

Practices for Managing Information Flows Within Organizations

Joel S. Demski
University of Florida

Tracy R. Lewis
University of Florida

Dennis Yao
University of Pennsylvania

Hüseyin Yildirim
University of Florida

Firm organization determines how coworkers communicate and how information flows within the firm. Banking, accounting, consulting, and legal firms process proprietary information which their clients wish to protect. The firm's ability to safeguard and manage information determines its market demand. Yet employees may leak and otherwise abuse information to enhance their personal performance and wealth. This article analyzes how bureaucracies are erected within the firm to control information flows and protect clients.

1. Introduction

Information intermediaries, firms specializing in the collection and analysis of information, benefit by undertaking complementary activities and servicing clients with related interests. Leading examples of information intermediaries include investment and commercial banks, accounting firms, consulting firms and legal practices. For such firms, the knowledge gleaned from performing one activity aids in the performance of related tasks. For example, an investment bank learns information by underwriting new securities, enabling it to effectively market assets to its customers. A law firm representing clients from related markets acquires knowledge of market contacts, conditions, and regulations enhancing the firm's performance in future work. For all

This article was prepared for presentation at the April 1998 *Journal of Law, Economics, & Organization* Conference on Bureaucracy. The authors thank George Baker, Bob Gibbons, Paul Milgrom, Bill Rogerson, Alan Schwartz, Pablo Spiller, Lars Stole, *JLEO* conference participants and seminar attendees at MIT and the University of Pennsylvania for their insightful comments on a previous draft of this article.

these cases, intrafirm information flows facilitate the creation of information economies.¹

Some management consultants have further argued corporations should abandon the tendency to keep knowledge confined to the organization. Instead, knowledge should be allowed to flow across corporate boundaries.² This argument relies on the belief that the global economy is becoming more information based. Firms utilizing information more rapidly and effectively prosper. Cooperative generation and sharing of information endows firms with economies of scale and scope.³ Barriers preventing information flows defeat this process. Thus the traditional “need to know” rule for controlling knowledge within a firm is counterproductive.

However, the unfettered transmission of information within and between firms is unwise. When information flows are uncontrolled, a client’s sensitive and proprietary information about an unpatented production idea, business plans, customer lists, and financial situation cannot be protected. Information property rights cannot be defined, much less enforced.⁴ Information leakages from employee discussions, betrayal of client confidences by financial and legal advisors, and the careless management of a client’s commercial secrets are some primary information abuses. Opportunities for the illicit transfer of confidential information multiply as buyer and seller links increase and corporate strategic alliances grow.

Absent safeguards for managing and protecting information, markets for certain legal, financial, and consulting services may not exist, as clients prevent

1. Stewart (1997) cites several examples of firms pursuing conscious policies to facilitate internal information transfer. Booz Allen has a system called Knowledge On-Line that allows its consultants to access other experts of the firm (p. 112). McKinsey has a team trained to connect its people with the firm’s existing information and expertise (p. 125). Monsanto has a knowledge management architecture providing its salespeople with both hard and soft information (p. 117).

2. See, for example, Stewart (1997:102), “The biggest risk, however, is not that they will blurt company secrets or wander off irrelevant intellectual byways but that the heavy hand of management will choke them. Learning communities cannot be contiguous with the boundaries of the corporation, business unit, or department; nor should they be.” Traditional buyer-supplier relationships are also undergoing change. For example, a senior account executive for supermarkets for Coors Brewing Co. remarks “Like never before, sales reps will be privy to a wealth of confidential information—a retailer’s category sales, costs and pricing, profit measures and allowances. In return, with considerable input from the retailer, the reps will be expected to reveal all they know about marketing the category, in terms that the retailer can use to make decisions.” “Trust, and a willingness to share”. 1994 *Progressive Grocer* 73(12):SS14-SS15.

3. See Hughes and Kao (1966) for a discussion of the benefits and costs of information flows in vertically integrated firms. Also see the account by Saxenian (1994) on the importance of information flows between high-technology firms in the success of Silicon Valley.

4. Laws, professional codes, and commercial practices militate against the breach of commercial confidences. But the intangible nature of knowledge and information, and the difficulty associated with determining the source of a leak makes misuse of commercial confidences relatively easy. Further, the misuse of the confidential information may not even be deliberate. For example, a consultant’s recommendation to client B may not make explicit use of confidential information from another client A. But the ideas or organizing principle that the consultant conveys may reveal sensitive information about client A.

their commercial confidences from being leaked to outsiders. The welfare losses from such market failure are potentially large. Policy makers debate how best to eliminate mismanagement of proprietary information. One view holds that competition among information intermediaries to attract and retain clients should by itself induce these firms to adequately protect client's proprietary information.⁵ Others argue that market competition is insufficient to prevent information abuses.⁶ One needs legal and regulatory intervention restricting firms' activities and requiring the firms to protect information with physical and organizational walls.

This article is a first attempt to formally evaluate these alternative approaches to information management.⁷ We model the information intermediary's internal organization and consider the strategies for these firms to regulate information. To be concrete, we model a "consulting firm" who advises clients on some aspect of their business. Clients retain the firm because of the "brilliance of its employees," and the firm's available stock of information to assist clients. Each client reveals sensitive information to the firm in the course of being served. Firm employees wish to access a client's proprietary information to reduce their personal costs of assisting other clients.⁸

The firm employs various structural and organizational strategies for protecting clients' information. One strategy is to regulate the mixture of clients to reduce conflicts of interests. A second strategy is to select compensation to affect employees' incentives to breach information security. Typically employees are imperfect agents for the firm, and they must be financially motivated to perform. High-powered performance incentives may cause employees to breach information excessively. A third approach is to erect physical and organization barriers to restricting employees' access to the firm's proprietary information bank. Such barriers are sometimes called Chinese walls.^{9,10}

This article is organized as follows: we present the elements of our model in Section 2. In Section 3 we examine the claim that market forces may discipline the firm to implement efficient structural and organizational strategies for managing information. We find market forces will typically be insufficient to induce

5. See Fischer et al. (1984), Soare (1988), Kelley (1995), and Saunders (1995) and the references cited therein for a discussion of this view in the context of accounting firms and banks.

6. Doty and Powers (1988), for example, discuss the requirement of The Insider Trading and Securities Fraud Enforcement Act for 1988 for securities firms to institute some Chinese walls. In recent years the U.S. federal antitrust agencies have also negotiated some Chinese wall requirements as the price to allow some acquisitions to consummate.

7. Previous analyzes of information management have primarily been informal and institutional.

8. Alternatively, as in exploiting insider information for personal profit, the employee may wish to use a client's private information for personal profit or gain.

9. See McVea (1993) (especially pp. 213–230) for a discussion of the costs and benefits of Chinese walls.

10. These bureaucratic and compensatory approaches are specifically designed for regulating information leaks. Other bureaucratic responses to managing organization including the control of influence costs (Milgrom, 1988), assignment of authority (Aghion and Tirole, 1997), restricting the scope of operations (Rotemberg and Saloner, 1994), and the oversight by multiple principals (Martimort, 1996) are designed to induce certain behaviors from employees.

efficient information management. Absent legal and regulatory enforcement, firms are unable to credibly commit to safeguard their clientele's information. In a market equilibrium, clients will rationally infer that firms will underinvest in information security. Nonetheless, we find that firms can signal their intention to prevent information leakage, by their client mix, by their client contracts, and by the organization of production. In particular, we find that employee-owned organizations and firms where employees are closely monitored may best exploit information economies and prevent information leakage with minimal distortion of performance incentives.

Section 4 examines legal and regulatory intervention in assigning liability for harmful information disclosure, and in mandating Chinese walls. We find firms typically benefit by bearing disclosure liability because they can thereby credibly commit to protecting a client's information. Such commitment increases the client's value of firm services. Regulations requiring the firm to erect information walls may also help. However, this policy is dominated by imposing greater financial sanctions on employees who leak private information.¹¹ Imposing sanctions is a more direct disincentive for employees to breach security than erecting information walls. However, the limited liability of employees restricts the sanctions one can practically enforce.

