. Wonham. 2008. The compliance budget: Managing security behavior in organisations. *Proceedings of the 2008 New Security Paradigms Workshop*. Lake Tahoe, CA, 47–58.

Blythe, J., R. Koppel, S.W. Smith. 2013. Circumvention of security: Good users do bad things. *IEEE Security and Privacy* **11**(5) 80–1720.

Bowen, P., J. Hash, M. Wilson. 2006. Information security handbook: A guide for managers. NIST Special Publication 800-100. URL `https://www.nist.gov/publications/information-security-handbook-guide-managers`. Accessed May 2, 2017.

Bulgurcu, B., H. Cavusoglu, I. Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* **34**(3) 487–502.

Caldwell, F. 2016. Why sharing passwords is now illegal and what this means for employers and digital businesses. Forbes. URL `https://www.forbes.com/sites/ciocentral/2016/08/23/why-sharing-passwords-is-now-illegal-and-what-this-means-for-employers-and-digital-businesses/#3a46e3ff3a46`. Accessed May 9, 2017.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2005. The value of intrusion detection systems in information technology security architecture. *Information Systems Research* **16**(1) 28–46.

Cavusoglu, H., S. Raghunathan, W.T. Yue. 2008. Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems* **25**(2) 281–304.

D'Arcy, J., A. Hovav, D. Galletta. 2009. Hacker behavior, network effects, and the security software market. *Information Systems Research* **20**(1) 79–98.

Dey, D., A. Lahiri, G. Zhang. 2012. Hacker behavior, network effects, and the security software market. *Journal of Management Information Systems* **2**(2) 77–108.

Feighery, E., D.G. Altman, G. Shaffer. 1991. The effects of combining education and enforcement to reduce tobacco sales to minors. *Journal of the American Medical Association* **266**(22) 3168–3171.

Goodchild, J. 2010. Workarounds: 5 ways employees try to access restricted sites. CSOOnline. URL `http://www.csoonline.com/article/2125818/access-control/workarounds--5-ways-employees-try-to-access-restricted-sites.html`. Accessed on May 2, 2017.

Gordon, L.A., M.P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* **5**(4) 438–457.

Gordon, L.A., M.P. Loeb. 2006. Budgeting process for information security expenditures. *Communications of the ACM* **49**(1) 121–125.

Guttman, B., E. Roback. 1995. An introduction to computer security: the nist handbook. NIST Special Publication 800-12. URL `https://www.nist.gov/publications/introduction-computer-security-nist-handbook`. Accessed May 2, 2017.

Harrison, M., R. Koppel, S. Barlev. 2007. Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *Journal of the American Medical Informatics Association* **14**(5) 542–549.

Heckle, R.R. 2011. Security dilemma: Healthcare clinicians at work. *IEEE Security and Privacy* **9**(6) 14–19.

Herath, H.S.B., T.C. Herath. 2008. Investments in information security: A real options perspective with bayesian postaudit. *Journal of Management Information Systems* **25**(3) 337–375.

Herley, C. 2009. So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 New Security Paradigms Workshop*. Oxford, UK, 133–144.

Kankanhalli, A., H.-H. Teo, B.C.Y. Tan, K.-K. Wei. 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management* **23**(2) 139–154.

Kelly, M. 2017. 3 steps to elevating corporate security. CIO Review. URL `https://rsa-security.cioreview.com/cioviewpoint/3-steps-to-elevating-corporate-security-nid-10584-cid-151.html`. Accessed Jan 12, 2018.

Kirlappos, I., M.A. Sasse. 2014. What usable security really means: Trusting and engaging users. *Proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust*. Crete, Greece, 69–78.

Koppel, R., S. Smith, J. Blythe, V. Kothari. 2015. Workarounds to computer access in healthcare organizations: You want my password or a dead patient? *Studies in Health Technology and Informatics*, vol. 208. IOS Press, 215–220.

Koppel, R., T. Wetterneck, J.L. Telles, B.-T. Karsh. 2008. Workarounds to barcode medication administration systems: Their occurrences, causes, and threats to patient safety. *Journal of the American Medical Informatics Association* **15**(4) 408–423.

