Managing Information Access in Data-Rich Enterprises with Escalation and Incentives

Xia Zhao and M. Eric Johnson

ABSTRACT: Managing information access in highly dynamic e-business environments is increasingly challenging. In large firms with thousands of employees accessing thousands of applications and data sources, managers must protect information against misuse but ensure that employees can access the information needed for value creation. An escalation scheme with audits to increase flexibility while maintaining security is proposed. By coupling incentives with controls, escalation aligns employees' self-interest with the firm's profit objective. A game-theoretic model shows that an incentives-based policy with escalation and audit can control both overentitlement and underentitlement while maintaining flexibility.

KEY WORDS AND PHRASES: Access control, audit, e-business, e-commerce, economic analysis, entitlement, escalation policy, information security, information systems.

The innovations of e-business have enabled firms to link their internal and external systems, making it possible to work more closely with customers, suppliers, and partners [12, 31]. As a result, enterprise information systems (IS) contain vast amounts of e-commerce-generated customer data as well as process data from throughout the supply chain. Likewise in the service sector, such as banking and health care, organizations can assemble diverse customer data from many sources, providing service providers with a more complete picture of customer needs. However, managers of such data-rich enterprises often find themselves struggling to ensure that employees have access to pertinent and timely information. The benefits of information access are largely unchallenged. For example, the literature on innovation has long discussed the benefits of free-flowing information, linking it to innovation productivity (e.g., [5, 38, 39]). Likewise, the services and supply chain literatures also extol the benefits of increased information availability (e.g., [25, 28, 32]). For example, in many retail supply chains, manufacturers and retailers often share forecast information and jointly develop forecasts and replenishment plans (e.g., Wal-Mart and Warner-Lambert). Over the past ten years, firms have invested heavily in information systems to enable timely access to information.

However, wide information access also comes at a risk. Unfettered information access provides insiders and cyberattackers with opportunities to misap-

This research was supported by the Institute for Security Technology Studies at Dartmouth College, under award Number 2006-CS-001-000001 from the U.S. Department of Homeland Security (NCSD). The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the Department of Homeland Security. We are grateful for helpful comments on earlier versions of this work from participants of the Hawaii International Conference on System Sciences (HICSS) and the Workshop on the Economics of Information Security (WEIS).

International Journal of Electronic Commerce / Fall 2010, Vol. 15, No. 1, pp. 79–111.

1086-4415/2010 $9.50 + 0.00.
DOI 10.2753/JEC1086-4415150104

propriate or corrupt an organization's data sources. According to the CSI 2008 Computer Crime and Security Survey, 29 percent of respondents reported experiencing unauthorized access to information. In addition, identity and access control was listed as a top issue facing enterprise security managers [33]. In addition, managers are under pressure to comply with various government regulations, such as the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data-Security Standard (PCI/DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Personal Information Protection and Electronic Documents Act (PIPEDA), and the European Union Directive on Data Privacy (EU Directive), which all include language requiring firms to maintain some level of access control. Driven by fears of data breaches, intellectual property losses, and compliance violations, firms are working to reduce information access through better controls and governance [18].

Managers face the challenge of finding the right balance between availability and security. On one hand, controls can eliminate unauthorized data access. The current practice of access control focuses on the technical implementation of privileges. For example, access controls dictate users' privileges to view a file, execute an application, share data with other agents, and so on. Users can only use data when they have the corresponding entitlement.[1] The goal of such access control is to prevent misuse of data—whether intentional (e.g., using data to make illegal stock trades) or unintentional (e.g., storing data on a device vulnerable to a security breach). On the other hand, control should not become a barrier to value creation. Anecdotal evidence suggests that many users bypass annoying security rules in order to accomplish their tasks. This paper explores the use of incentives, application escalation, and audit to improve information availability while protecting against misuse.

Under the so-called rule of least access, a popular criterion of access control, agents are provided with the minimum entitlements needed to perform their respective roles [3, 10]. To enforce the rule of least access, user access profiles must be customized through an access-control system. In practice, a typical access-control system includes five components—request, approve, administer, enforce, and monitor. Specifically, a user requests an entitlement; the owner examines the request and then approves or rejects it; the administrator modifies the user's entitlements; the user accesses the resource and the system logs the user's activities; and the auditor examines the logs and evaluates the user's activities. Figure 1 shows an access-control system with the rule of least access.

However, the rule of least access is limiting in situations where it is difficult to foresee all information needs in advance. For example, in a hospital setting, emergencies arise where an attending physician may unexpectedly have to care for another doctor's patient. In increasingly dynamic environments, organizations frequently face unanticipated situations and have to adjust their organizational structures and personnel to adapt to consumers' needs. In a field study of an investment bank, Sinclair et al. found that a business group of 3,000 people witnessed 1,000 changes to organizational structure within just a few months [36].[2] The grant of an entitlement typically requires significant interaction among users, resource owners, and administrators. In large

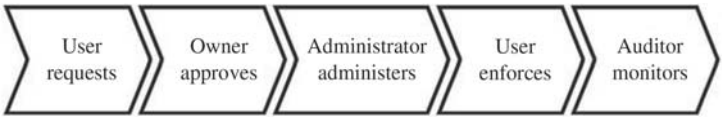


Figure 1. Access System with the Rule of Least Privilege

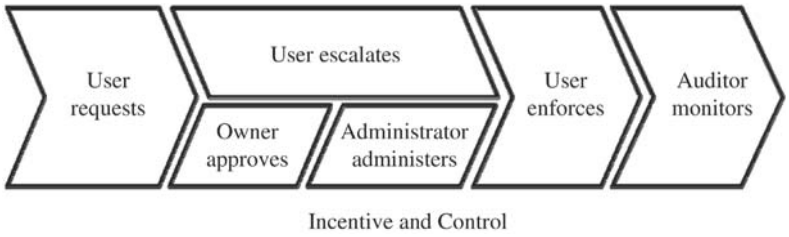


Figure 2. Access System with Escalation, Audit, and Incentives

organizations with thousands of users interacting with thousands of different applications and data sources, each having many levels of privilege, the assignment of access is laborious. Often, business opportunities are missed or service quality is degraded because of delays in an organization's response to user requests. In addition, employees' access must be continually updated and audited to remain in synchronization with the changing organization to ensure least access. Such maintenance of access is daunting.

Likewise, flexibility is also a requisite in today's e-business environment, where organizations frequently face unanticipated situations. In practice, flexible access is sometimes achieved by "overentitlement." For example, in the banking context mentioned earlier, Sinclair et al. found that from 50 to 90 percent of employees were overentitled [36]. This practice is rationalized by the argument that long-term employees are valuable and need quick access to information to create value for the firm. However, permanently overentitled employees also present a security risk to the organization because their accesses could be used maliciously or accidentally. While malicious insiders make the headlines, in many cases benign overentitled employees pose a much larger risk to themselves and the organization because of secondary vulnerabilities, as when an employee loses a laptop with sensitive data or a malicious hacker gains access to substantial firm information through a single overentitled account [19].

To achieve both control and flexibility, this paper considers an access system that includes escalation with audit and incentive schemes to drive appropriate behavior. The goal is to ensure that information systems deliver the right information to the right people at the right time, while protecting the information from misuse. Figure 2 shows a system with escalation, audit, and incentives. To eliminate opportunistic escalation behavior, incentive schemes are employed by coupling reward and penalty with access and escalation activities.

The solution framework is different from previous approaches in that it expands the scope of access management beyond simple controls to include

incentives and escalation. Employees are given a base level of access, and allowed to escalate into controlled data and applications when needed. This makes one-time access possible without any time-delaying approval process. Such an approach has been witnessed in several settings, including investment banking, where it is sometimes referred to as "override," and health care, where it is called "break the glass" [10, 34].

Unfortunately, escalation breeds significant security risks, since employees may abuse their rights (i.e., access information for personal benefit rather than business reasons). The associated security risks are mitigated by considering the case where escalation activities are later audited, and employees found to be abusing their access are penalized. Auditing (or monitoring) with violation penalties has been implemented by firms seeking to deter undesired behavior by employees or partners with respect to financial reporting and contract and regulation compliance. For example, Intel issues "speeding tickets" to employees who violate information security policies [18]. This approach empowers users to quickly respond to unanticipated situations and seize business opportunities while providing a measure of data security.

It is worth noting that escalation must be confined to cases where the risk of failure or the cost of recovery is relatively low compared to the cost of not granting access (e.g., the potential value created through escalation). It may not be suited to some financial or trading systems where there is significant risk of massive fraud. Rather, it is useful in cases where there are many small risks or where the potential value of escalation is very high. For example, escalation is very effective in situations such as access to private medical information, where emergency access may save someone's life, or in a time-critical system where the person with the necessary privileges may be unavailable [30].

Related Literature

The technological aspect of incorporating an escalation scheme into access control has been studied in the computer science literature. Povey discussed an optimistic access-control scheme with escalation and developed a formal model that ensures the integrity of computer systems including accountability, auditability, and recoverability [30]. Rissanen emphasized the importance of audit and manual recovery when access overrides are allowed [34]. Ferreira et al. described a design and initial implementation of a "break-the-glass" policy in a virtual electronic medical record system [10]. This paper focuses on the economic aspects of information access and proposes an incentive-based information access.

Cheng et al. proposed a fuzzy multilevel security (MLS) model that allows users to escalate within a specific region based on a risk and benefit analysis [8]. They focused on quantifying the risk-associated information access and partitioning risk bands for exceptional access. Escalation behavior, although briefly mentioned, was not explicitly modeled or analyzed. The paper considers users' incentives and applies a principal and agent setting to study the policy-design problem.

Principal-agent models have been examined in a variety of contexts (e.g., [1, 2, 4, 13, 15, 16, 35]). This paper closely relates to a large stream of literature that studies audit policies in a principal-agent framework. Townsend proposed one of the first models to examine the costs of verification [37]. Dye showed that optimal monitoring policies are deterministic and lower-tailed [9]. Kim and Suh also focused on deterministic monitoring policies in which the optimal investment in audit technology is endogenously determined [21]. They found that the lower-tailed policy is a special case. Baron and Besanko investigated random audit policies in a regulatory pricing setting where firms have private information about their cost functions that they are required to disclose to regulators [6]. They showed that the optimal audit policy includes the possibility that firms be penalized even in cases where they report their best knowledge (because of *ex post* uncertainty). Harris and Raviv explored random audit policies in capital budgeting and identified cases of overinvestment and underinvestment [14].