Section 5 concludes with some thoughts and conjectures about organizational and bureaucratic strategies for information management.

2. The Model

2.1 Customers

Customers require consulting services, like advice on locating a new store, marketing analysis, assistance in locating and purchasing an input, or litigation support. The firm's efforts can result in two levels of service, high (H) or low (L). Low service provides the customer with normalized utility of zero. High service yields customer utility levels of $U > 0$. The service delivered is publicly observable, and thus contractible. The client pays the firm a base fee R , plus a bonus ΔR if the service provided is high. Contracts with large rewards for high service are high-powered performance contracts, inducing the firm to provide superior service.

For now we imagine there is a single firm capable of providing the required services. Customers may alternatively self-supply services and receive an expected normalized payoff of zero. Section 5 considers the expanded setting where customers competing in the same market may be served by a common firm or by independent consulting firms.

2.2 The Firm

The firm's service level depends stochastically on the effort firm employees allocate. We denote by $p(e)$ the probability that service will be high, where e

11. The beneficial use of legal sanctions to modify employee behavior is discussed in Polinsky and Shavell (1993).

is the employee's effort. We assume $p'(e) > 0$, $p''(e) < 0$. Effort embodies research, data collection, and information analysis the employee performs for the client.

The employee's personal cost of supplying effort to a particular client is $bC(e; s)$, with $C(0; s) = 0$, $C_e, C_{ee} > 0$, and $C_s < 0$. The variable s is the firm's scope of clientele. Costs are decreasing in s , as firms servicing a rich and wide scope of clients enjoy economies of information and scope, lowering their employees' effort costs. For instance, a legal or management consulting firm advising most of the major corporations within an industry increases its collective knowledge of the market, participants' characteristics and influential contacts, and pertinent regulations. This information reduces employees' cost of service. As another example, accounting firms become more adept at auditing and advising clients, as the clientele scope and scale increases.¹²

The variable b , $\varepsilon[b, 1]$, is specific to each client and is observed by the employee but not by the client. b reflects the employee's cost saving by breaching the confidentiality of the firm's information trust. For example, an employee reduces his cost of advising a client by a factor of $1 - b$ by accessing private information about the strategic plan of the client's rivals. However, employees who breach may be detected and fined. L is the expected cost of breach to the employee if he is detected. For now we imagine that L is exogenously fixed, postponing until Section 4 an analysis of how employee sanctions are optimally determined. An employee deciding not to breach incurs the full cost of effort with $b = 1$, but he avoids financial sanctions, L .

The distribution of b , $G(b; s)$, is effected by the firm's scope of operation, s . $G(b; s)$ is increasing in s , as the opportunities for effort cost savings increase with firm scope and the greater knowledge of industry conditions and contacts the firm acquires.

The firm may restrict employees' information access by erecting a security system or information wall. The erection of a wall may include physically separating employees to discourage communication, controlling employee access to documents, and regulating employees' exposure to different clients. These measures affect the firm's bureaucracy and organization, and we discuss in detail bureaucratic strategies for managing information in Section 5. For now, we assume erecting a wall reduces the probability the employee may breach and access the firm's private information pool. $1 - z$ is the probability an employee may acquire private information to reduce effort costs. Walls are difficult to erect, and we assume there is a cost $f(z)$ of establishing security increasing at an increasing rate in z .

2.3 Employee Behavior

Employee payments are conditioned on the service level they provide. Employees receive a base payment of w and a bonus of Δw if performance is high. There are two types of firms, employee-owned firms and hired-employee

12. Recent mergers in the audit industry presumably reflect these scale and scope effects.

firms. In employee-owned firms, employees are the residual claimants of the profits they generate.¹³ Consequently the employee receives a bonus Δw for good performance equal to the additional revenues, ΔR , which the client pays for superior performance. In hired employee firms, the bonus payment, Δw , is selected by the firm to be some fraction of ΔR .

When confronting a client of type b , the employee decides whether to breach, and what effort to allocate in maximizing his expected net return as given by

$$W(b) \equiv \max[W^b, W^n], \quad (2.1)$$

where

$$W^n \equiv \max_e w + p(e)\Delta w - C(e, s) \quad (2.2)$$

$$W^b \equiv \max_e w + p(e)\Delta w - bC(e, s) - L \quad (2.3)$$

The employee compares expected return when he breaches and when he doesn't breach to select his preferred action. Employee behavior as characterized above, is summarized by the following:¹⁴

Observation 2.1. The employee allocates greater effort and the probability of high service increases whenever he breaches. The employee breaches whenever $b < b^*(\Delta w, L, s)$ and does not breach otherwise. The break frequency increases with Δw and decreases with L .

(Observation derivations not contained in the text appear in the Appendix.) Observation 2.1 indicates employees enhance performance by breaching, and they are induced to breach more often when their pay is sensitive to their performance. Sanctions, L , discourage breach. It is not possible to predict the effect on employee behavior of varying the scope of activities without placing greater structure on our model.

2.4 Firm Behavior in Setting Wages

When the firm is employee owned, the employee-owners receive a bonus $\Delta w = \Delta R$ whenever they provide high-level service. When the firm hires an employee it selects wage payments $(w, \Delta w)$ to maximize its profits. The employee enjoys limited liability and therefore receives nonnegative payment. For now we assume the firm does not incur any fines if it's employee breaches, although the employee is subject to a breach sanction, L . The firm sets wages $(w, \Delta w)$

13. In cases where there are several employee-owners, we assume each employee receives wages equaling the profits that he alone has generated. This is distinguished from employee-owned firms in which employees share common profits and are therefore not the residual claimants of the revenues they personally generate.

14. Throughout our analysis, we assume an interior solution to the employee's problem, with $e > 0$.

to maximize expected profits for each client,¹⁵

$$V = \max E_b[R - w + (\Delta R - \Delta w)p(e^*(b, \Delta w))], \quad (2.4)$$

subject to (for hired employee firm)

$$W = E_b W(b) \geq 0, \quad (2.5)$$

where E_b is the expectation taken over b , and $e^*(b, \Delta w)$ is the agent's optimal effort conditional on the breach decision and Δw . Since $w > 0$, it is easy to see Equation (2.5) is not binding. (The employee always attains nonnegative wages by not breaching and supplying zero effort.) The firm's optimal wage is characterized in:

Observation 2.2. Under the optimal wage contract, the hired employee receives a fraction of the performance surplus, so that $\Delta w < \Delta R$. The wage differential, Δw , awarded for high performance is increasing in ΔR .

Observation 2.2 points out an important difference between employee-owned and hired-employee firms. Since a hired employee receives a fraction of the surplus generated from superior performance, his incentives to exploit sensitive information for improving firm performance is reduced compared to the employee-owner. Further, the firm can ensure clients that the employee is less likely to breach by reducing the employee performance incentive. Observation 2.2 indicates a credible device, reducing performance incentives not requiring clients to monitor the firm's wages is for the firm to negotiate low-powered performance contracts. Since it's unlikely that clients can observe an employee's actual compensation, the setting of the client's performance contracts is effective for controlling employees' incentives to breach.

3. Market Force Discipline

This section examines the power of market forces in disciplining the firm to control the misuse of sensitive information. To abstract from market structure, and to examine a setting where market forces are most powerful, we envision the firm captures all the client's surplus from service. This occurs when the firm provides a unique service and therefore has a surplus of clients. (Section 5 explores settings where customers have a choice with whom to contract). Recall, when service is low, the client receives a normalized return of zero. When service is high, the client receives $U > 0$. In addition, the client may be harmed in subsequent periods if the employee misuses the client's sensitive information to assist other clients of the firm. All clients are expected to be harmed from an information breach, with the same probability. The expected harm is $DG(b^*(\Delta w, L, s); s)$. D is each client's expected cost from breach.