Kothari, V., J. Blythe, S. Smith, R. Koppel. 2014. Agent-based modeling of user circumvention of security. *Proceedings of the 1st International Workshop on Agents and Cybersecurity*. Paris, France.

Lee, C.H., X. Gang, S. Raghunathan. 2016. Mandatory standards and organizational information security. *Information Systems Research* **27**(1) 70–86.

McGowan, J. 2016. Stop throwing money at cybersecurity. Banking Blog. URL `http://bankingblog.celent.com/2016/10/12/stop-throwing-money-at-cybersecurity/`. Accessed May 2, 2017.

Morgan, S. 2016. Worldwide cybersecurity spending increasing to $170 billion by 2020. Forbes. URL `https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#5f8913876832`. Accessed May 4, 2017.

Myyry, L., M. Siponen, S. Pahnila, T. Vertiainen, A. Vance. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* **18**(2) 126–139. doi:10.1057/ejis.2009.10.

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

Rajavel, M. 2017. Rethinking your cybersecurity approach: Thoughts from a CIO. CSO Online. URL `https://www.csoonline.com/article/3238847/security/rethinking-your-cybersecurity-approach-thoughts-from-a-cio.html`. Accessed Jan 12, 2018.

Ransbotham, S., S. Mitra. 2009. Choice and chance: A concepual model of paths to information security compromise. *Information Systems Research* **20**(1) 121–139.

Schick, S. 2017. Insider threats account for nearly 75 percent of security breach incidents. Security Intelligence. URL `https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/`. Accessed January 29, 2018.

Silverman, L. 2017. Turning to VPNs for online piracy? You might be putting your data at risk. National Public Radio. URL `https://www.npr.org/sections/alltechconsidered/2017/08/17/543716811/turning-to-vpns-for-online-privacy-you-might-be-putting-your-data-at-risk`. Accessed Jan 12, 2018.

Siponen, M., A. Vance. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* **34**(3) 487–502.

Straub, D.W., Jr. 1990. Effective is security: An empirical study. *Information Systems Research* **1**(3) 255–276.

Straub, D.W., Jr., W.D. Nance. 1990. Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly* **14**(1) 45–60.

Straub, D.W., Jr., R.W. Welke. 1998. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* **22**(4) 441–469.

Sundaram, R.K. 1996. *A First Course in Optimization Theory*. Cambridge University Press, Cambridge, UK.

Upton, D.M., S. Creese. 2014. The danger from within. Harvard Business Review. URL `https://hbr.org/2014/09/the-danger-from-within`. Accessed May 6, 2017.

Varian, H. R. 2000. Managing online security risks. *The New York Times* URL `http://www.nytimes.com/library/financial/columns/060100econ-scene.html`.

Walsh, L.M. 2004. Making an example: Enforcing company information security policies. SearchSecurity.com. URL `http://searchsecurity.techtarget.com/Making-an-example-Enforcing-company-information-security-policies`. Accessed May 2, 2017.

Wilson, M., J. Hash. 2003. Building an information technology security awareness and training program. NIST Special Publication 800-50. URL `https://www.nist.gov/publications/building-information-technology-security-awareness-and-training-program`. Accessed May 2, 2017.

Proofs

Proofs of Propositions 1 and 2

Circumvention Region: Note that:

$$z_x = \frac{\partial z}{\partial x} = \frac{\mu(y-c)}{2\alpha} - \beta x \quad \text{and} \quad z_y = \frac{\partial z}{\partial y} = \frac{\mu(1+x)}{2\alpha} - \gamma y.$$

Simultaneously equating the derivatives above to zero leads to the following interior solution:

$$x^* = \frac{\mu(\mu - 2\alpha c\gamma)}{4\alpha^2\beta\gamma - \mu^2} \quad \text{and} \quad y^* = \frac{\mu(2\alpha\beta - c\mu)}{4\alpha^2\beta\gamma - \mu^2}.$$

Since $c < 0$, the numerators in both the above expressions are positive. Therefore, the above interior solution is valid only if $4\alpha^2\beta\gamma - \mu^2 > 0$, or equivalently, if $\beta\gamma - \frac{\mu^2}{4\alpha^2} > 0$. If not, we get the boundary solution of $x^* = y^* = 0$.