This paper uses the principal-agent framework in a novel context to better understand the value of escalation. In the model presented here, all escalation activities are monitored and audited (e.g., as required by regulators). The focus is on the firm's optimal strategies in response to audit results (e.g., penalties for misuse). Since a perfect audit is impossible or extremely costly to achieve, penalties by themselves are incapable of eliminating misuse. Thus it is necessary to also consider incorporating a reward scheme (e.g., a bonus) to alleviate the adverse consequences of imperfect monitoring. The optimal escalation scheme balances the need for flexibility against the risk to information security.

Modeling Escalation and Incentives

The discussion that follows examines the case where users gain access to data and applications through a system employing access control and where the user's actions are monitored to support auditing. The collection of applications and data is modeled as measured on a continuous scale of information, with each privilege weighted to reflect the amount and sensitivity of the data. The total weighted sum of information that could possibly be made available to an employee is A. Note that this does not include all firm information, as compliance and regulatory requirements make some data and applications off-limits. All the notation for the modeling and analysis is in Table 1.

Information Flows

Based on value generated by its employees and the associated information risk, the firm assigns employees a regular access level a on $[0, A]$ to perform routine tasks. However, employees occasionally observe business opportunities that are outside their routine duty. It is assumed that with probability γ, employees will observe such an opportunity and successfully create more value if they

Table 1. Notation Table.

Notation	Definition	Comments
A	Total weighted sum of information that could be made available to an employee	
a	Employee's regular information-access level	$a \in [0, A]$
γ	Probability of employee observing a business opportunity (or emergent task) outside his/her routine duty	
x	Information requirement of emergent task	x is distributed on $[0, A]$ following $F(x)$
e	Employee's escalated access level	
$U(a)$, $U(\min\{a + e, x\})$	Firm's value from employee's regular task and emergent task	
$u(a + e)$	Employee's private benefit	
$S(U(\min\{a + e, x\}))$	Employee's bonus from performing emergent task	
$R(a)$	Firm's cost of managing regular access level	A quadratic cost function is used, $R(a) = (1/2)sa^2$
$R_o(\max\{a + e - x, 0\})$	Firm's auditing cost associated with overentitlement	A quadratic cost function is used, $R_o(\max\{a + e - x, 0\}) = (1/2)\,t(\max\{a + e - x, 0\})^2$
$r(e)$	Employee's cost of escalation	A quadratic cost function is used, $r(e) = (1/2)\beta e^2$. In addition, $s, t > \beta > 1$.

$n_o(a, e, x, \varepsilon)$	Penalty for overentitlement	
$n_u(a, e, x, \varepsilon)$	Penalty for underentitlement	
B	Firm's unit value	
b	Employee's unit private benefit	We assume the private benefit function is linear, $u(a + e) = b(a + e)$
w	Bonus rate	We consider a linear bonus incentive, $S(U(\min\{a + e, x\})) = (w/B)U(\min\{a + e, x\})$
ε	Audit error	
p	Penalty rate for overentitlement	We consider the linear penalty incentive, $n_o(a, e, x, \varepsilon) = p[a + e - x - e]^+$
q	Penalty rate for underentitlement	We consider the linear penalty incentive, $n_u(a, e, x, \varepsilon) = q[x - (a + e) - \varepsilon]^+$
v	Employee's payoff	
V	Firm's profit	

Notes: s = cost coefficient for the firm's cost of managing regular access level. t = cost coefficient for the firm's auditing cost associated with overentitlement. β = cost coefficient for the employee's cost of escalation. $^+$ see note 4.

can access the requisite information. The information requirement of this business opportunity may or may not be beyond an employee's entitlement. The information required by the emergent task is represented as a random variable x, distributed $F(x)$ on $[0, A]$. In some cases, the information requirement of the emergent opportunity is within the employee's access level and thus the employee can seize the opportunity without any additional information. In other cases, the information requirement is greater than the employee's access level, and thus the firm's potential gain is limited unless the employee is allowed to temporarily escalate to a higher access level. The escalated access level is denoted by e. To mitigate the risk of unnecessary escalation, it is assumed that the firm audits each instance of escalation *ex post.*

Financial Flows

Research has shown that information technology may indeed contribute to improved organizational performance [7, 22, 29]. Information technology enables firms to gather information from various sources and provides timely access to information that is critical for value creation. Earlier work in banking observed that increased accessibility of information facilitated employee productivity [36]. In this paper, it is assumed that an employee's information access influences the firm's benefit from a business opportunity. In particular, it is assumed that a firm's net value from an employee's regular tasks is $U(a)$. The firm bears costs associated with the regular access level of $R(a)$, including security risks and routine auditing of regular access usage along with the technical support required to prudently maintain that access. It is assumed that $U(.)$ is an increasing and concave function [$U'(.) > 0$, and $U''(.) \leq 0$], and that $R(a)$ is an increasing and convex function [$R'(.) > 0$, and $R''(.) > 0$]. The firm's net value from emergent tasks is $U(\min\{a + e, x\})$.

Employees receive bonuses from the firm based on the value they create performing emergent tasks $S(U(\min\{a + e, x\}))$, where $S(.)$ is an increasing and concave function [$S'(.) > 0$, and $S''(.) \leq 0$]. In addition, employees also derive some private benefit both from regular access and from escalating into information beyond their regular access levels. Such private benefit may be the feeling of trust and power that comes from seeing the information. It may also make an employee's job more convenient by reducing dependence on supervisors or the need to ask others for access to privileged data. In some cases, employees may use information to plan personal purchases—for example, an employee of a retailer who has access to future promotional plans may postpone a purchase, knowing that a product will soon be on sale. This is something the employer may not discourage for employees, but information the firm would certainly not want leaking out to customers or competitors. Finally, the private benefit might simply be driven by curiosity. Such "snooping" value is not uncommon—instances have been witnessed in health care, where a provider may examine the records of a patient for its private benefit [11]. The employee's private benefit from escalation is $u(a + e)$, which depends on both the regular access level and the escalated access level; $u(.)$ is an increasing and concave

function [$u'(.) > 0$, and $u''(.) \leq 0$]. The employees bear the cost of $r(e)$ from the escalated access in terms of personal risk (the personal pain of being audited or having a security breach) and of the documentation required when escalating past their regular access. Higher levels of information include more risk and more complex documentation in the audit process. It is assumed that $r(e)$ is an increasing and convex function of e ($r'_e > 0$ and $r''_e > 0$).

Employees escalate their access levels to meet the information requirements of emergent tasks. Since employees are self-interested, an employee may escalate to a level higher or lower than the information requirement. If the employee's total access level, $a + e$, is higher than the information requirement, x, the employee is referred to as over-entitled in the discussion that follows, whereas risk-averse employees who choose not to escalate to the level needed to achieve the full emergent benefit are here referred to as under-entitled. It is assumed that all escalation requests receive a screening audit and that this initial audit cost is fixed, and thus not relevant to the model. However, if overentitlement is suspected, a more thorough investigation is required. For example, the firm would need to carefully verify the overentitlement before bringing any action. It would also need to document and evaluate the overentitlement, in compliance with SOX Section 404, which requires firms to assess the effectiveness of the internal control structure and procedures for financial reporting. This additional auditing cost related to overentitlement is represented with $R_o(\max\{a + e - x, 0\})$. $R_o(.)$ is an increasing and convex function ($R'_o(.) \geq 0$ and $R''_o(.) \geq 0$). But underentitlement degrades business performance, as represented in the firm's value function. To minimize overentitlement or underentitlement, the firm audits escalation activities and penalizes employees who abuse their rights or fail to escalate when opportunities arise. It is assumed that the firm can figure out the information requirement x e*x post* via communication with managers and co-workers of the employee. However, it is unable to accurately measure the access level required to fulfill the information requirement and hence unable to precisely detect the difference. The imperfect audit process is modeled as the firm does not take action unless the overentitlement or underentitlement exceeds a threshold ε. An employee who is overentitled will be penalized by the firm at a level $n_o(a, e, x, \varepsilon)$ and likewise $n_u(a, e, x, \varepsilon)$ for underentitlement.

The timing of events is shown in Figure 3. At Stage 1, the firm announces its access-management policy $\{a, S(.), n_o(.), n_u(.)\}$; at Stage 2, an employee observes the information requirement, x, and escalates to conduct the task. Finally, the firm investigates the escalation, rewarding or penalizing the employee according to the announced access-management policy.

The firm's access policy will influence the employee's escalation strategies, and, by backward induction, anticipation of the latter will influence the firm's policy design. Given the policy parameters of the firm, the employee chooses e to maximize the payoff for each business task, denoted by v. The employee's problem is

$$v = \max_e S\left(U\left(\min\left\{a+e, x\right\}\right)\right) + u(e) - r(e) - n_o(a, e, x, \varepsilon) - n_u(a, e, x, \varepsilon).$$

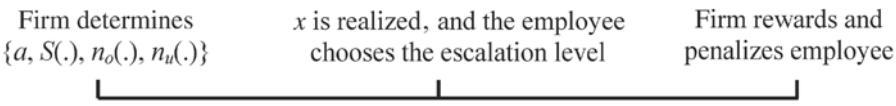


Figure 3. The Sequence of Events

Considering the employee's response, the firm chooses $\{a, S(.), n_o(.), n_u(.)\}$ to maximize its profit, denoted by V.

$$V = \max_{a,S(.),n_o(.),n_u(.)} U(a) - R(a) + \gamma E\Big[U\big(\min\{a+e,x\}\big) - S\Big(U\big(\min\{a+e,x\}\big) - R_o\big(\max\{a+e-x,0\}\big)\Big)\Big].$$

It is worth noting that both the employee and the firm are risk averse.

Analysis and Results

Employee

To gain managerial insight, the following (tractable) functional forms were analyzed. It was assumed that the firm's value function is linear, $U(\min\{a+e,x\}) = B \cdot (\min\{a+e,x\})$ where B is the firm's net benefit per unit of access level (B is hereinafter referred to as the *unit value*) and $\min\{a+e,x\}$ implies that underentitlement degrades business performance. The employee's private benefit function is linear, $u(a+e) = b \cdot (a+e)$, where b is the private benefit per unit access level (b is hereinafter referred to as the *unit private benefit*). The assumption of linear value and private benefit functions do not result in any loss of generality because the firm can always redefine the map between the continuous scale of information for business opportunities and the collection of data for applications, transforming the relationship between the benefit and the access to a linear one. The cost functions are quadratic, $r(e) = (1/2)\beta e^2$, $R(a) = (1/2)sa^2$, and $R_o(\max\{a+e-x,0\}) = (1/2)t(\max(a+e-x,0\})^2$. Since individual users generally bear less cost per unit of information access than the firm, it is assumed that $s,t > \beta > 1$.[3] Besides the frequent use of convex cost functions in the literature (e.g., [20, 23, 27]), quadratic cost functions nicely capture higher security risks associated with higher access as well as the cost of additional IT resources for maintaining and auditing access.