15. In the case of a hired employee, we abstract from the possibility that firm owners may offer different wage schedules conditioned on the employees report of b . Given the employee is unable to make positive payments to the firm, it would be expensive for owners to implement a separating wage policy. To avoid unnecessary complications, we ignore this possibility.

For example, D reflects the expected cost increase to a client of doing business in the future when strategic information is leaked to its competitors.¹⁶ The probability of breach, $G(b^*; s)$, is effected by wages Δw , by employee sanctions L , and by the scope of operations s . For now we imagine $z = 0$, so employees can freely access the firm's proprietary information bank. (We consider the erecting of walls to restrict access in our discussion of legal policy and regulation in Section 4. There we show firms will not erect walls to restrict information flows unless regulated to do so.)

3.1 Employee-Owned Firms

The firm selects a performance contract $(R, \Delta R)$ to maximize its net expected profit. The base payment, R , is set to tax away all the client's expected surplus, and the firm selects the differential performance award, ΔR , to induce the desired effort from itself, the employee-owner. We first consider the case where the firm can commit to a breach policy. The firm commits to only breach for clients with $b < b^*$, where b^* is chosen by the firm. That such a policy could be feasibly implemented and verified by clients is, we admit, unlikely.¹⁷ We introduce the possibility as a benchmark to evaluate contracts for more realistic settings to follow.

For this setting the firm chooses ΔR , and b^* to¹⁸

$$\max E_b[p(e^*)U - bC(e^*) - DG(b^*)], \quad (3.1)$$

(where for convenience, we delete functional arguments where no confusion exists.) Equation (3.1) is the firm's expected profit for a representative client. Notice clients differ by their specific characteristics, as reflected by b , but all customers face the same expected breach costs $DG(b^*)$. Equation (3.1) indicates the firm captures all the client's surplus; it becomes the residual claimant of all benefits and costs generated from its behavior. For this setting we find

Observation 3.1. An employee owned firm that commits to a breach policy will manage information optimally, and will provide socially optimal service.

This benchmark setting identifies conditions for market forces to lead an expected profit-maximizing firm to optimally manage information. These conditions are (1) the employee is a perfect agent for the firm, and (2) the firm can commit to an information management policy. Relaxing either condition leads the firm to act suboptimally.

16. Although we focus on cases where D is a cost, in principle, D could be negative, reflecting a benefit to the firm when its private information is leaked. For instance, rival firms may benefit from coordination when the marketing plans of one firm are leaked to a rival.

17. It might be possible for the firm to credibly limit leakage of information, by restricting access to sensitive information by segmenting tasks, and by consciously rotating personnel. Both are common features in the audit industry. Blackjack dealers are also routinely rotated. The idea in both cases is to interrupt a building relationship. In one case we interpret this as interrupting the acquisition of information that could be useful in sabotaging the control system.

18. In deriving Equation (3.1) we assume fines for employee sanctions are paid directly to the client. This is a transfer of wealth from the firm to the client, which the firm taxes away in setting R .

Now consider the more realistic setting where the firm is unable to commit to a breach policy. The compensation contracts now determine the probability of breach. The firm chooses ΔR to

$$\max E_b[p(e^*)U - bC(e^*)] - DG(b^*) = V \quad (3.2)$$

Equation (3.2) indicates that the benefits from breach accrue to the firm as a current reduction in the cost of servicing a client. However, the firm incurs costs from breach because clients reduce payments anticipating the eventual harm they may suffer from having their information misused. In maximizing Equation (3.2) the firm recognizes its own opportunistic subgame behavior. The first-order condition characterizing the solution to Equation (3.2) is

$$E_b(p_e U - bC_e)(de^*/d\Delta R) + \{[p(e^*(b^*)) - p(e^*(1))]U - [b^*C(e^*(b^*)) - C(e^*(1))] - D\}g(b^*)(db^*/d\Delta R) = 0. \quad (3.3)$$

The first term in Equation (3.3) is the expected return of inducing greater effort from increasing rewards for success, ΔR . The second term is the firm's net return as breach increases in response to greater incentives to succeed. Notice this private return from breach coincides with social returns. That is, social returns equal $[p(e^*(b^*)) - p(e^*(1))]U$, the expected value of the increase in the probability of success, minus $[b^*C(e^*(b^*)) - C(e^*(1))]$, the additional cost of greater effort, minus D , the client's expected breach cost.

The firm's incentive to breach will depend on the contract it signs and on the breach sanction the employee incurs. When sanctions are small, the employee will breach too frequently. Of interest, the firm will benefit from greater sanctions reducing the frequency of breach. Generally, though, the firm will be unable to commit to assessing its employees higher breach fines.¹⁹ An alternative strategy for the firm to reduce breach is to decrease the employee bonus from succeeding. The following observation indicates how the firm adjusts performance incentives to affect the breach frequency. In this observation dV/db^* is the marginal breach profits defined by

$$dV/db^* = \{[p(e^*(b^*)) - p(e^*(1))]U - [b^*C(e^*(b^*)) - C(e^*(1))] - D\}g(b^*)$$

Observation 3.2. The firm's preferences for sanctions coincide with social incentives. In addition $U(<, =, >)\Delta R$ as $dV/db^*(>, =, <)0$.

Comparing Observations 3.1 and 3.2 reveals the firm's benefit of committing to a breach policy. Absent this commitment, the firm must distort its compensation contract to affect the breach probability. In the most likely case, where breach sanctions are low, dV/db^* is negative as breach occurs too frequently, and the firm decreases performance incentives, ΔR , to limit breach. The firm's

19. Typically it will not be possible for the client to observe whether the firm enforces a policy of penalizing its employees when they breach. Further, for the setting of this model the firm will have no incentive to enforce such a policy since it will deter employees from exerting greater effort to supply good service.

inability to directly manage proprietary information forces it to operate under lower-power incentives.

3.2 Hired-Employee Firm

The firm hiring an employee must solve two agency problems. First, the firm cannot monitor the agent's effort to succeed, and must induce the agent to provide high quality service by offering a bonus Δw . Second, the employee privately observes b , reflecting breach benefits. Again the firm must control the agent's breach frequency by manipulating Δw .

To deal with these two problems, the firm selects compensation to

$$\max E_b[p(e^*)(U - \Delta w)] - DG(b^*) = V. \quad (3.4)$$

In maximizing Equation (3.4) the firm must contend with the employee's subgame opportunistic behavior. The first-order condition characterizing the solution to Equation (3.4) is

$$E_b[p_e(de^*/d\Delta w)(U - \Delta w) - p] + (dV/db^*)(db^*/d\Delta w) = 0, \quad (3.5)$$

where

$$dV/db^* = \{[(p(e(b^*)) - p(e^*(1)))(U - \Delta w) - D]g(b^*)\}. \quad (3.6)$$

The first term in Equation (3.5) is the net return from offering employees a greater performance bonus. Higher bonuses increase the probability of superior performance, but also increase the employee's reward.

The second term in Equation (3.5) is the firm's marginal breach profit, dV/db^* , multiplied by the rate of breach increase resulting from a performance bonus increase. Expected marginal breach profits dV/db^* , given by Equation (3.6), consist of two terms. The first is the firm's net increase in breach returns, $[p(e^*(b^*)) - p(e^*(1))](U - \Delta w)$. The second, $-D$, is the client's expected breach loss. The firm absorbs this expected loss in lower fees it can charge clients. Note that at b^* the firm must pay the employee $[p(e^*(b^*)) - p(e^*(1))]\Delta w$, which exceeds the additional effort costs from breach, $b^*C(b^*) - C(e^*(1))$. Combining this with Equation (3.6) implies

$$\begin{aligned} dV/db^* &= \{[p(e^*(b^*)) - p(e^*(1))](U - \Delta w) - D\}g(b^*) \\ &< \{[(p(e^*(b^*)) - p(e^*(1)))]U \\ &\quad - [b^*C(e^*(b^*)) - C(e^*(1))] - D\}g(b^*). \end{aligned} \quad (3.7)$$

The right-hand side of Equation (3.7) is the net social return from breach. This together with Equation (3.4) implies

Observation 3.3. When employees are hired, the firm undervalues breaches, given Δw . In addition the firm receives a fraction of the surplus generated from good performance as $U > \Delta R > \Delta w$, provided $dV/db^* < 0$ and $db^*/\Delta w > 0$.