Now, $\frac{\partial^2 z}{\partial x^2} = -\beta < 0$, and $\frac{\partial^2 z}{\partial x^2} \times \frac{\partial^2 z}{\partial y^2} - \left(\frac{\partial^2 z}{\partial x \partial y}\right)^2 = \beta\gamma - \frac{\mu^2}{4\alpha^2}$, which is positive whenever the interior solution is valid. Therefore, the second-order condition is automatically satisfied for this solution.

The solution above assumes that $s(x^*, y^*) \geq 0$ (that is, the condition $s(x, y) \geq 0$ is not binding or barely binding). Substituting the above x^* and y^*, this condition can be expressed as

$$\frac{1}{2} + \frac{\left(1 + \frac{\mu(2\alpha c\gamma - \mu)}{\mu^2 - 4\alpha^2\beta\gamma}\right)\left(c - \frac{\mu(c\mu - 2\alpha\beta)}{\mu^2 - 4\alpha^2\beta\gamma}\right)}{2\alpha} \geq 0,$$

Solving the above as an equality, we get two roots for β:

$$\beta_1 = \frac{1}{2\alpha} \times \frac{\mu^3}{\gamma\left(2\alpha\left(\gamma c^2 + \mu\right) - c\mu\right) + \sqrt{\gamma\left(\gamma c^2 + 2\mu\right)\left(2\alpha\gamma c - \mu\right)^2}},$$
$$\beta_2 = \frac{1}{2\alpha} \times \frac{\mu^3}{\gamma\left(2\alpha\left(\gamma c^2 + \mu\right) - c\mu\right) - \sqrt{\gamma\left(\gamma c^2 + 2\mu\right)\left(2\alpha\gamma c - \mu\right)^2}}.$$

Now, if $\gamma > \frac{\mu}{2\alpha(c+\alpha)}$, $\beta_2 > 0$ and $s(x^*, y^*) \geq 0$ becomes equivalent to $\beta \geq \beta_2$ or $\beta \leq \beta_1$. On the other hand, if $\gamma \leq \frac{\mu}{2\alpha(c+\alpha)}$ or $\mu \geq 2\alpha\gamma(c+\alpha)$, $s(x^*, y^*) \geq 0$ becomes equivalent to $\beta \leq \beta_1$ because then β_2 is negative. However, the condition $\beta \leq \beta_1$ is always irrelevant. This is because $\beta_1 - \frac{\mu^2}{4\alpha^2\gamma} = \mu^2\phi(\mu)$, where

$$\phi(\mu) = \frac{1}{2\alpha} \times \frac{\mu}{\gamma\left(2\alpha\left(\gamma c^2 + \mu\right) - c\mu\right) + \sqrt{\gamma\left(\gamma c^2 + 2\mu\right)\left(2\alpha\gamma c - \mu\right)^2}} - \frac{1}{4\alpha^2\gamma}$$

is a decreasing function of μ, and at $\mu = 2\alpha\gamma(c+\alpha)$, $\phi(\mu)$ equals $-\frac{1}{8\alpha^2\gamma + 4\alpha c\gamma}$. Therefore, for $\mu > 2\alpha\gamma(c+\alpha)$, $\phi(\mu)$ is negative, which in turn implies that $\beta_1 < \frac{\mu^2}{4\alpha^2\gamma}$. Now, if $\beta < \beta_1$, we would have $\beta < \frac{\mu^2}{4\alpha^2\gamma}$, which is impossible since that would imply that x^* and y^* above are also negative.