We define w as the bonus rate, where employees are paid w/B of the firm's value created, $S(U(\min\{a+e,x\})) = (w/B)U(\min\{a+e,x\})$. Additionally, for ease of communication and implementation, it is assumed that the firm adopts a linear penalty scheme. In particular, $n_o(a,e,x,e) = p[a+e-x-\varepsilon]^+$ and $n_u(a,e,x,\varepsilon) = q[x-(a+e)-\varepsilon]^+$ where p and q are the penalty rates for over- and underentitlement, respectively.[4] This paper considers a linear reward and penalty scheme because linear incentives are very common in practice. There

are many reasons such linear schemes are popular, including the relatively low cost of writing compared with an intricate contract, the ease of eliciting the hidden information from the agents, and their propensity for discouraging agents from manipulating the outcomes over time or across agents [17, 24, 26]. The information requirements of business opportunities are assumed to be uniformly distributed on $[0, A]$ (i.e., $f(x) = 1/A$).

The analysis begins with the employee's problem, which is formally stated:

$$v = \max_{e} w\left(x - \left[x - (a+e)\right]^{-}\right) + b(a+e) - \frac{1}{2}\beta e^2 - p\left[a+e-x-\varepsilon\right]^{+} - q\left[x-(a+e)-\varepsilon\right]^{+}. \tag{1}$$

With the model fully specified, it is possible to solve for the employees' optimal behavior, arriving at the following escalation strategy:

$$\text{If } x \le a + \frac{b-p}{\beta} - \varepsilon,\ e = \frac{b-p}{\beta};$$

$$\text{If } a + \frac{b-p}{\beta} - \varepsilon < x \le a + \frac{b}{\beta} - \varepsilon,\ e = x + \varepsilon - a;$$

$$\text{If } a + \frac{b}{\beta} - \varepsilon < x \le a + \frac{b}{\beta},\ e = \frac{b}{\beta};$$

$$\text{If } a + \frac{b}{\beta} < x \le a + \frac{w+b}{\beta},\ e = x - a;$$

$$\text{If } a + \frac{w+b}{\beta} < x \le a + \frac{w+b}{\beta} + \varepsilon,\ e = \frac{w+b}{\beta};$$

$$\text{If } a + \frac{w+b}{\beta} + \varepsilon < x \le a + \frac{w+b+q}{\beta} + \varepsilon,\ e = x - \varepsilon - a;$$

$$\text{If } a + \frac{w+b+q}{\beta} + \varepsilon < x \le A,\ e = \frac{w+b+q}{\beta}.$$

(All proofs are included in the Appendix.)

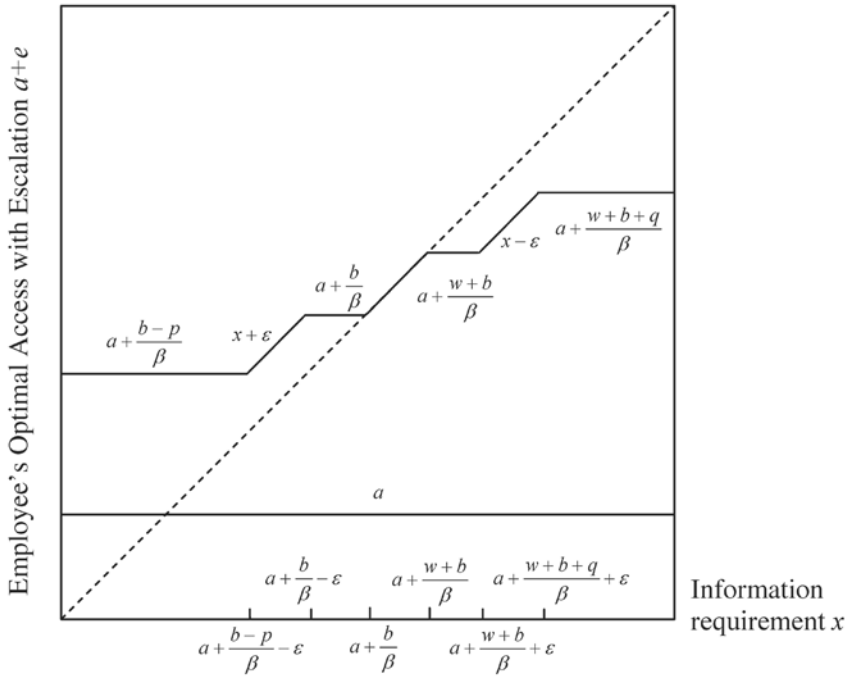
Using this escalation strategy, Proposition 1 is obtained.

> ***Proposition 1 (Entitlement and Information Requirement Proposition)****: The employee will be overentitled (or underentitled) if the information requirement is low (or high). That is, if* $x < a + b/\beta$, $a + e > x$, *and if* $x > a + (w + b)/\beta$, $a + e < x$.

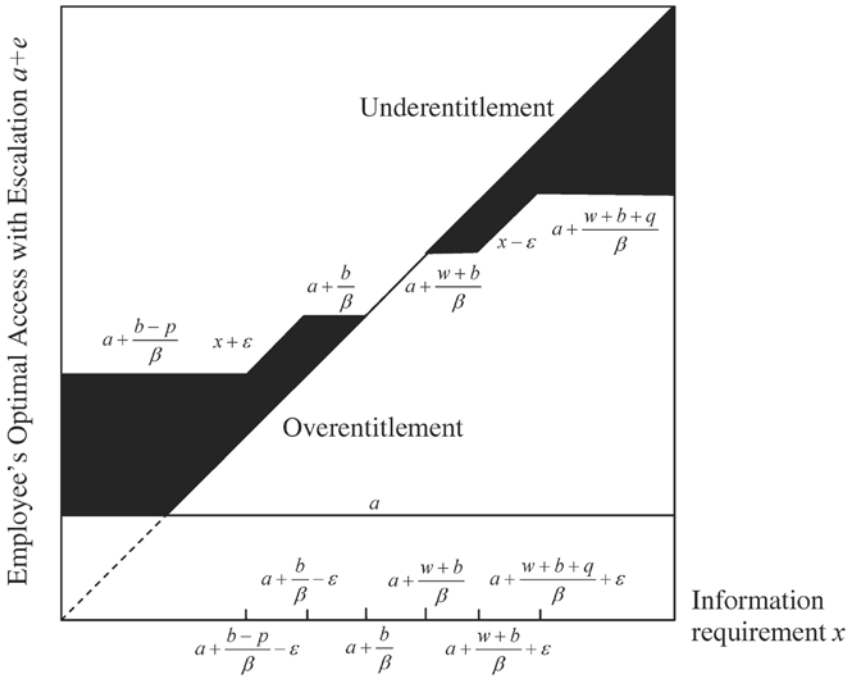
Figure 4 depicts the employee escalation strategy. The horizontal axis represents the level of information requirement and the vertical axis represents the employee's total access level. The graph in Figure 4(a) represents the employee's total access level after escalation, given the different information requirements of emergent tasks.

When the information requirement of the emergent task is lower than $a + b/\beta$, employees will always seek access beyond the information requirement. This "snooping" behavior is driven by the employee's private benefit. The marginal benefit of the escalated access is b and the marginal cost is βe, which is proportional to the magnitude of the escalated access. Employees will escalate as much as possible until the cost of the incremental access exceeds the benefit. The firm can mitigate the overentitlement by auditing the escalation activities and penalizing employees who are overentitled. This penalty reduces the benefit of the incremental access from b to $b - p$, and the escalated access drops from b/β to $(b-p)/\beta$. Consequently, when the information requirement is lower than $a + (b-p)/\beta - \varepsilon$, employees will escalate to $a + (b-p)/\beta$. When the information requirement falls in the range $(a + (b-p)/\beta - \varepsilon, a + b/\beta]$, it is not worthwhile for employees to escalate to a level that precipitates a penalty. Instead, the employees will take advantage of the audit imperfection and escalate to a level that is either ε higher than the information requirement or $a + b/\beta$, which is the optimal total access an employee would achieve without the incentive scheme. The lower shaded area in Figure 4(b) represents all cases where employees are overentitled.

When the information requirement of the emergent task is larger than $a + b/\beta$, the cost of escalating to the information requirement dominates the marginal private benefit from the escalated access. In this case, employees tend toward underentitled if no bonus incentive w is offered. Using bonuses and underentitled penalties, the firm can motivate the desired behavior. When the access is less than the information requirement, the bonus increases the marginal benefit of the escalated access from b to $w + b$. Thus, in cases where the information requirement falls in the range of $(a + b/\beta, a + (w+b)/\beta]$, where $(c_1, c_2]$ is used to indicate an interval from c_1 to c_2 that is inclusive of c_2 but exclusive of c_1, employees will escalate to the correct information requirement (i.e., no overentitlement or underentitled). When the information requirement increases beyond $a + (w+b)/\beta$, the bonus, by itself, is incapable of providing enough escalation incentive. Employees will escalate to a level that is lower than the information requirement. The penalty for underentitlement increases the marginal benefit of the escalated access to $w + b + q$ and further motivates employees to escalate to a higher level. When the information requirement falls into the range $(a + (w+b)/\beta, a + (w+b+q)/\beta + e]$, employees will again take advantage of the audit imperfection and escalate as close to $(w+b)/\beta$ as possible. When the information requirement is greater than $a + (w+b+q)/\beta + \varepsilon$, the escalated access becomes $(w+b+q)/\beta$. The upper shaded area in Figure 4(b) represents all cases where employees are underentitled. Overall, the shaded areas represent the cases where employee' access is inconsistent with the information requirement of the emergent task, which imposes cost to the firm. The firm can adjust its access governance policy $\{a, w, p, q\}$ to influence employee escalation. In the next section, the firm's optimal strategies are analyzed.