The intuition for the first part of Observation 3.3 is the firm's hired employee earns rents because the effort supply cannot be monitored. To induce effort the

firm pays its employee an expected breach bonus, $[p(b^*) - p(1)]\Delta w$, exceeding the employee's additional costs of effort under breach. Consequently the firm undervalues breach, as it does not realize the full social return from breach.

The second part of Observation 3.3 indicates how the dilution of the firm's performance incentives results from its need to control its employees' breach activity.²⁰ Note if breaching activity is unaffected by small variations in employee compensation, so $db^*/\Delta w = 0$, Observation 3.1 implies that $\Delta R = U$, and the firm retains all additional surplus from performing well. The employees will not adjust his breach frequency in extreme settings where his breach cost, L , is zero, so he will always breach.

In intermediate settings, where L is strictly positive and the employee breaches occasionally, increasing compensation induces more breach. To credibly control the breach probability, the firm selects a lower-powered payment scheme. This reduces the firm's performance rewards and consequently reduces the performance surplus the firm offers its employees. This results in less frequent breach and a performance decline.

The performance decline is a necessary cost the firm incurs in managing its employees when other controls, such as Chinese walls, and monitoring (either by the firm or concerned client) aren't available. One would predict that the firm's normal agency problems are exacerbated when the firm must also control proprietary information leaks. This prediction is reflected in the following observation. Let Δw^i , V^i , and SS^i denote the equilibrium performance bonus, firm profits, and social surplus, respectively, where $i = O$ (the firm is employee owned) or $i = H$ (employee are hired). Assume in both cases that the firm is unable to commit to a breach frequency. Then we have

Observation 3.4. In equilibrium $\Delta w^H < \Delta w^O$, $V^H < V^O$, and $SS^H < SS^O$.

Observation 3.4 implies employee-owned firms who can closely monitor their employees can manage information leakage with smaller performance distortions. Consequently these firms offer their employees higher performance incentives, and consequently generate greater profit and social surplus. Firms contending with agency problems respond by reducing employee performance incentives. While this diminishes performance, it also decreases information leakage.²¹

20. When $dV/db^* > 0$, $\Delta R > U$, as the firm offers super-powered incentives to induce employees to breach more often.

21. Weakening of performance incentives in response to information problems has been identified in other contexts as well. Laffont and Tirole (1991) demonstrate it may be useful to reduce performance incentives where agents may be bribed or corrupted. Holmström and Milgrom (1991) demonstrate that incentives to perform one task may be diluted to prevent the employee from shirking on other tasks. The weakening of performance incentives also corresponds to institutional features of some organizations. Auditors typically operate under low-power explicit incentives. Professional standards of due care, internal labor markets, and credible professional sanctions are also factors influencing auditors behavior.

3.3 Scope of Activities

Aside from setting contract terms and wages, the firm also controls performance and employee breach frequency by the scope of clients it serves. Firms adjust their service scope by selecting service variety. Audit firms, for example, routinely offer managerial consulting in addition to accounting services. Reducing scope decreases employees' opportunities to leak information, however, it will also reduce information economies from offering complementary services.²²

When a firm's scope is fixed, by technology or institutional constraints, it is interesting to know how scope affects the firm's contracting and wage policy. Whether wider-scope firms offer higher- or lower-powered employee incentives cannot be determined without placing additional structure on our model. For this purpose, consider this special case:

Example: $p(e) = ke^\gamma, k > 0, 0 < \gamma < 1,$
 $bC(e, s) = be/f(s), f(s) > 0$
 $g(b; s)$ is uniformly distributed over $[b(s), 1], db/ds < 0$

For this example we define effort in efficiency units, with a unit effort cost $b/f(s)$ which increases with b , and decreases with s . The success probability is an isoelastic function of effort. The value of information breach, which decreases with b , is uniformly distributed with the expected breach value increasing with s . For this example we assume sanctions are low, so that on the margin there is excessive breach in equilibrium. This seems most reasonable because the firm's ability to impose large employee sanctions is reduced by employees limited liability responsibility, and by the fact it is difficult to prove culpability. (If a breach occurred, it is difficult to identify which of several employees having access to sensitive information is culpable.) We find for our example:

Observation 3.5. Employee-owned firms and hired-employee firms offering a wider scope of services (a) operate under higher-powered contracts, (b) offer their employees higher-powered employee incentives, (c) provide higher levels of service, and (d) breach more frequently.

Wide-scope firms enjoy information economies, enabling their employees to supply effort at low cost. The firm offers high-powered employee incentives to exploit these information economies and generate high effort at low cost. Firm performance is high. However, by offering large performance rewards, the firm encourages employee breach, which is already high in wide-scope firms. This illustrates how firm compensation reinforces the effects of greater scope on performance and breach frequency.

22. Contracting for a variety of tasks may also allow the firm to better control the activities of its employees through the use of countervailing incentives [see Lewis and Sappington (1989a,b) and Antle and Demski (1991)].

4. Walls and the Regulation of Information Security

This section examines the beneficial role of legal requirements for firms to establish walls and information security. In the absence of regulation, or the assignment of liability, firms failing to protect clients from breach costs suffer revenue loss. Despite the firm's incentive to avoid excess breach, we find market forces are generally ineffective in inducing proper levels of security. This finding is reported in

Observation 4.1. In a market equilibrium without regulation, the firm implements minimal information security unless clients monitor the firm's activity to manage information flows.

Market forces alone are insufficient to induce the firm to control employee activities.²³ This occurs because customers are unable to observe and monitor the firm's information security system. Absent the ability for firms to commit to an information security level $z > 0$, clients rationally expect the firm to implement the least cost security level $z = 0$. Once the firm has signed a client contract, it has no incentives to restrict information flows, unless it is liable for its customers' breach damages. However, to establish and enforce liability requires outside legal and regulatory intervention.

The static nature of our model overstates the firm's difficulty in policing breach. In an ongoing customer relationship, a firm might establish walls to restrict information access to avoid losing clients adversely affected by breach in the future. However, the firm's self-policing incentive to restrict information flows will be imperfect, as some customers will be one time clients and other customers may eventually exit the market to be replaced by new ones. Though the firm's commitment to establishing walls is understated in our model, it would still be imperfect in a more realistic dynamic setting.

When a client suffers breach damages, she may be partially compensated from the collection of employee sanctions. The firm will benefit by becoming liable for any uncompensated breach damages its client suffers. The reason is the firm may credibly commit to establishing some level of information security to reduce its liability from employee breaches. If it is unprofitable to implement walls, due to their expense, the firm does not suffer from the imposition of liability. The firm recoups the additional liability payments to the client by charging higher initial service fees. These findings are recorded in

Observation 4.2. The firm benefits from being liable for any uncompensated client damages from breach.

23. In theory, firms could contract to compensate clients for costs of breach whenever the firm's employee is observed breaching. If such contracts could be enforced, then firms could presumably commit to installing efficient security to guard information. While this is a theoretical possibility, we doubt it could be practically implemented. The difficulty of observing and convicting guilty employees, and the possible collusion between the firm and its employee to conceal breach would render this scheme impractical.

For employee-owned firms, assigning firms liability for uncompensated expenses will induce the firm employee to maximize social surplus. The employee becomes the residual claimant of all costs and benefits from his actions. For hired employee firms, liability assignment will increase welfare, though it will be insufficient to induce employees to behave efficiently.