Taken together, for the above x^* and y^* to provide a valid interior maximum, we must have $\beta > h_1(\gamma)$ where $h_1(\gamma)$ is as defined in the proposition statement. Now, suppose $\beta > h_1(\gamma)$ and the interior maximum

is valid. Then, the maximum value corresponding to this solution is:

$$z(x^*, y^*) = \frac{8\alpha^2\beta\gamma - 4\alpha\beta\gamma(\alpha + c)\mu + \left(\beta + \gamma c^2 - 2\right)\mu^2 + \mu^3}{2(4\alpha^2\beta\gamma - \mu^2)}.$$

This value must exceed 0 for the control to be desirable. Since $\beta\gamma > \frac{\mu^2}{4\alpha^2}$ (necessary for x^* and y^* to be positive), we require that

$$8\alpha^2\beta\gamma - 4\alpha\beta\gamma(\alpha + c)\mu + \left(\beta + \gamma c^2 - 2\right)\mu^2 + \mu^3 \geq 0,$$

which is equivalent to

$$\beta \leq \frac{\mu^2\left(2 - \gamma c^2 - \mu\right)}{8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha)} \quad \text{and} \quad 8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha) < 0, \quad \text{or}$$
$$\beta \geq \frac{\mu^2\left(2 - \gamma c^2 - \mu\right)}{8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha)} \quad \text{and} \quad 8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha) > 0.$$

However, the second condition is irrelevant. Further, when $8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha) < 0$, μ is between μ_1 and μ_2 where:

$$\mu_1 = 2\alpha\left(\gamma(\alpha + c) - \sqrt{\gamma\left(\gamma(\alpha + c)^2 - 2\right)}\right) \quad \text{and} \quad \mu_2 = 2\alpha\left(\gamma(\alpha + c) + \sqrt{\gamma\left(\gamma(\alpha + c)^2 - 2\right)}\right).$$

Now, note that $\mu_1 > (2 - \gamma c^2)$ because

$$\left(2\alpha\gamma(\alpha + c) - (2 - \gamma c^2)\right)^2 - 4\alpha^2\gamma\left(\gamma(\alpha + c)^2 - 2\right) = \left(2 - \gamma c(c + 2\alpha)\right)^2.$$

Therefore, $\mu > \mu_1$ implies that $\mu > (2 - \gamma c^2)$, which in turn implies that $\frac{\mu^2\left(2 - \gamma c^2 - \mu\right)}{8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha)} < 0$. Since β is a positive parameter, $\beta \geq \frac{\mu^2\left(2 - \gamma c^2 - \mu\right)}{8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha)}$ would be trivially true. In other words, the only relevant constraint is $\beta \leq \frac{\mu^2\left(2 - \gamma c^2 - \mu\right)}{8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha)}$, which is required when $8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha) < 0$. Recognizing that $8\alpha^2\gamma + \mu^2 - 4\alpha\gamma\mu(c + \alpha) = 4\alpha\gamma(c\mu + \alpha(\mu - 2)) - \mu^2$, it becomes obvious that we need $\beta \leq h_2(\gamma)$ for the interior solution to be superior to not having any control in place whatsoever.

Altogether, it is clear that $\{x^*, y^*\}$ is both valid and optimal when $h_1(\gamma) \leq \beta \leq h_2(\gamma)$.

No-Circumvention Region: It is clear from the above that no interior solution exists when $\beta < h_1(\gamma)$. Therefore, $s(x, y) = 0$ must bind. This leads to $y = c + \frac{\alpha}{1 + x}$. Substituting this into z and taking the first order condition with respect to x, we get

$$z_x = \frac{\partial z}{\partial x} = \frac{\alpha\gamma(c(1 + x) + \alpha)}{(1 + x)^3} - x\beta = 0.$$

This equation above can be rewritten as $\phi(r) = r^4\beta - \beta r^3 - \alpha c\gamma r - \alpha^2\gamma = 0$, where $r = 1 + x$. The discriminant of $\phi(r)$ can be expressed as

$$-\alpha^3\beta^2\gamma^2\left(27\alpha\beta^2 + 2\left(2c^2(c + \alpha) - 5c\alpha(c - \alpha) + 91\alpha^2(c + \alpha) + 37\alpha^3\right)\beta\gamma + 27c^4\alpha\gamma^2\right).$$

Since $c < 0$ and $c + \alpha > 0$, this discriminant is negative. Therefore, there are two real roots. Now, since $\phi(r)$ goes to ∞ when either $r \to -\infty$ or $r \to \infty$, and $\phi(r)$ is negative when $r = 0$, it is immediate that there is only one positive real root. It is to verify that this real root provides the solution to the optimization

problem when $s(x,y)=0$ is binding.