(a) Optimal Access with Escalation



(b) Overentitlement and Underentitlement

Figure 4. Employee's Escalation Strategy

Firm

The firm chooses a, w, p, and q to maximize its profit. Its optimization problem is

$$V = \max_{a,w,p,q} Ba - \frac{1}{2}sa^2 + \gamma E\left[(B-w)\left(x-\left[x-(a+e)\right]^-\right) - \frac{1}{2}t\left(\left[(a+e)-x\right]^+\right)^2\right]. \quad (2)$$

Considering the employee escalation strategy, (2) is represented by

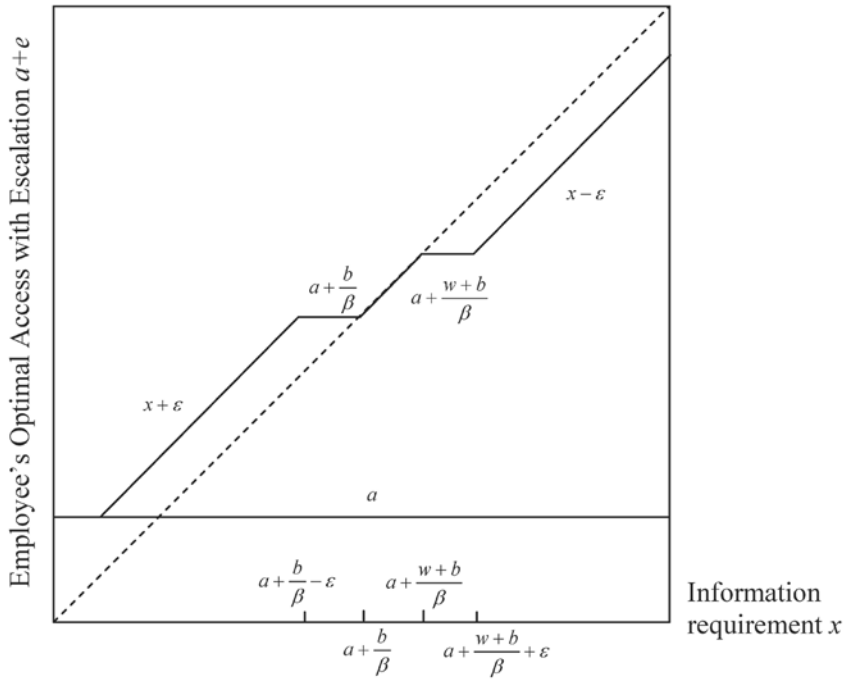
$$\begin{aligned} V = \max_{a,w,p,q} Ba - \frac{1}{2}sa^2 &+ \gamma\int_0^{a+\frac{b-p}{\beta}-\varepsilon}\left((B-w)x - R_o\left(a+\frac{b-p}{\beta}-x\right)\right)f(x)dx \\ &+ \gamma\int_{a+\frac{b-p}{\beta}-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon}\left((B-w)x - R_o(\varepsilon)\right)f(x)dx \\ &+ \gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}}\left((B-w)x - R_o\left(a+\frac{b}{\beta}-x\right)\right)f(x)dx \\ &+ \gamma\int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}}(B-w)xf(x)dx + \gamma\int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon}(B-w)\left(a+\frac{w+b}{\beta}\right)f(x)dx \\ &+ \gamma\int_{a+\frac{w+b}{\beta}+\varepsilon}^{a+\frac{w+b+q}{\beta}+\varepsilon}(B-w)(x-\varepsilon)f(x)dx \\ &+ \gamma\int_{a+\frac{w+b+q}{\beta}+\varepsilon}^{A}(B-w)\left(a+\frac{w+b+q}{\beta}\right)f(x)dx. \end{aligned} \quad (3)$$

Lemma 1 gives the firm's penalty strategies.

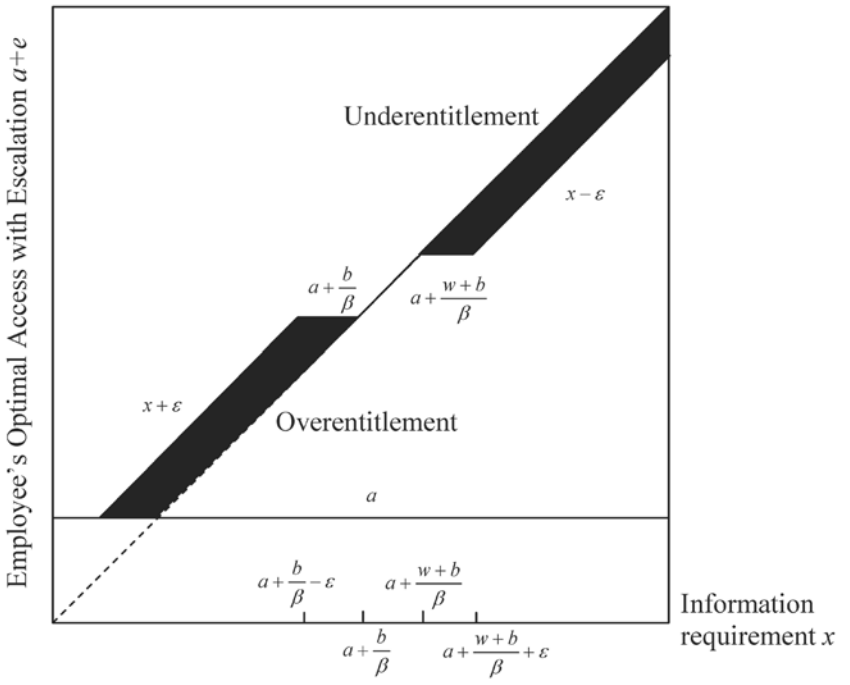
> ***Lemma 1 (Over- and Underentitlement Penalty Proposition)****: The penalty for overentitlement eliminates an employee's private benefit (i.e.,* $p = b$*), and the penalty for the underentitlement is large enough to minimize underentitlement (i.e.,* $q \geq [(A - a - \varepsilon)\beta - w - b]^+$*).*

Employee escalation beyond the information requirement is driven by their private benefit. Lemma 1 shows that the optimal penalty for overentitlement should completely eliminate the employee's private benefit from additional access. The penalty for underentitlement should be large enough to motivate employees to escalate as closely to the information requirement as possible. Figure 5(a) shows the employee escalation strategy with the optimal penalty rates.

In Figure 5(b), overentitlement and underentitlement (the shaded areas) still exist. With an imperfect audit instrument, the penalty scheme by itself cannot completely eliminate over- and underentitlement. Since a bonus increases the



(a) Optimal Access with Escalation



(b) Overentitlement and Underentitlement

Figure 5. Employee's Escalation Strategy with Optimal Penalty Rates

employee's benefit from the incremental access and this effect is valid only when the total access level is less than the information requirement, firms can use bonuses to reduce occurrences of underentitlement. Figure 5(b) shows that a larger bonus rate, w, moves the light-shaded area upward and decreases the size of the underentitlement area.

Next explored is how the firm uses bonuses to motivate employees. With the optimal penalty rates, the firm's optimization problem can be represented by

$$\begin{aligned} V = \max_{a,w} Ba - \frac{1}{2}sa^2 &+ \gamma\int_0^{a-\varepsilon}\left((B-w)x - R_o(a-x)\right)f(x)dx \\ &+ \gamma\int_{a-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon}\left((B-w)x - R_o(\varepsilon)\right)f(x)dx \\ &+ \gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}}\left((B-w)x - R_o\left(a+\frac{b}{\beta}-x\right)\right)f(x)dx \\ + \gamma\int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}}(B-w)xf(x)dx &+ \gamma\int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon}(B-w)\left(a+\frac{w+b}{\beta}\right)f(x)dx \\ &+ \gamma\int_{a+\frac{w+b}{\beta}+\varepsilon}^{A}(B-w)(x-\varepsilon)f(x)dx. \end{aligned} \tag{4}$$

Proposition 2 (Audit and Penalty Scheme Proposition): *If the audit is perfect, the firm only adopts the penalty scheme (i.e.,* w = *0).*

The implementation of a penalty scheme is based on the assumption that the firm can detect misuse through auditing. If there is no audit error, a penalty scheme can completely eliminate overentitlement and underentitlement. If the audit process is imperfect, escalation misuse will exist.

The bonus and penalty rates are different incentive instruments. Bonus schemes require the firm to share its gains with employees and motivate the employees to consider the firm's loss of business. Therefore, they can be used to address underentitlement. Although this incentive is costly to the firm, the firm still has an incentive to implement a bonus scheme in the presence of the audit imperfection.

When there is audit error, the optimal bonus rate w can be represented by

$$w_1 = \left[\frac{(B-b)\varepsilon - \beta\varepsilon a - \frac{1}{2}\beta(A-\varepsilon)^2}{2\varepsilon}\right]^+ \quad \text{if } a+\frac{w+b}{\beta}+\varepsilon \le A$$

$$w_2 = \frac{-2\beta\left(a+\frac{b}{\beta}-A-\frac{B}{2\beta}\right)+\beta\sqrt{\left(a+\frac{b}{\beta}+\frac{B}{\beta}-A\right)^2+3A^2}}{3} \quad \text{otherwise.}$$

When the bonus rate is small ($a + (w + b)/\beta + \varepsilon \le A$), the firm's total benefit from a specific bonus rate w is $(B - w)\varepsilon(w/b)$, where $\varepsilon(w/b)$ is proportional to the expected level of the escalated access motivated by the bonus and $(B - w)$ is the net unit benefit from the escalated access. The total benefit is first increasing and then decreasing as the bonus rate increases. The bonus scheme with rate w costs the firm $w((A - \varepsilon)^2/2 + \varepsilon(a + (w + b)/\beta))$, where $(A - \varepsilon)^2/2 + \varepsilon(a + (w + b)/\beta)$ is proportional to the value that the firm gains from the expected escalated access. Thus, the total bonus (or the cost of the bonus to the firm) is increasing in w, and the firm will choose a bonus rate w to maximize the difference between $(B - w)\varepsilon(w/b)$ and $w((A - \varepsilon)^2/2 + \varepsilon(a + (w + b)/\beta))$, resulting in the optimal bonus rate w_1.

However, if $a + (w + b)/\beta + \varepsilon > A$, the expected benefit of the bonus is constrained by the maximal information access A, and the optimal w is given by w_2.