The firm's incentive to erect walls and restrict information access will depend on its employees breach frequency, and the firm's marginal breach profitability. For instance, if employee breach sanctions are high, so breach is infrequent, erecting walls is unnecessary. However, if minimal breach sanctions exist, and breach occurs too often, the firm may strictly benefit from erecting walls to restrict information leaks. Given the existing level of walls, the firm will select a performance contract maximizing expected profits. The contract will determine the employees' effort in allocation and breach frequency. When the employee doesn't breach, and $b = 1$, the firm will earn an expected profit denoted by $v(1)$. When the employee breaches, the firm's profit will depend on b , the breach information advantage, and the firm will receive expected profit $v(b)$. The firm's expected profits of $V(z)$ as a function of the walls, level z , is

$$V(z) = zv(1) + (1 - z)\{v(1)[1 - G(b^*)] + E_{b < b^*}v(b)\} - f(z). \quad (4.1)$$

The firm's expected profit consists of the profit $v(1)$ when breach cannot occur, arising with probability z , plus the expected return when proprietary information is accessed, arising with probability $(1 - z)$. When breach is possible, it occurs when $b < b^*$, yielding a firm profit of $v(b)$, otherwise for $b > b^*$ the firm earns $v(1)$. The firm's marginal returns to erecting higher walls is²⁴

$$dV(z)/dz = -E_{b < b^*}[v(b) - v(1)] - f'(z). \quad (4.2)$$

As the firm erects higher walls it avoids the (possibly negative) differential profit from breaching over states $[b, b^*)$ and incurs additional security costs. Notice $v(b^*) - v(1)$, the firm's net breaching return in the marginal state b^* , is less than $v(b) - v(1)$ for all $b < b^*$, since breaching profits increase with lower b 's. This implies

Observation 4.3. Erecting walls to restrict information access will only benefit the firm if $v(b^*) - v(1) < 0$ and the firm desires to reduce the breach frequency. However, incentives to reduce breach frequency on the margin are not sufficient to warrant tighter security.

Observation 4.3 illustrates how employee sanctions and walls are substitutes for managing information. Only when employee breach sanctions are sufficiently low that breach occurs too frequently will the firm implement walls. The firm will most likely lobby to increase legal sanctions for breach against its employee before it erects higher walls. Increasing legal sanctions reduces the frequency of breach at zero cost to the firm, whereas erecting higher walls to reduce breach is costly. Further, erecting higher walls is less predictable in

24. Here we are employing the envelope theorem.

reducing unprofitable breach.²⁵ Compared to increasing breach sanctions, reducing access to information decreases the opportunities for breach in profitable instances where b is sufficiently small.

4.2 Response of Performance and Compensation Contracts to Walls

It is interesting to know how the firm's compensation varies with the level of walls. To examine this we return to our example where we find²⁶

Observation 4.4. Firms with higher walls implement more powerful performance and compensation schemes.

We find the erection of walls permits firms to implement more powerful performance contracts, and to provide greater inducement to employee performance. The erection of walls reduces the risk of excessive breach which otherwise occurs when performance incentives are high. Notice it is not possible to determine the net effect of walls in reducing breach frequency. Higher walls reduce breach, but breach increases when the firm implements more powerful performance incentives in response to a tighter security.

5. Bureaucratic Responses to Information Management

To this point we have explored the use of (1) explicit performance incentives, (2) the choice of clients to serve and activities to perform, and (3) the assignment of liability as the menu of instruments that might be used to manage information and, in particular, deal with the potential leakage of proprietary information.²⁷ Sensitive information is also managed by the ways in which customers and firms organize themselves, including their internal operating bureaucracies.

These organizational strategies for managing information are, however, more difficult to formally analyze. Consequently, at this stage we offer some preliminary and informal conjectures about how corporations, using auditing firms and clients as a canonical example, might employ organizational strategies to manage information flows and use. Throughout we continue with the theme of restricting, rather than encouraging, the leakage of proprietary information.

We have not explicitly modeled the role of repeated interaction between clients and consultants in managing information. Nonetheless, we acknowledge the importance of reputation in understanding the commercial and social fabric of information production, destruction, and transmission. Indeed, a folk theorem analogy might also be applied, arguing for a significant multiperiod perspective in approaching the breach decision. Auditors, lawyers, and peace officers are arguably reasonably well modeled in such fashion, at least for some

25. However, if Chinese walls could differentially restrict access so that information was less likely to leak when it was least valuable to the employee, it would become a more effective instrument for managing information flows.

26. The results for the employee-owned firm hold generally.

27. This follows a more or less traditional view of organization considerations, such as the emphasis on decision rights, rewards, and evaluation by Brickley, Smith, and Zimmerman (1996).

matters.²⁸ Entrepreneurs are, apparently, another matter.²⁹ And although an ongoing business relationship may dissuade a firm from exploiting a client's sensitive information, the incentives to guard information are unlikely to be perfect as some clients are not repeat customers, and consulting and commercial firms enter and exit the market with regularity. Furthermore, because many of the types of breaches we discuss are infrequently proven in court, and competing firms have an incentive to spread false rumors, most reputations may be rather soft.

5.1 Organizing the Firm to Manage Information

Regardless of reputation issues, though, organization appears to matter. Informally we predict firms become more hierarchical and more decentralized in their assignment of tasks in response to managing proprietary information. In particular, we expect such concern will lead the firm to delegate the supervision and management of particular clients to "employee-owners" or "partners" in the firm. This partner will be exclusively concerned with serving an identified set of clients. Exclusive oversight of these clients will provide the partner the focus and incentives to appropriately safeguard the clients' sensitive information. The compensation of the partner will be closely linked to his performance in satisfying these clients, especially in maintaining and expanding the firm's relationship with them. Our analysis in Section 3 suggests partners (i.e., "employee-owners") are more easily motivated to perform without abusing proprietary information (e.g., Observation 3.4). In addition, larger sanctions can be assessed the partner, thus providing the firm an additional instrument with which to control information breach (Observation 2.1). Thus we find that distributing firm ownership among employees is also beneficial in managing clients' information as well as solving the traditional agency problems of the firm identified by Jensen and Meckling (1976).³⁰

In complimentary fashion, the size of the partner's activities will be limited by his ability to delegate and supervise tasks to subordinates, or hired employees. The hired employees will be assigned specific tasks, tasks that are more

28. For example, Datar, Feltham, and Hughes (1991). Notice professional sanctions for, say, auditors suggest L is "large" (recall Observation 2.1). Repetition, in turn, reinforces the incentive to respect confidentiality. Even here, though, the issue is far from settled. Recent mergers in the audit industry have led to auditor turnover, ostensibly over security issues. Pepsi, for example, stresses its auditor must be well distanced from its chief rival, Coke. Apparently auditor reputation and expertise in internal control and confidentiality are not sufficient to appease some customers.

29. For that matter, the audit industry also exhibits entrepreneurial tendencies. The "Elliott Committee" (*Journal of Accountancy*, September 1996) stresses a broader product focus, one that emphasizes "assurance services." In this view, audit firms would become much more entrepreneurial, stressing services aimed at improving the quality of information in the hands (and minds) of various customers. This raises, in our view, important questions of organization design, both for the audit firm and its customers.

30. Our analysis has focused on how the structure of information flow and access within organizations impacts the incentives of employees to misuse confidential information within the firm. A closely related problem for the firm is that employees may choose to leave the firm and exploit the value of the information via a start-up. See, for example, Anton and Yao (1995) for a model of this problem.

generic in character and do not encompass sizable “amounts” of proprietary information. The tasks will be supervised, and outsourcing some tasks may also be exploited to advantage.³¹ In addition, the hired employees may be frequently rotated to work on different clients and to perform in different areas of the firm, thereby reducing their exposure to client-specific information. In short, we predict bureaucratic frictions will be used to limit breach possibilities.

We further suspect reliance on team production and relative performance evaluation schemes will be minimal in these instances. Team production will be discouraged to prevent dissemination of client sensitive information within the firm. Likewise, explicit tournaments will be less frequently used, again discouraging widespread dissemination of information within the firm. This suggests that bureaucratic responses to managing clients’ information may interfere with comparative compensation programs to enhance employee performance. On the other hand, the bureaucratic structure designed to prevent information leaks can also shield the “at risk” employees from heightened external labor market visibility.