No Control Region: As discussed above, the interior solution is clearly inferior to doing nothing when $\beta > h_2(\gamma)$. ■

Proof of Proposition 3

Circumvention Region: In this region:

$$\frac{\partial x^*}{\partial \beta}=\frac{4\alpha^2\gamma\mu(2\alpha c\gamma-\mu)}{\left(4\alpha^2\beta\gamma-\mu^2\right)^2},\quad \frac{\partial x^*}{\partial \gamma}=\frac{2\alpha\mu^2(c\mu-2\alpha\beta)}{\left(4\alpha^2\beta\gamma-\mu^2\right)^2},\quad \frac{\partial y^*}{\partial \beta}=\frac{2\alpha\mu^2(2\alpha c\gamma-\mu)}{\left(4\alpha^2\beta\gamma-\mu^2\right)^2},\quad \text{and}\quad \frac{\partial y^*}{\partial \gamma}=\frac{4\alpha^2\beta\mu(c\mu-2\alpha\beta)}{\left(4\alpha^2\beta\gamma-\mu^2\right)^2}.$$

Since $c<0$, all these derivatives are negative.

No-Circumvention Region: We use the implicit function theorem:

$$\frac{\partial x^*}{\partial \beta}=-\frac{\frac{\partial z_x}{\partial \beta}\Big|_{x=x^*}}{\frac{\partial z_x}{\partial x}\Big|_{x=x^*}},$$

where x^* solves $z_x=\frac{\partial z}{\partial x}=0$. Now, recall from the proof of Proposition 1 that $z_x=\frac{\alpha\gamma(c(1+x)+\alpha)}{(1+x)^3}-x\beta$, which means that $\frac{\partial z_x}{\partial \beta}\Big|_{x=x^*}=-x^*<0$. Further, $\frac{\partial z_x}{\partial x}\Big|_{x=x^*}$ is negative because x^* must satisfy the second-order condition for it to be a maximum. Hence, $\frac{\partial x^*}{\partial \beta}$ must be negative.

Recall that $s(x,y)=0$ binds in the no-circumvention region, implying that $y^*=c+\frac{\alpha}{x^*+1}$. Since $\frac{\partial x^*}{\partial \beta}$ is negative, $\frac{\partial y^*}{\partial \beta}$ ought to be positive.

Also, from the implicit function theorem, we can also find that:

$$\frac{\partial x^*}{\partial \gamma}=-\frac{\frac{\partial z_x}{\partial \gamma}\Big|_{x=x^*}}{\frac{\partial z_x}{\partial x}\Big|_{x=x^*}}.$$

Further, it follows from the first-order condition that $\frac{\alpha\gamma(c(1+x^*)+\alpha)}{(x^*+1)^3}-\beta x^*=0$. Therefore, $\frac{\partial z_x}{\partial \gamma}\Big|_{x=x^*}=\frac{\alpha(c(1+x^*)+\alpha)}{(x^*+1)^3}=\frac{\beta x^*}{\gamma}>0$. Also, $\frac{\partial z_x}{\partial x}\Big|_{x=x^*}$ is negative because x^* is a maximum. Hence, $\frac{\partial x^*}{\partial \gamma}$ must be positive in the circumvention region.

Since $y^*=c+\frac{\alpha}{x^*+1}$ holds in the no-circumvention region, and since $\frac{\partial x^*}{\partial \gamma}$ is positive there, $\frac{\partial y^*}{\partial \gamma}$ ought to be negative.

No-Control Region: The optimal x and y are both zero in the no-control region, and β and γ have no impact on these optimal values. ■

Proof of Theorem 1

Circumvention Region: Taking derivative of the organization's objective function, z, with respect to x and y, we find that:

$$\frac{\partial^2 z}{\partial x\partial y}=\frac{\mu}{2\alpha}>0.$$

From Theorem 10.4 in (Sundaram 1996, p.257), we know that z is supermodular in x and y. Then, from Theorem 10.6 in (Sundaram 1996, p.258), we can see that x^* and y^* always increase or decrease together, making them complements of each other.