The optimal regular access assigned by the firm will now be examined. The optimal regular access level is

$$a^* = \frac{A}{\gamma t}\left(-s + \sqrt{s^2 + \frac{2}{A}\gamma t\left(B + \left(B - w^*\right)\gamma\frac{\varepsilon}{A}\right)}\right), \text{ if } a^* + \frac{w^* + b}{\beta} + \varepsilon \le A$$

$$\left(\text{where } w^* = w_1\right);$$

$$a^* = \frac{1}{\gamma t}\left(-\left(As + \gamma\left(B - w^*\right)\right) + \sqrt{\left(As + \gamma\left(B - w^*\right)\right)^2 + 2\gamma t\left(\gamma\left(B - w^*\right)\left(A - \frac{w^* + b}{\beta}\right) + AB\right)}\right)$$

otherwise $\left(\text{where } w^* = w_2\right)$.

Proposition 3 (Bonus and Regular Access Substitution Proposition): *Bonus and regular access are substitutes.*

Proposition 3 is evident from the fact that $V''_{wa} = \partial V_{firm}/\partial w \partial a < 0$. The benefit of the bonus rate is decreasing when the regular access increases, and vice versa. The regular access and the bonus potentially substitute for each other. In particular, if the regular access increases, the bonus rate decreases. When the regular access increases, the cost of the bonus increases and hence the firm will choose a lower bonus rate.

Corollary 1 (Decreasing Bonus Rate in Regular Access Corollary): *The bonus rate is decreasing in the regular access.*

The discussion now proceeds to the question of how regular access and bonus rate are influenced by parameters of the model. Figure 6 illustrates how the firm assigns regular access levels a and bonus rates w for different unit value B. The graph in Figure 6(a) shows that the optimal regular access level increases in the unit value. The trend is driven by the increased marginal benefit from routine business tasks. The curve in Figure 6(b) shows that the bonus rate first increases then drops back to zero as the unit value increases.

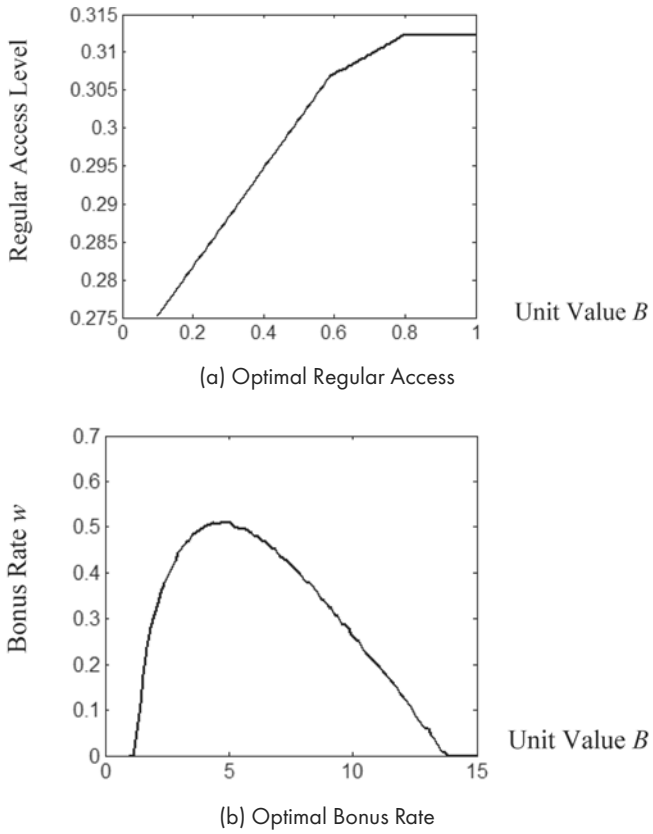


Figure 6. Optimal Regular Access and Bonus Rate Given Different Unit Value

$A = 2$, $\gamma = 0.5$, $t = s = 9$, $\beta = 1$, $\varepsilon = 1$, $b = 0.5$

The unit value influences the firm's incentives to use the bonus in two ways. On one hand, the higher unit value implies that the firm benefits more from the increased access and hence has more incentives to use bonuses to motivate its employees. On the other hand, the higher unit value results in higher regular access, which mitigates the need for additional access to accomplish emergent tasks. In this regard, the firm has less incentive to use bonuses.

Figure 7 shows the optimal regular access and bonus rate given different audit errors. Note that penalty schemes are ineffective in addressing the over- and underentitlement caused by the audit imperfection, but the bonuses can reduce underentitlement. When the audit error increases, the firm loses more from underentitlement and hence has more incentive to increase the bonus rate. Likewise, the regular access can reduce underentitlement (the upper shaded area in Figure 5(b) shrinks). Therefore, the firm has an incentive to assign higher regular access to the employee when the audit error increases.

In contrast to the audit error, the private benefit negatively affects the optimal regular access and the bonus rate as Figure 8 illustrates. When the private

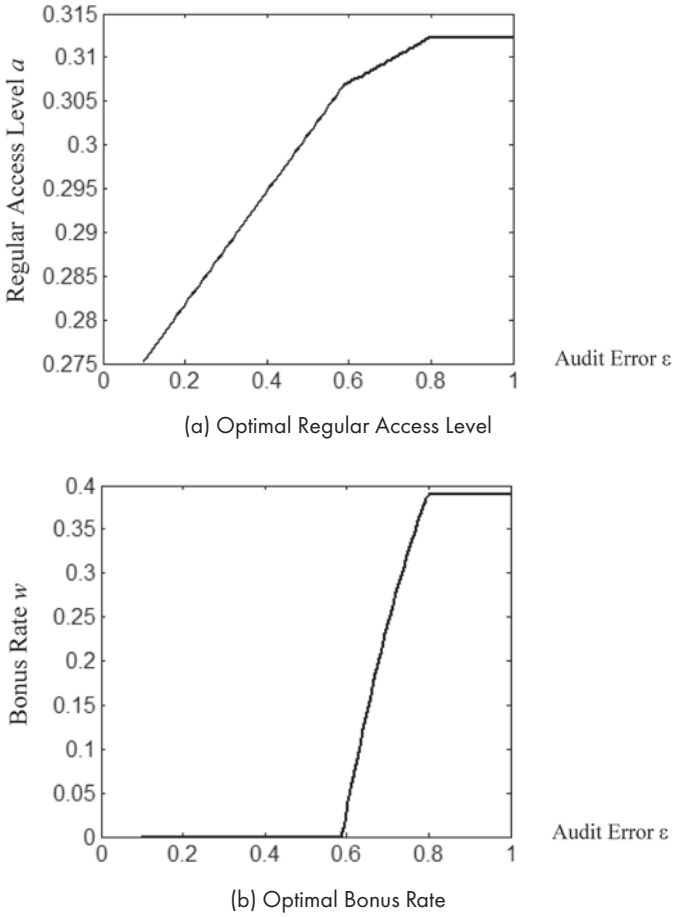


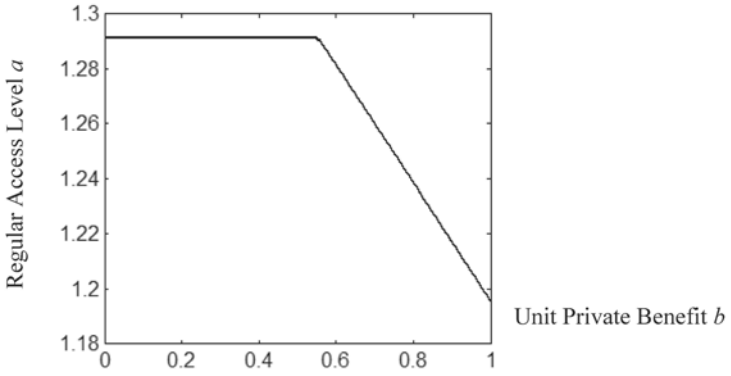
Figure 7. Optimal Regular Access and Bonus Rate Given Different Audit Error

$A = 2$, $\gamma = 0.5$, $t = s = 9$, $\beta = 1$, $b = 0.5$, $B = 2.5$

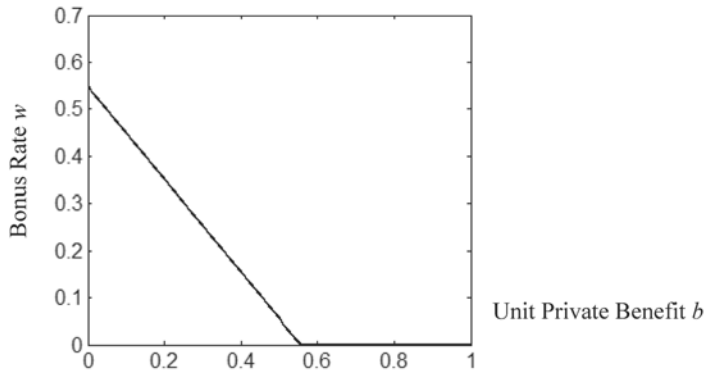
benefit increases, the underentitlement situations are less likely to occur. The benefit of the bonus scheme decreases. Thus, the firm will set a lower bonus rate and a lower regular access.

Conclusion

Firms in data-intense industries compete through e-business initiatives that leverage technology to make information more accessible throughout the extended enterprise. In such industries, firms that can best utilize data to create customer value find new sources of revenue and competitive advantage. However, the ubiquity of information poses significant security risks. As systems and data pools become more integrated, managing information



(a) Optimal Regular Access Level



(b) Optimal Bonus Rate

Figure 8. Optimal Regular Access and Bonus Rate Given Different Unit Benefit *b* Rate

$A = 2$, $\gamma = 0.5$, $t = s = 9$, $\beta = 1$, $\varepsilon = 1$, $B = 13$

access presents new challenges. Successful access management must ensure that information is available to employees for value creation while protecting it from misuse. This paper proposes an incentive-based information access policy that controls employee self-interested behavior and balances the availability and security of firm information.

Contribution

Using a game-theoretic analysis, this paper showed that incentives can be used to encourage value creation through flexible information access schemes and to control information misuse. Set properly, penalties can nearly eliminate employee propensities to access unnecessary information, reducing risk. However, simple penalties alone are not always sufficient to encourage employees to access the information required to create value. Rather, the analysis showed that

positive rewards tied to firm performance are needed to improve outcomes for both firms and employees. This paper examined how these results are linked to the firm's audit capability and showed that audit quality can reduce the need for incentives. The trade-off between investments required to improve audit capability and the corresponding reduction in incentive payouts is an area of ongoing research.