Going further out on the proverbial limb, this sketch of bureaucratic tendencies bears some resemblance to anecdotal impressions of internal organizations observed in law firms, consulting firms, accounting houses, and advertising agencies. A common practice in consulting, for example, is for the lead individual, the partner, to select a team for a specific project, with the partner maintaining overall responsibility for the engagement. Likewise, audit firm clients are managed at the partner level, with elaborate task assignments, internal supervision, and rotation. The hired workers are jointly supervised by the client firm and by the customer, and the partner’s success or failure is gauged by his management of the long-term relationship with the client.³² This long-term relationship, in turn, covers a variety of audit, tax, and consulting services.

5.2 Matching Clients and Firms

Clients also manage their sensitive information through their choice of firms to employ. Competing clients may, for example, elect to contract with the same firm for some types of consulting services or with independent firms. Using a common firm affords the opportunity to exploit industry knowledge. For example, a particular audit firm might be specialized in agribusiness or in entertainment services. The common firm may also be positioned to coordinate

31. The typical consulting engagement relies on experts within the client and the consulting firm, implying both an exchange of expertise and mutual monitoring. Similarly, the typical audit relies on audit work by both the audit firm and the client’s internal audit staff. And recently, a trend of outsourcing the internal audit function has surfaced, implying yet a deeper web of mutual monitoring.

32. The customer sees a great deal of the consultant or the auditor; and customer evaluations of the personnel assigned by the producing firm are commonplace. In a related vein, a common practice in disposing of sensitive documents (shredding) is to outsource the service (reflecting a scale economy, as well as a certain social distance or wall), but to have the hired agent bring the shredding equipment and perform the shredding service on site, thereby affording an element of supervision.

the activities of its clients to their mutual advantage. To illustrate, the firm might offer aggregate survey data to each of the common firms, survey data that are summarization's of otherwise confidential information supplied by the clients themselves.

Naturally, too much movement in this direction increases the possibility of proprietary information leakages, not to mention antitrust concerns. Common agency frictions as highlighted in Stole (1990) and Martimort (1996) may also arise. In this instance, firms relying upon a common agent to provide service and advice must bid against each other to attain the allegiance and loyalty of their advisor and to avoid being sold out to other clients. This suggests clients may select different firms on different occasions and yet on other occasions may rely on internal provision of the service in question. For example, it is commonly claimed the course of action suggested most often by a consultant is the plan originally championed by the client management. Cynicism aside, this suggests a degree of competition between inside and outside professionals, which further speaks to the information leakage issue.

The ability of the firm to provide service and well manage proprietary information will also depend on its composition of clients. This, in turn, affects its attractiveness to various clients, and highlights the importance of its customer list. Thus customers will seek to "belong" to firms who service a desirable mixture of clients, just as individuals choose to belong to a golf club based on its membership. We expect value-enhancing mixtures of clients will tend to contract with the same firm as both firms and clients seek to find matches that enhance the value of service.³³ An interesting issue here is how firms will set service fees and how they will compete with each other to secure the most desirable membership or customer list.³⁴ Such lists are, for example, jealously defended in the audit industry, where auditor turnover is an unusual event (and one that calls for SEC mandated disclosure).

5.3 The Dynamic Side of Information Management

Turning to more of a dynamic perspective, repetition, as noted, is clearly important. So, too, is the economic environment. For this purpose, think of the client as an entrepreneurial organization. It searches for and selectively harvests production options in an ever-changing economic climate. It is not well defined by legal circumscription, as it manages a host of implicit relationships. In turn, information is a key factor in this ever-changing stock of options and web of relationships.

Historically, physical architecture was sufficient to control information flows. Sequestering employees in different buildings was a guarantee they would not converse or exchange information. The 13th-century trader did not have to worry about midtrip information leakage. Modern technology, though, has removed many of the attractive features of physical architecture in this regard. In

33. It also brings us to the analysis of clubs. See Sandler and Tschirhart (1980).

34. See the analysis of Scotchmer (1985) on the pricing of club membership to encourage optimal composition of members.

its place we see (and envision) the need for frictions of a far more subtle kind: bureaucracy or organizational architecture.³⁵ If currently popular management consultants like Stewart (1997) are correct, generating, processing, and managing information is likely to become an increasingly important factor influencing the bureaucratic structure and scope of the modern corporation.

This leads to our stress on endogenous frictions as an important instrument in controlling the temporal allocation of information (e.g., Observation 4.3). Moreover, the dynamic perspective leads us to envision an ebb and flow of various frictions as the environment changes. Varying procedures in internal labor markets, varying personnel practices, varying affiliations, varying subcontracting activities, and varying customer sets come to mind. More important, flexibility per se to mold bureaucracies to restrict or encourage information flows strikes us as being essential. Just as flexible manufacturing is the ability to quickly adapt, with minimal cost, to changing product specifications, flexible bureaucracy is the ability to quickly implement the appropriate array of organization frictions to manage information, a type of flexible wall, so to speak.

Appendix A

Proof of Observation 2.1. The employee's breach decision is governed by Equations (2.1)–(2.3) in the text. Denote $e(b, \Delta w, s)$ and $e(1, \Delta w, s)$ as the unique choices of efforts maximizing W^b and W^n , respectively. It is easy to verify that $e(b, \Delta w, s)$ is strictly decreasing in b , for $e(b, \Delta w, s) > 0$, and therefore the probability of success is greater under breach as $b \leq 1$, and $p(e)$ is increasing in e .

The employee breaches for all b such that

$$W^b \geq W^n$$

Since W^b is strictly decreasing in b for $e(b, \Delta w, s) > 0$, and W^n is constant in b , there exists a unique $b^*(\Delta w, L, s) \leq 1$ (with $<$, if $L > 0$), such that breach arises for all $\underline{b} \leq b \leq b^*$. When $b^* \leq \underline{b}$ breach does not occur.

For $b^* \in (\underline{b}, 1)$, b^* satisfies

$$[p(e(b^*, \Delta w, s))\Delta w - b^*C(e(b^*, \Delta w, s), s) - L] - [p(e(1, \Delta w, s))\Delta w - C(e(1, \Delta w, s), s)] = 0. \quad (\text{A1.1})$$

Totally differentiating (A1.1) with respect to Δw and L reveals that

$$\frac{\partial b^*}{\partial \Delta w} \stackrel{s}{=} p(e(b^*, \Delta w, s)) - p(e(1, \Delta w, s)) > 0 \quad (\text{A1.2})$$

$$\frac{\partial b^*}{\partial L} \stackrel{s}{=} -1 < 0, \quad (\text{A1.3})$$

thus completing the proof of Observation 2.1. ■

35. Milgrom (1988) stresses this theme in terms of managing influence costs.

Proof of Observation 2.2. For hired employees, Δw is chosen to maximize V as given by Equation (2.4) in the text. The solution for Δw is characterized by the first-order condition

$$\begin{aligned} \frac{dV}{d\Delta w} = E_b \left[(\Delta R - \Delta w) p_e \cdot \frac{de(\cdot)}{d\Delta w} - p(\cdot) \right] \\ + \{ [p(e(b^*, \Delta w, s))] \\ - p(e(1, \Delta w, s))] (\Delta R - \Delta w) \} g(b^*; s) \frac{db^*}{d\Delta w} = 0. \end{aligned} \quad (\text{A2.1})$$

Equation (A2.1) implies $\Delta R - \Delta w > 0$. Totally differentiating Equation (A2.1) with respect to ΔR reveals that

$$\begin{aligned} \frac{d\Delta w}{d\Delta R} \stackrel{s}{=} E_b \left\{ p_e \frac{de(\cdot)}{d\Delta w} \right\} + [p(e(b^*, \Delta w, s))] \\ - p(e(1, \Delta w, s))] g(b; s^*) \frac{db^*}{d\Delta w} > 0. \end{aligned} \quad (\text{A2.2})$$