No-Circumvention Region: In this region, $s(x,y)=0$ implying that $y^* = c + \frac{\alpha}{x^*+1}$. It is clearly visible from this relationship that y^* decreases with x^* and vice versa. ■

Proof of Lemma 1

This lemma follows from the direct substitution of the damage caused by hackers into the organization's net benefit from the control. ■

Proof of Theorem 2

The no-circumvention outcome in Proposition 1 is a boundary solution and applies only to the region where the interior solution violates the constraint that $s(x,y) \geq 0$. However, this constraint is never violated when hackers are strategic. To prove it, assume that there exists an interior solution $(\hat{x},\hat{y})$ to the organization's decision problem with $s(\hat{x},\hat{y}) < 0$. Then:

$$\left.\frac{\partial z}{\partial x}\right|_{x=\hat{x},y=\hat{y}} = \frac{\mu^2(\hat{y}-c)s(\hat{x},\hat{y})}{\alpha\eta} - \beta\hat{x} \quad \text{and} \quad \left.\frac{\partial z}{\partial y}\right|_{x=\hat{x},y=\hat{y}} = \frac{\mu^2(1+\hat{x})s(\hat{x},\hat{y})}{\alpha\eta} - \gamma\hat{y}.$$

Since $c<0$ and $s(\hat{x},\hat{y})<0$, it is easy to see that the partial derivatives above are both negative, contradicting our assumption that $(\hat{x},\hat{y})$ is an interior solution. Therefore, all interior solutions automatically abide by the constraint $s(x,y)\geq 0$, and the corner solution of no circumvention is subsumed by an interior solution. ■

Proof of Proposition 4

Since $\frac{\partial^2 z}{\partial y^2} = -\gamma - \frac{\mu^2(1+x)^2}{2\alpha^2\eta} < 0$, for any given $x>0$, we can solve the first order condition, $\frac{\partial z}{\partial y}=0$, to obtain:

$$y^* = \frac{\mu^2\,(1+x)\,(c\,(1+x)+\alpha)}{2\alpha^2\gamma\eta + \mu^2\,(1+x)^2}.$$

Substituting this into the profit function, we get:

$$z = \frac{\mu^2(1+x)^2\left(2-\beta x^2-c^2\gamma\right) - 2c\alpha\gamma\mu^2(1+x) - \alpha^2\gamma\left(\mu^2 - 2\eta\left(2-\beta x^2\right)\right)}{2\left(2\alpha^2\gamma\eta + \mu^2(1+x)^2\right)}.$$

Now, solving the first order condition with respect to x, we get the desired result. ■

Proof of Theorem 3

According to Theorems 10.4 and 10.6 in (Sundaram 1996, pp.257–258), $\frac{\partial^2 z}{\partial x \partial y}$ must be positive for x and y to be complements; if not, they will be substitutes. Now

$$\frac{\partial^2 z}{\partial x \partial y} = \frac{\alpha - 2(1+x)(y-c)}{2\alpha^2\eta}.$$

Therefore, the sign of the cross-derivative above is the same as that of $(\alpha - 2(1+x)(y-c))$. Therefore, in equilibrium, $\alpha - 2(1+x^*)(y^*-c) = 0$ becomes the boundary separating the complementarity and substitutability regions. The theorem follows. ■

Proof of Lemma 2

This result follows from the direct substitution of the circumvention damage into the organization's net benefit from the control. ■