Insights, Limitations, and Implementation

The foregoing analysis provides many interesting insights into the implementation challenges of access with user-driven escalation. It showed that audit quality is an important element of flexible information-access schemes. Without the ability to catch cheaters, firms are better off moving toward a more traditional role-based access approach. Escalation must be implemented in a way that provides an audit trail, including records of who requests information, when it is requested, what information is accessed, and what value is created (e.g., the type of transaction performed) [34]. Nevertheless, perfect monitoring is not technologically or financially feasible in most cases. As was shown above, bonus schemes can counteract audit imperfection, making an escalation strategy desirable even in cases with significant audit error. The combination of audit with penalties can motivate employees to align their actions to benefit themselves and the organization. Note that audit precision was presumed to be exogenous to the model. An interesting area for future research would be to extend this analysis to consider the case where firms can invest to reduce audit error and thus face a trade-off between audit imperfection and bonus.

The model addresses the use of incentives when escalation is employed. It did not consider possible penalties for abuse of routine access. However, while the focus was on an economic model, it is worth noting that penalty instruments need not be monetary. In fact, in most practical cases, it is not in the firm's interest to gain from employees' misuse, and thus penalties were not included as positive contributions to the firm's objective function. In most instances, the penalties implemented involve a range of nonmonetary actions, such as requiring the employee to attend mandatory compliance training, file a report explaining the violation, or make a public apology for illegitimate escalation. In addition, penalties need not be directly levied against employees. Cases have also been observed where security fines were levied against the employee's manager, highlighting the manager's responsibility for training [18].

The flexible access policy described in this paper is most applicable in situations where information availability is critical to organizational success and thus creates great benefit for the firm. The discussion considered instances where a firm's benefit from a business opportunity is determined by its employees' use-escalated access level. Of course, the firm's payoff is influenced by a number of factors, such as the complexity of its business processes, the organizational knowledge base, and the experience of its employees. The ability to access the requisite information is necessary, but not sufficient, for knowledge workers to monetize business opportunities.

Certainly, escalation policies must be confined within the allowable zone dictated by regulatory requirements. Some data or applications cannot be made available through an escalation scheme. For example, PCI/DSS requires businesses to ensure that critical data can only be accessed by authorized personnel and systems, and processes must be in place to limit access based on "need to know" and "according to job responsibilities." Thus, in e-commerce environments, escalation must be limited by the firm's PCI-compliant security policy. In addition, escalation schemes must be implemented to ensure that the risk of security failures and the cost of recovery are relatively low compared with the loss of not granting access. For example, IBM's fuzzy MLS model complements the approach proposed in this paper by using risk analysis to determine the escalation boundary [8].

One interesting benefit of escalation schemes is the information gathered from employees by monitoring their escalation usage. This information allows the firm to learn the dynamics of the business environment from employees. Employees often have knowledge of potential business opportunities, and without escalation, that information can be lost. Escalation schemes create an implicit communication channel between the firm and its employees. Likewise, they make it possible for the firm to spot trends in escalation activity that could identify a malicious insider before a major loss occurs. Employees may be presumed to obtain some private benefit from information, such as a feeling of trust or the entertainment value of snooping. Escalation schemes require some knowledge of employees' private benefit from information (in order to properly specify incentives). Observing employees over time can allow firms to learn their characteristics and adjust incentives appropriately.

Finally, escalation can be very helpful in establishing regular access levels and understanding how employees' roles change over time (sometimes referred to as role drift). By observing employees' needs over time, the firm can adjust their regular access accordingly.

NOTES

1. An entitlement is a resource that a person is authorized to access in a certain way, for example, opening case files might be an entitlement for an application. The terms "entitlement," "privilege," and "permission" are used interchangeably.
2. Examples of organizational structural changes include establishing a new team, changing the leader of a team, removing a business unit, and transferring a team from one group to another.
3. This assumption also ensures that the firm's optimization problem is concave.
4. $[y]^+ = \max\{y, 0\}$ and $[y]^- = \min\{y, 0\}$.

REFERENCES

1. Antle, R., and Eppen, G.D. Capital rationing and organizational slack in capital budgeting. *Management Science, 31,* 2 (February 1985), 163–174.
2. Arrow, K.J. The economics of agency. In J.E. Pratt, R.J. Zeckhauser, and K.J. Arrow (eds.), *Principals and Agents: The Structure of Business*. Boston: Harvard Business School Press, 1985, pp. 37–53.

3. Aveksa. Enterprise roles-based access governance. White Paper, 2007, Aveksa, Waltham, MA (available at www.aveksa.com/company/resource-center/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=1324/).
4. Baiman, S. Agency research in managerial accounting: A second look. *Accounting Organizations and Society*, *15,* 4 (1990), 341–371.
5. Baker, N.R., and Freeland, J.R. Structuring information flow to enhance innovation. *Management Science*, *19,* 1 (Theory Series) (September 1972), 105–116.
6. Baron, D.P., and Besanko, D. Regulation, asymmetric information, and auditing. *RAND Journal of Economics, 15,* 4 (winter 1984), 447–470.
7. Brynjolfsson, E., and Hitt, L. Paradox lost? Firm-level evidence on the returns to information systems spending. *Management Science, 42,* 4 (April 1996), 541–558.
8. Cheng, P.C.; Pankaj, R.; and Keser, C. Fuzzy MLS: An experiment on quantified risk-adaptive access control. Yorktown Heights, NY: IBM, January 3, 2007 (available at http://domino.research.ibm.com/comm/research_projects.nsf/pages/system_s_security.index.html/$FILE/ATTH4YZ5.pdf).
9. Dye, R.A. Optimal monitoring policies in agencies. *RAND Journal of Economics, 17,* 3, (autumn 1986), 339–350.
10. Ferreira, A.; Cruz-Correia, R.; Antunes, L.; Farinha, P.; Oliveira-Palhares, E.; Chadwick, D.; and Costa-Pereira, A. How to break access control in a controlled manner. In D.J. Lee, B. Nutter, S. Antani, S. Mitra, and J. Archibale (eds.), *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems.* Los Alamitos, CA: IEEE Computer Society Press**,** 2006, pp. 847–854.
11. Grad, S. Guilty plea in UCLA medical records snooping case. *Los Angeles Times* (December 1, 2008) (available at http://latimesblogs.latimes.com/lanow/2008/12/guilty-plea-in.html).
12. Han, K.; Kauffman R.J.; and Nault B.R. Relative importance, specific investment and ownership in interorganizational systems. *Information Technology Management, 9,* 3 (September 2008), 181–200.
13. Harris, M., and Raviv, A. Optimal incentive contracts with imperfect information. *Journal of Economic Theory, 20,* 2 (April 1979), 231–259.
14. Harris, M., and Raviv, A. The capital budgeting process: Incentives and information. *Journal of Finance, 51,* 4 (September 1996), 1139–1174.
15. Harris, M.; Kriebel, C.; and Raviv, A. Asymmetric information, incentives and intrafirm resource allocation. *Management Science, 28,* 6 (June 1982), 604–620.
16. Holmstrom, B. Moral hazard and observability. *Bell Journal of Economics, 10,* 1 (spring 1979), 74–91.
17. Holmstrom, B., and Milgrom, P. Aggregation and linearity in the provision of intertemporal incentive. *Econometrica, 55,* 2 (March 1987), 303–328.
18. Johnson, M.E., and Goetz, E. Embedding information security into organizations. *IEEE Security and Privacy, 5,* 3 (May/June 2007), 16–24.
19. Jolly, D. Fraud costs French bank $7.1 billion. *New York Times* (January 25, 2008) (available at www.nytimes.com/2008/01/25/business/worldbusiness/25bank-web.html?_r=1/).
20. Kannan, K., and Telang, R. Market for software vulnerabilities? Think again. *Management Science, 51,* 5 (May 2005), 726–740.

21. Kim, S.K., and Suh, Y.S. Conditional monitoring policy under moral hazard. *Management Science, 38,* 8 (August 1992), 1106–1120.
22. Kohli, R., and Devaraj, S. Measuring information technology payoff: A meta-analysis of structural variables in firm-level empirical research. *Information Systems Research, 14,* 2 (June 2003), 127–145.
23. Krishnan, V., and Zhu, W. Designing a family of development intensive products. *Management Science, 52,* 6 (June 2006), 813–825.
24. Laffont, J., and Tirole, J. Auctioning incentive contracts. *Journal of Political Economy, 95,* 5 (October 1987), 921–937.
25. Lee, H.L.; So, K.C.; and Tang, C.S. The value of information sharing in a two-level supply chain. *Management Science, 46,* 5 (May 2000), 626–643.
26. McAfee, R.P., and McMillan, J. Competition for agency contracts. *RAND Journal of Economics, 18,* 2 (summer 1987), 296–307.
27. Motta, M. Endogenous quality choice: Price vs. quantity competition. *Journal of Industry Economics, 41,* 2 (June 1993), 113–131.
28. Mouzakitis, S.; Sourouni, A.M.; and Askounis, D. Effects of enterprise interoperability on integration efforts in supply chains. *International Journal of Electronic Commerce, 12,* 2 (winter 2009–10), 127–155.
29. Mukhopadhyay, T.; Kekre, S.; and Kalathur, S. Business value of information technology: A study of electronic data interchange. *MIS Quarterly, 19,* 2 (June 1995), 137–156.
30. Povey, D. Optimistic security: A new access control paradigm. In D. Kienzle, M.E. Zurko, S.J. Greenwald, and C. Serbau (eds.), *Proceedings of the 1999 Workshop on New Security Paradigms*. New York: ACM Press, 2000, pp. 40–45.
31. Ranganathan, C.; Dhaliwal, J.S.; and Teo T.S.H. Assimilation and diffusion of Web technologies in supply-chain management: An examination of key drivers and performance impacts. *International Journal of Electronic Commerce, 9,* 1 (fall 2004), 127–161.
32. Rathnam, S.; Mahajan, V.; and Whinston, A.B. Facilitating coordination in customer support teams: A framework and its implications for the design of information technology. *Management Science, 41,* 12 (December 1995), 1900–1922.
33. Richardson, R. *CSI Computer Crime and Security Survey.* New York: Computer Security Institute, 2008.
34. Rissanen, E.; Firozabadi, S.B.; and Sergot, M. Towards a mechanism for discretionary overriding of access control. In B. Christianson, B. Crispo, J.A. Malcolm, and M. Roe (eds.), *Revised Selected Papers: Lecture Notes in Computer Science,* vol. 3957. Berlin: Springer, 2006, pp. 320–323.
35. Shavell, S. Risk sharing and incentives in the principal and agent relationship. *Bell Journal of Economics, 10,* 1 (spring 1979), 55–73.
36. Sinclair, S.; Smith, S.W.; Trudeau, S.; Johnson, M.E.; and Portera, A. Information risk in financial institutions: Field study and research roadmap. In D.J. Veit, D. Kundisch, T. Weitzel, C. Weinhardt, F.A. Rabhi, and F. Rajola (eds.), *Enterprise Applications and Services in the Finance Industry.* Springer Lecture Notes in Business Information Processing Series, vol. 4. Berlin: Springer, 2008, pp. 165–180.