Appendix B

Proof of Observation 3.1. The proof is supplied in the text. ■

Proof of Observation 3.2. Substituting the expression for dV^*/db^* in the text into Equation (3.3) yields the first-order condition for ΔR ,

$$\begin{aligned} E_b(p_e U - bC_e) de^*/d\Delta R + \partial V/\partial b^* (db^*/d\Delta R) = 0 \\ \Leftrightarrow E_b[p_e(U - \Delta R)] = -(\partial V/\partial b^*) (db^*/d\Delta R)/(de^*/d\Delta R) \\ \Leftrightarrow U \stackrel{\geq}{\leq} \Delta R \text{ as } \partial V/\partial b^* \stackrel{\leq}{\geq} 0, \end{aligned} \quad (\text{B2.1})$$

where the second line of Equation (B2.1) follows from the fact that $p_e \Delta R = bC_e$, and the third line results from the fact that $db^*/d\Delta R$ and $de^*/d\Delta R > 0$. ■

Proof of Observation 3.3. The first part of the observation is provided in the text. Substituting Equation (A2.1) into the first-order condition for Δw in Equation (3.5) of the text yields

$$E_b(U - \Delta R)(de^*/d\Delta w) = -(dV/db^*)(db^*/d\Delta w), \quad (\text{B3.1})$$

implying that $U > \Delta R$ when $dV/db^* < 0$. ■

Proof of Observation 3.4. Note that the marginal profitability of an increase in Δw for firm types O and H are, respectively,

$$\begin{aligned} dV^o/d\Delta w = E_b P \left[\frac{de}{e d\Delta w} (U - \Delta W) \right] \\ + g(b^*) \frac{db^*}{d\Delta w} \{ [p(e^*(b^*)) - p(e^*(1))] U \\ - [b^* C(e^*(b^*)) - C(e^*(1))] - D \} \end{aligned} \quad (\text{B4.2})$$

$$dV^H/d\Delta w = E_b \left[p_e \frac{de}{d\Delta w} (U - \Delta w) - p \right] + g(b^*) \frac{db^*}{d\Delta w} \{ [p(e^*(b^*)) - p(e^*(1))] (U - \Delta w) - D \}. \quad (\text{B4.2})$$

Subtracting Equation (B4.1) from (B4.2) yields

$$\frac{d(V^H - V^\circ)}{d\Delta w} = -g(b^*) \frac{db^*}{d\Delta w} \{ E_b p + [p(e^*(b^*)) - p(e^*(1))] \Delta w - [b^* C(e^*(b)) - C(e^*(1))] \} < 0. \quad (\text{B4.3})$$

Equation (B4.1) implies that since

$$\frac{dV(\Delta w^H)}{d\Delta w} = \frac{dV^\circ(\Delta w^\circ)}{d\Delta w} = 0,$$

that $\Delta w^H < \Delta w^\circ$.

That $V^H(\Delta w) > V^\circ(\Delta w)$ follows by inspection of Equations (3.1) and (3.4) in the text. Finally, notice that Δw° maximizes V° . Further, V° coincides with SS° , implying that Δw° maximizes social surplus. Consequently, $SS^\circ > SS^H$, since $\Delta w^\circ \neq \Delta w^H$. ■

Proof of Observation 3.5. For example in the text, $e^*(\Delta w, b, s)$ is given by

$$e^*(\Delta w, b, s) = \left(\frac{f(s) \cdot k \cdot \Delta w}{b} \right)^{\frac{1}{1-\gamma}} \quad (\text{B5.1})$$

and $p(e^*)$ is

$$p(e^*) = \frac{k^{\frac{1}{1-\gamma}}}{\gamma} \left(\frac{f(s) \Delta w}{b} \right)^{\frac{\gamma}{1-\gamma}} \quad (\text{B5.2})$$

For the employee-owned firm, $\Delta R^\circ = \Delta w^\circ$ is determined by the condition

$$V_{\Delta w}(\Delta w(s), s) = 0, \quad (\text{B5.3})$$

where V is defined in Equation (3.1) of the text. Totally differentiating Equation (B5.3) yields

$$\frac{d\Delta w}{ds} \stackrel{s}{=} V_{\Delta w, s}. \quad (\text{B5.4})$$

Substituting for e^* and $p(e^*)$ into $V(\Delta w(s), s)$, one can show with straightforward, though tedious calculations that $V_{\Delta w, s} > 0$. This proves that Δw (and ΔR) are increasing in s .

The performance of the firm as captured in the expected probability of success varies with scope, s , according to

$$\frac{d}{ds} [E_b p(e^*(\Delta w(s), s, b))] = E_b \left\{ p_e \left(\frac{de^*}{d\Delta w} \frac{d\Delta w}{ds} + \frac{de^*}{ds} \right) \right\} + \int_{\underline{b}}^1 p(e^*(\Delta w(s), s, b)) g_s(b) db$$

$$\begin{aligned}
& - \left(\frac{db}{ds} \right) p(e^*(\Delta w(s), \underline{b}))g(\underline{b}) \\
& + \frac{db^*(\Delta w, s)}{ds} \{p(e^*(\Delta w(s), s, b^*)) \\
& - p(e^*(\Delta w(s), s, 1))\}g(b^*). \tag{B5.5}
\end{aligned}$$

Evaluating Equation (B5.5) term by term, the first term is positive since $d\Delta w/ds > 0$ by Equation (B5.4) and $de^*/ds > 0$ by Equation (B5.1). Integrating the first part of the second term by parts we find that the second term simplifies to $\int_{\underline{b}}^1 p(e^*(\Delta w(s), s, b))G_s(b)db > 0$, since $G_s(b) > 0$. The third term is shown to be positive by substituting Equation (B5.1) into Equations (2.1)–(2.3) in the text to demonstrate that $db^*/ds > 0$. This proves that performance is increasing with scope.

The probability of breach, $G(b^*(s); s)$ is increasing in s , since

$$\frac{d}{ds}G(b^*(s), s) = G_s(b^*(s), s) + g(b^*)\frac{db^*}{ds} > 0. \tag{B5.5}$$

This completes our proof of Observation 3.5 for the case of employee-owned firms. For hired-employee firms, the proof proceeds similarly. ■

Appendix C

Proof of Observation 4.1. Consider the employee-owned firm. Once the performance bonus has been set, the firm selects z , the probability of restricting access to proprietary information, to

$$\begin{aligned}
& \max_z (1-z)E_b[p(e^*(b, \Delta R))\Delta R - bC(e^*(b, \Delta R)) - G(b^*)L] \\
& + z[p(e^*(1, \Delta R))\Delta R - C(e^*(1, \Delta R))] - f(z). \tag{C1.1}
\end{aligned}$$

Clearly the firm's profit is decreasing in z , since employees decide whether to breach optimally to maximize firm profits. Restricting the possibility of beach therefore decreases profits.

The hired employee firm selects z to

$$\begin{aligned}
& \max_z (1-z)E_b[p(e^*(b, \Delta w))(\Delta R - \Delta w)] \\
& + z[p(e^*(1, \Delta w))(\Delta R - \Delta w)] - f(z).
\end{aligned}$$

By the envelope theorem $V'(z)$, the increase in firm profit from restricting access is

$$\begin{aligned}
V'(z) = & -E_b(p(e^*(b, \Delta w))(\Delta R - \Delta w)) \\
& + p(e^*(1, \Delta w))(\Delta R - \Delta w) - f'(z) < 0. \tag{C2.1}
\end{aligned}$$

Consequently, z is set equal to zero. ■

Proof of Observations 4.2 and 4.3. The observations are proved in the text. ■

Proof of Observation 4.4. For the hired-employee firm, Δw is chosen to

$$\max(1 - z)E_b V^H(b) + zV^H(1) = V^H(\Delta w, z), \quad (\text{C4.1})$$

where

$$V^H(b) = p(e^*(b, \Delta w))(U - \Delta w) - \delta(b)D \text{ and } \delta(b) = \begin{cases} 1, & \text{if } b \leq b^* \\ 0, & \text{otherwise} \end{cases}. \quad (\text{C4.2})$$