Proof of Theorem 4

The no-circumvention outcome in Proposition 1 is a boundary solution and applies only to the region where the interior solution violates the constraint that $s(x, y) \geq 0$. However, this constraint is never violated when users have a marginal cost for circumvention. To prove it, assume that there exists an interior solution $(\hat{x}, \hat{y})$ with $s(\hat{x}, \hat{y}) < 0$. Now, since $c < 0$, $s(\hat{x}, \hat{y})$ is negative if and only if $-(1+x)(c-y) > \alpha$ or $(1+x)^2(c-y)^2 > \alpha^2$. Then:

$$\left.\frac{\partial z}{\partial x}\right|_{x=\hat{x},y=\hat{y}} = -\frac{\mu\left((1+\hat{x})^2(c-\hat{y})^2 - \alpha^2\right)}{4\alpha\chi(1+\hat{x})^2} - \beta\hat{x} < 0 \quad \text{and} \quad \left.\frac{\partial z}{\partial y}\right|_{x=\hat{x},y=\hat{y}} = \frac{\mu\left((1+\hat{x})(c-\hat{y}) + \alpha\right)}{2\alpha\chi} - \gamma\hat{y} < 0.$$

Since the partial derivatives are both negative, they provide a contradiction to our assumption that $(\hat{x}, \hat{y})$ is an interior solution. Therefore, all interior solutions automatically abide by the constraint $s(x, y) \geq 0$, and the corner solution of no-circumvention disappears. ■

Proof of Proposition 5

Since $\frac{\partial^2 z}{\partial y^2} = -\gamma - \frac{\mu(1+x)}{2\alpha\chi} < 0$, for any given $x > 0$, we can solve the first order condition, $\frac{\partial z}{\partial y} = 0$, to obtain:

$$y^* = \frac{\mu\left(c\left(1+x\right) + \alpha\right)}{2\alpha\gamma\chi + \mu\left(1+x\right)}.$$

Substituting this into the profit function and solving the first order condition with respect to x, we get the desired result. ■

Proof of Theorem 5

According to Theorems 10.4 and 10.6 in (Sundaram 1996, pp.257–258), $\frac{\partial^2 z}{\partial x \partial y}$ must be positive for x and y to be complements; if not, they will be substitutes. Now, since

$$\frac{\partial^2 z}{\partial x \partial y} = -\frac{\mu(y-c)}{2\alpha\chi} < 0,$$

the result follows. ■

Additional Technical Details

Spillover Effects of Education and Entertainment

In this case, $s(x, y) = \frac{1}{2} - \frac{(1+x+\epsilon y)(y+\delta x-c)}{2\alpha}$, which can be substituted into:

$$z = \left(1 - \mu s(x, y) - \frac{\beta x^2}{2} - \frac{\gamma y^2}{2}\right).$$

Therefore, in the circumvention region, we get:

$$\frac{\partial^2 z}{\partial x \partial y} = \frac{\mu(1+\delta\epsilon)}{2\alpha} > 0.$$

According to Theorems 10.4 and 10.6 in (Sundaram 1996, pp.257–258), we can see that x and y are always complements in the circumvention region.

In the no-circumvention region, $s(x,y) = 0$, which implies that this boundary solution must abide by:

$$y = \frac{\sqrt{(1+x(1-\delta\epsilon)+c\epsilon)^2 + 4\alpha\epsilon} - (1+x(1+\delta\epsilon)-c\epsilon)}{2\epsilon}.$$

After some algebra, we can show that the right hand side of the above expression is a decreasing function of x, making x and y substitutes for each other in this region.

Network Effect

In this case, $s(x,y) = \frac{1}{2} - \frac{(1+x)(y-c-\frac{\nu}{2})}{2\alpha-\nu(1+x)}$, which is then be substituted into $z = \left(1 - \mu s(x,y) - \frac{\beta x^2}{2} - \frac{\gamma y^2}{2}\right)$. In the circumvention region, therefore:

$$\frac{\partial^2 z}{\partial x \partial y} = \frac{2\alpha\mu}{(2\alpha - \nu(1+x))^2} > 0.$$

Then, using Theorems 10.4 and 10.6 in (Sundaram 1996, pp.257–258), we can see that x and y are always complements in the circumvention region.

In the no-circumvention region, $s(x,y) = 0$, which implies that this boundary solution must abide by:

$$y = c + \frac{\alpha}{1+x},$$

clearly indicating substitutability between x and y in this region. Viewed alternatively, when $s(x,y) = 0$, the network effect disappears, and we get back the result of the basic model.