37. Townsend, R.M. Optimal contracts and competitive markets with costly state verification. *Journal of Economy Theory, 21,* 2 (1979), 265–293.
38. Tsai, W. Knowledge transfer in intraorganizational networks: Effects of network position and absorptive capacity on business unit innovation and performance. *Academy of Management Journal, 44,* 5 (2001), 996–1004.
39. Von Hippel, E. Sticky information and the locus of problem solving: Implications for innovation. *Management Science, 40,* 4 (April 1994), 429–439.

Appendix

Proof of Employee's Escalation Strategy

If $x \le a + e - \varepsilon$, the first-order condition (FOC) of (1) w.r.t. e is $b - \beta e - p = 0$ and the second-order condition (SOC) satisfies $-\beta < 0$. The escalated access level is given by $e = (b - p)/\beta$. The condition can be rewritten as $x \le a + (b - p)/\beta - \varepsilon$.

If $a + e - \varepsilon < x \le a + e$, the FOC of (1) w.r.t. e is $b - \beta e = 0$ and the SOC satisfies $-\beta < 0$. The escalated access level is given by $e = b/\beta$. The condition can be rewritten as $a + b/\beta - \varepsilon < x \le a + b/\beta$.

If $a + e < x \le a + e + \varepsilon$, the FOC of (1) w.r.t. e is $w + b - \beta e = 0$ and the SOC satisfies $-\beta < 0$. The escalated access level is given by $e = (w + b)/\beta$. The condition can be rewritten as $(w + b)/\beta < x \le a + (w + b)/\beta + e$.

If $A \ge x > a + e + \varepsilon$, the FOC of (1) w.r.t. e is $w + b - \beta e + q = 0$ and the SOC satisfies $-\beta < 0$. The escalated access level is given by $e = (w + b + q)/\beta$. The condition can be rewritten as $x > a + (w + b + q)/\beta + \varepsilon$.

Next, three ranges missing from the previous analysis are considered: $a + (b - p)/\beta - \varepsilon < x \le a + b/\beta - \varepsilon$, $a + (w + b)/\beta + \varepsilon < x \le a + (w + b + q)/\beta + \varepsilon$, and $a + b/\beta < x \le a + (w + b)/\beta$.

The first range checked is $a + (b - p)/\beta - \varepsilon < x \le a + b/\beta - \varepsilon$. Suppose an employee claims the escalated access level as $x + \varepsilon + e_1 - a$ instead of $x + \varepsilon - a$. The employee will choose $x + \varepsilon - a + e_1$ if $w(x) + b(x + \varepsilon - a) - R(x + \varepsilon - a) < w(x) + b(x + \varepsilon - a + e_1) - R(x + \varepsilon - a + e_1) - p(e_1)$. We then obtain $x < a + (b - p)/\beta - \varepsilon - e_1/2$, which is lower than the lower bound of the range. Thus, $e \le x + \varepsilon - a$. Suppose an employee claims the escalated access level as $x + \varepsilon - a - e_2$ instead of $x + \varepsilon - a$. The employee will choose $x + \varepsilon - a - e_2$ if $w(x) + b(x + \varepsilon - a) - R(x + \varepsilon - a) < w(x) + b(x + \varepsilon - e_2 - a) - R(x + \varepsilon - e_2 - a)$. We then obtain $x > a + b/\beta - \varepsilon + e_2/2$, which is higher than the upper bound of the range. Thus, $e \ge x + \varepsilon - a$. Overall, we conclude $e = x + \varepsilon - a$.

Second, the range $a + (w + b)/\beta + \varepsilon < x \le a + (w + b + q)/\beta + e$ is checked. Suppose an employee claims the escalated access level as $x - \varepsilon - a - e_3$ instead of $x - a - \varepsilon$. The employee will choose $x - \varepsilon - a - e_3$ if $w(x - \varepsilon) + b(x - a - \varepsilon) - R(x - a - \varepsilon) < w(x - \varepsilon - e_3) + b(x - \varepsilon - a - e_3) - R(x - \varepsilon - a - e_3) - q(e_3)$. We obtain $x > a + (w + b + q)/\beta + \varepsilon + e_3/2$, which is higher than the upper bound of the range. Thus, $e \ge x - a - \varepsilon$. Suppose an employee claims the escalated access level as $x - \varepsilon - a + e_4$ instead of $x - \varepsilon - a$. The employee will choose $x - \varepsilon - a + e_4$ if $w(x - \varepsilon) + b(x - \varepsilon - a) - R(x - \varepsilon - a) < w(x - \varepsilon + e_4) + b(x - \varepsilon + e_4 - a) - R(x - \varepsilon + e_4 - a)$. We then obtain $x < a + (w + b)/\beta + \varepsilon - e_4/2$, which is lower than the lower bound of the range. Thus, $e \le x - \varepsilon - a$. Overall, we conclude $e = x - \varepsilon - a$.

Finally, consider the range $a + b/\beta < x \le a + (w + b)/\beta$. Suppose an employee claims the escalated access level as $x + e_5 - a$ instead of $x - a$. The employee will choose $x + e_5 - a$ if $w(x) + b(x - a) - R(x - a) < w(x) + b(x + e_5 - a) - R(x + e_5 - a)$. We then obtain $x < a + b/\beta - e_5/2$, which is lower than the lower bound of the range. Thus, $e \le x - a$. Suppose an employee claims the escalated access level as $x - e_6 - a$ instead of $x - a$. The employee will choose $x - e_6 - a$ if $w(x) + b(x - a) - R(x - a) < w(x - e_6) + b(x - e_6 - a) - R(x - e_6 - a)$. We then obtain $x > a + (w + b)/\beta + e_6/2$, which is higher than the upper bound of the range. Thus, $e \ge x - a$. Overall, we conclude $e = x - a$. Q.E.D.

Proof of Proposition 1 (Entitlement and Information Requirement Proposition)

Given the employee escalation strategy, it can be verified that when $x < a + b/\beta$, $a + e > x$; when $a + b/\beta \le x \le a + (w + b)/\beta$, $a + e = x$; and when $a + (w + b)/\beta < x \le A$, $a + e < x$. Q.E.D.

Proof 3 of Lemma 1 (Over- and Underentitlement Penalty Proposition)

The first-order derivative of (3) with respect to p is

$$\begin{aligned} V_p' &= \gamma\left((B-w)\left(a+\frac{b-p}{\beta}-\varepsilon\right)-R_o(\varepsilon)\right)\frac{-1}{\beta}f(x) \\ &\quad+\gamma\int_0^{a+\frac{b-p}{\beta}-\varepsilon}-t\left(a+\frac{b-p}{\beta}-x\right)\frac{-1}{\beta}f(x)dx \\ &\quad-\gamma\left((B-w)\left(a+\frac{b-p}{\beta}-\varepsilon\right)-R_o(\varepsilon)\right)\frac{-1}{\beta}f(x) \\ &= \gamma\int_0^{a+\frac{b-p}{\beta}-\varepsilon}t\left(a+\frac{b-p}{\beta}-x\right)\frac{1}{\beta}f(x)dx. \end{aligned}$$

Since $V_p' > 0$, the optimal p is given by

$$p = b. \tag{5}$$

The first-order derivative of (3) w.r.t. q is

$$\begin{aligned} V_q' &= (B-w)\left(a+\frac{w+b+q}{\beta}+\varepsilon-\varepsilon\right)\frac{1}{\beta}\frac{1}{A}-(B-w)\left(a+\frac{w+b+q}{\beta}\right)\frac{1}{\beta}\frac{1}{A} \\ &\quad+\int_{a+\frac{w+b+q}{\beta}+\varepsilon}^{A}\left((B-w)\frac{1}{\beta}\right)\frac{1}{A}dx \\ &= (B-w)\frac{1}{A\beta}\left(A-a-\frac{w+b+q}{\beta}-\varepsilon\right). \end{aligned}$$

The second-order derivative of (3) w.r.t. q is

$$V_{qq}'' = -(B-w)\frac{q}{A\beta^2} < 0.$$

Therefore, $q = (A - a - \varepsilon)\beta - w - b$ if $a + (w + b)/\beta + \varepsilon \le A$. Otherwise, $q = 0$. Overall,

$$q = \left[(A - a - \varepsilon)\beta - w - b\right]^{+}. \tag{6}$$

Q.E.D.

Proof of Proposition 2 (Audit and Penalty Scheme Proposition)

If ε = 0, the firm's optimization problem can be simplified as

$$V = \max_{a,w} Ba - \frac{1}{2}sa^2 + \gamma\int_0^a \left((B-w)x - R_o(a-x)\right) f(x)dx + \gamma\int_a^A (B-w)xf(x)dx.$$

We have the following first-order derivative,

$$V'_w = \gamma\int_0^A -xf(x)dx < 0.$$

Therefore, $w = 0$. Q.E.D.

Proof of Optimal Bonus Rate w

If $a + (w + b)/\beta + \varepsilon \le A$, the first-order derivative of (4) w.r.t. w is

$$V'_w = \gamma\int_0^{a+\frac{w+b}{\beta}} (-x) f(x)dx + \gamma\int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon} \left(-\left(a + \frac{w+b}{\beta}\right) + (B-w)\frac{1}{\beta}\right) f(x)dx$$
$$+ \gamma\int_{a+\frac{w+b}{\beta}+\varepsilon}^{A} \left(-(x-\varepsilon)\right) f(x)dx.$$

The second-order derivative of (4) w.r.t. w is

$$V''_{ww} = -\frac{2\gamma\varepsilon}{A\beta} < 0.$$

Given a regular access level, the optimal rate is

$$w = \left[\frac{\frac{1}{\beta}(B-b)\varepsilon - \varepsilon a - \frac{1}{2}(A-\varepsilon)^2}{2\varepsilon\frac{1}{\beta}}\right]^{+}. \tag{7}$$

If $a + (w + b)/\beta + \varepsilon > A$, the optimization problem becomes

$$V = \max_{a,w} Ba - R_s(a)$$
$$+ \gamma\int_0^{a-\varepsilon}\left((B-w)x - R_o(a-x)\right)f(x)dx + \gamma\int_{a-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon}(B-w)x - R_o(\varepsilon)f(x)dx$$
$$+ \gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}}\left((B-w)x - R_o\left(a+\frac{b}{\beta}-x\right)\right)f(x)dx + \gamma\int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}}(B-w)xf(x)dx \quad (8)$$
$$+ \gamma\int_{a+\frac{w+b}{\beta}}^{A}\left((B-w)\left(a+\frac{w+b}{\beta}\right)\right)f(x)dx.$$

And the first-order derivative of (8) w.r.t. w is

$$V'_w = \gamma\int_0^{a+\frac{w+b}{\beta}}(-x)f(x)dx + \gamma\int_{a+\frac{w+b}{\beta}}^{A}\left(-\left(a+\frac{w+b}{\beta}\right)+\frac{B-w}{\beta}\right)f(x)dx.$$

The second-order derivative of (8) w.r.t. w is

$$V''_{ww} = \frac{2\gamma}{A\beta}\left(a+\frac{w+b}{\beta}-A\right)-\frac{\gamma(B-w)}{A\beta^2} < 0.$$

Therefore,

$$w = -\frac{2\beta}{3}\left(a+\frac{b}{\beta}-A-\frac{B}{2\beta}\right)+\frac{\beta}{3}\sqrt{\left(a+\frac{b}{\beta}-A+\frac{B}{\beta}\right)^2+3A^2}. \quad (9)$$

Q.E.D.

Proof of Optimal Regular Access

If $a^* + (w^* + b)/\beta + \varepsilon \le A$, the first-order derivative of (4) w.r.t. a is,

$$V'_a = B - sa + \gamma\int_0^{a-\varepsilon} -t(a-x)f(x)dx + \gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} -t\left(a+\frac{b}{\beta}-x\right)f(x)dx$$
$$+ \gamma\int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon}(B-w)f(x)dx.$$

The second-order derivative of (4) w.r.t. a and the crossing derivative are

$$V''_{aa} = -s - \frac{\gamma ta}{A} < 0$$

and

$$V''_{aw} = -\frac{\gamma\varepsilon}{A} < 0.$$

The Hessian is

$$H = \begin{vmatrix} V''_{ww} & V''_{aw} \\ V''_{aw} & V''_{aa} \end{vmatrix}.$$

We have that $V''_{ww} < 0$ and $V''_{aa} < 0$. Since $s > \beta$, $A > \varepsilon$, and $\gamma < 1$, we have

$$V''_{ww}V''_{aa} - \left(V''_{aw}\right)^2 = \left(-s - \frac{1}{A}\gamma ta\right)\left(-\frac{2\gamma\varepsilon}{A\beta}\right) - \left(\frac{\gamma\varepsilon}{A}\right)^2 = \frac{\gamma\varepsilon}{A^2}\left(\left(\frac{s}{\beta}2A + \frac{2\gamma ta}{\beta}\right) - \gamma\varepsilon\right) > 0.$$

Therefore, the Hessian is negative definite.

Thus, the access level is given by

$$a = \frac{A}{\gamma t}\left(-s + \sqrt{s^2 + \frac{2}{A}\gamma t\left(B + (B - w)\gamma\frac{\varepsilon}{A}\right)}\right). \tag{10}$$

Solving (7) into (10), we have the close form solution of the regular access level,

$$a_{11} = \frac{-\left(2As - \gamma\beta\varepsilon\right) + \sqrt{\left(2As - \gamma\beta\varepsilon\right)^2 - 4\gamma t\left(-2\gamma\varepsilon B - 2AB + \gamma(B - b)\varepsilon - \gamma\beta\frac{1}{2}(A - \varepsilon)^2\right)}}{2\gamma t}$$

or

$$a_{10} = \frac{A}{\gamma t}\left(-s + \sqrt{s^2 + \frac{2}{A}\gamma t\left(B + B\gamma\frac{\varepsilon}{A}\right)}\right).$$

Therefore,

$$a_1^* = \min\{a_{10}, a_{11}\}. \tag{11}$$

Substituting (11) into (6) and (7), we have the penalty for underentitlement and the optimal bonus rate.

If $a^* + (w^* + b)/\beta + \varepsilon > A$, the optimization problem is represented by (8).

The first-order derivative of (8) w.r.t. a,

$$V_a' = B - sa + \gamma\int_0^{a-\varepsilon}\left(-t\left(a-x\right)\right)f\left(x\right)dx + \gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}}\left(-t\left(a+\frac{b}{\beta}-x\right)\right)f\left(x\right)dx + \gamma\int_{a+\frac{w+b}{\beta}}^{A}\left(B-w\right)f\left(x\right)dx.$$

The second-order derivative of (8) w.r.t. a and the crossing derivative are

$$V_{aa}'' = -s - \frac{\gamma ta}{A} - \frac{\gamma\left(B-w\right)}{A} < 0$$

and

$$V_{aw}'' = -\frac{\gamma}{A}\left(A-a-\frac{w+b}{\beta}\right) - \frac{\gamma\left(B-w\right)}{A\beta} < 0.$$

The Hessian is

$$H = \begin{vmatrix} V_{ww}'' & V_{aw}'' \\ V_{aw}'' & V_{aa}'' \end{vmatrix}.$$

We have $V_{ww}'' < 0$ and $V_{aa}'' < 0$. We next examine

$$V_{ww}''V_{aa}'' - \left(V_{aw}''\right)^2 = \left(s + \frac{\gamma ta}{A} + \frac{\gamma}{A}\left(B-w\right)\right)\left(\frac{2\gamma}{A\beta}\left(A-a-\frac{w+b}{\beta}\right) + \frac{\gamma\left(B-w\right)}{A\beta^2}\right) - \left(\frac{\gamma}{A}\left(A-a-\frac{w+b}{\beta}\right) + \frac{\gamma\left(B-w\right)}{A\beta}\right)^2.$$

Since $s > \beta$, $A > \varepsilon$, and $\gamma < 1$, we have

$$\frac{s}{\beta} + \frac{\gamma ta}{A\beta} > \frac{\varepsilon}{A}\gamma > \frac{\gamma}{A}\left(A-a-\frac{w+b}{\beta}\right).$$

We can deduce that

$$\left(s + \frac{\gamma ta}{A} + \frac{\gamma}{A}\left(B-w\right)\right)\frac{1}{\beta} > \frac{\gamma}{A}\left(A-a-\frac{w+b}{\beta}\right) + \frac{\gamma\left(B-w\right)}{A\beta}$$

and

$$\frac{2\gamma}{A}\left(A-a-\frac{w+b}{\beta}\right) + \frac{\gamma\left(B-w\right)}{A\beta} > \frac{\gamma}{A}\left(A-a-\frac{w+b}{\beta}\right) + \frac{\gamma\left(B-w\right)}{A\beta}.$$

Therefore, $V''_{ww}V''_{aa} - (V''_{aw})^2 > 0$ and the Hessian is negative definite.

Thus, the access level is given by

$$a_2 = \frac{-\left(As + \gamma\left(B - w\right)\right) + \sqrt{\left(As + \gamma\left(B - w\right)\right)^2 + 2\gamma t\left(\gamma\left(B - w\right)\left(A - \frac{w + b}{\beta}\right) + AB\right)}}{\gamma t}. \quad (12)$$

Solving (9) and (12) together, we have the close form solution of the regular access level and bonus rate. Q.E.D.

Proof 6 of Proposition 3 (Bonus and Regular Access Substitution Proposition)

If $a^* + (w^* + b)/\beta + \varepsilon \le A$, the second-order crossing derivative of (4) w.r.t. w and a is, $V''_{aw} = -\gamma\varepsilon/A < 0$.

Otherwise, the second-order crossing derivative of (8) w.r.t. w and a is

$$V''_{aw} = -\frac{\gamma}{A}\left(A - a - \frac{w + b}{\beta}\right) - \frac{\gamma\left(B - w\right)}{A\beta} < 0.$$

Thus, w and a are substitutes. Q.E.D.

Proof of Corollary 1 (Decreasing Bonus Rate in Regular Access Corollary)

Differentiate w w.r.t. a, $w'_a = -\beta/2$ if $a^* + (w^* + b)/\beta + \varepsilon \le A$. Otherwise

$$w'_a = \frac{\beta}{3}\left(-2 + \frac{\left(a + \frac{b}{\beta} - A + \frac{B}{\beta}\right)}{\sqrt{\left(a + \frac{b}{\beta} - A + \frac{B}{\beta}\right)^2 + 3A^2}}\right) < 0.$$

Therefore, the bonus rate is decreasing in the regular access. Q.E.D.

XIA ZHAO (x_zhao3@uncg.edu) is an assistant professor of information systems at the Bryan School of Business and Economics, University of North Carolina at Greensboro. She is also a research fellow at the Center for Digital Strategies at the Tuck School of Business, Dartmouth College. She received her Ph.D. in management science and information systems from the McCombs School of Business at the University of Texas at Austin, and her master's and bachelor's degrees in engineering from Tsinghua University, China. Her research interests include the economics of information systems, information security, electronic commerce, and IT governance. Her publications have appeared in *Decision Support Systems*, *International Journal of Electronic Commerce*, *IEEE Computer*, and many conference volumes. Her recent paper on mechanism design for

better Internet security received the Citation of Excellence Award from the Emerald Management Review Independent Review Board.

M. ERIC JOHNSON (m.eric.johnson@dartmouth.edu) is director of the Glassmeyer/McNamee Center for Digital Strategies and the Benjamin Ames Kimball Professor of the Science of Administration Management at the Tuck School of Business, Dartmouth College. His teaching and research focuses on the impact of information technology on business processes. Through grants from the National Institute of Standards and Technology, Department of Justice, the Department of Homeland Security, and the National Science Foundation, he is studying the challenges of information security in the extended enterprise. He has testified before the U.S. Congress on information security and published many related articles in the *Wall Street Journal*, *Financial Times*, *Sloan Management Review*, *Harvard Business Review*, and *CIO Magazine*. He holds a B.S. in engineering, a B.S. in economics and an M.S. in engineering and operations research from Penn State University, and a Ph.D. in engineering from Stanford University.