Obviously

$$V^H(1) = p(e^*(1, \Delta w))(U - \Delta w). \quad (\text{C4.3})$$

The first-order condition for Δw is

$$V_{\Delta w}^H = (1 - z)E_b dV^H(b)/d\Delta w + z dV^H(1)/d\Delta w = 0. \quad (\text{C4.4})$$

Totally differentiating Equation (C4.4) with respect to z yields

$$\begin{aligned} \frac{d\Delta w}{dz} &\stackrel{s}{=} v_{\Delta w, z}^H \\ &= - \left\{ E_b \left[p_e \left(e^*(b, \Delta w) \frac{de^*}{d\Delta w} \right) (U - \Delta w) - p(\cdot) \right] + \frac{db^*}{d\Delta w} V_{b^*}^H \right\} \\ &\quad + p_e(e^*(1, \Delta w)) \frac{de^*}{d\Delta w} (U - \Delta w) - p(e^*(1, \Delta w)). \end{aligned} \quad (\text{C4.5})$$

Recall for the example, $p(e^*(b, \Delta w, s))$ is given by Equation (B5.2). Substituting Equation (B5.2) for p in Equation (C4.5) enables us to rewrite Equation (C4.5) as

$$\begin{aligned} \frac{d\Delta w}{dz} &\stackrel{s}{=} - \left\{ E_b \left[\left(\frac{\gamma}{1 - \gamma} \frac{(u - \Delta w)}{\Delta w} \right) - 1 \right] p(e^*(b, \Delta w)) + \frac{db^*}{d\Delta w} v_{b^*}^H \right\} \\ &\quad + \left(\frac{\gamma}{1 - \lambda} \frac{U - \Delta w}{\Delta w} - 1 \right) p(e^*(1, \Delta w)). \end{aligned} \quad (\text{C4.6})$$

Substituting for $dV^H/d\Delta w$ in Equation (C4.4) implies that

$$\begin{aligned} &\left(\frac{\gamma}{1 - \gamma} \frac{U - \Delta w}{\Delta w} - 1 \right) [(1 - z)E_b p(e^*(b, \Delta w)) + z p(e^*(1, \Delta w))] \\ &+ (1 - z) \frac{db^*}{d\Delta w} V_{b^*}^H = 0. \end{aligned} \quad (\text{C4.7})$$

This implies that $(\frac{\gamma}{1 - \gamma} \frac{U - \Delta w}{\Delta w} - 1) > 0$, since $V_{b^*}^H = [V^H(b^*) - V^H(1)]g(b^*) < 0$ for $z > 0$, as indicated in Observation 4.3. Combining Equations (C4.6) and (C4.7) yields

$$\frac{d\Delta w}{dz} \stackrel{s}{=} \frac{(1 + 2z)}{1 - z} \left(\frac{\gamma}{1 - \gamma} \frac{U - \Delta w}{\Delta w} - 1 \right) p(e^*(1, \Delta w)) > 0. \quad (\text{C4.8})$$

The proof for the employee-owned firm is established using the same argument. ■

References

- Aghion, Philippe, and Jean Tirole. 1997. "Formal and Real Authority in Organizations," 105 *Journal of Political Economy* 1–29.
- Antle, Rick, and Joel Demski. 1991. "Contracting Frictions Regulation, and the Structure of CPA Firms." *Journal of Accounting Research Supplement* 1–24.
- Anton, J. J., and D. A. Yao. 1995. "Start-ups, Spinoffs, and Internal Projects," 11 *Journal of Law, Economics, & Organization* 362–378.
- Brickley, Smith, and Zimmerman. 1996. *Organizational Architecture*. Irwin.
- Carlsson, Bo, David B. Audretsch, and Zoltan J. Acs. 1994. "Flexible Technology and Plant Size: U.S. Manufacturing and Metal Working Industries," 12 *International Journal of Industrial Organization* 359–372.
- Chang, Myong-Hun. 1993. "Flexible Manufacturing, Uncertain Consumer Tastes, and Strategic Entry Deterrence," 41 *Journal of Industrial Economics* 77–90.
- Datar, Srikant M., Gerald A. Feltham, and John S. Hughes. 1991. "The Role Of Audits and Audit Quality In Valuing New Issues," 14 *Journal of Accounting and Economics* 3–49.
- Doty, James R., and David N. Powers. 1988. "Chinese Walls: The Transformation of a Good Business Practice," 26 *American Criminal Law Review* 156–179.
- Eaton, B. Curtis, and Nicolas Schmitt. 1994. "Flexible Manufacturing and Market Structure," 84 *American Economic Review* 875–888.
- Fischer, Thomas G., William H. Gram, George G. Kaufman, and Larry R. Mote. 1984. "The Securities Activities of Commercial Banks: A Legal and Economic Analysis," 51 *Tennessee Law Review* 467–518.
- Holmström, Bengt, and Paul Milgrom. 1991. "Multitask Principal-Agent Analyses: Incentive Contracts, Asset Ownership, and Job Design," 7 *Journal of Law, Economics and Organization* 24–52.
- Hughes, John S., and Jennifer Kao. 1996. "Vertical Integration and Information Transfers: The AT&T Case," working paper, Duke University.
- Kelly, Edward J., III. 1985. "Conflicts of Interest: A Legal View," In Ingo Walter, ed., *Deregulating Wall Street: Commercial Bank Penetration of the Corporate Securities Market*. New York: John Wiley & Sons, pp. 231–254.
- Laffont, and Tirole. 1991. "The Politics of Government Decision Making: A Theory of Regulatory Capture," 106 *Quarterly Journal of Economics* 1089–1127.
- Lewis, Tracy R., and David E. M. Sappington. 1989a. "Countervailing Incentives in Agency Problems," 49 *Journal of Economic Theory* 294–313.
- Lewis, Tracy R., and David E. M. Sappington. 1989b. "Inflexible Rules in Incentive Problems," 79 *American Economic Review* 69–84.
- Martimort, David. 1996. "Exclusive Dealing, Common Agency, and Multiprincipals Incentive Theory," 27 *RAND Journal of Economics* 1–31.
- McVea, Harry. 1993. *Financial Conglomerates and the Chinese Wall*. Oxford: Clarendon Press.
- Milgrom, Paul R. 1988. "Employment Contracts, Influence Activities, and Efficient Organization Design," 96 *Journal of Political Economy* 42–60.
- O'Keefe, Terrence B., Dan A. Simunic, and Michael T. Stein. 1994. "The Production of Audit Services: Evidence from a Major Public Accounting Firm," 32 *Journal of Accounting Research* 241–261.
- Polinski, M., and Shavell, S. 1993. "Should Employees be Subject to Fines and Imprisonment Given the Existence of Corporate Liability?" 13 *International Journal of Law and Economics* 239–257.
- Rotemberg, Julia J., and Garth Saloner. 1994. "Benefits of Narrow Business Strategies," 84 *American Economic Review* 1330–1349.
- Sandler, Todd, and John T. Tschirhart. 1980. "The Economic Theory of Clubs: An Evaluative Survey," 18 *Journal of Economic Literature* 1481–1521.
- Saunders, Anthony. 1985. "Conflicts of Interest: An Economic View," in Ingo Walter, ed., *Deregulating Wall Street: Commercial Bank Penetration of the Corporate Securities Market*. John Wiley & Sons, pp. 207–230.
- Saxenian, Anna Lee. 1994. *Regional Advantage: Culture and Competition in Silicon Valley and Route 128*. Cambridge: Harvard University Press.

- Scotchmer, Suzanne. 1985. "Profit-Maximizing Clubs," 27 *Journal of Public Economics* 24–45.
- Simunic, Dan A., and Michael T. Stein. 1990. "Audit Risk in a Client Portfolio Context," 6 *Contemporary Accounting Research* 329–360.
- Stein, Michael T., and Dan A. 1994. Simunic and Terrence B. O'Keefe. "Industry Differences in the Production Of Audit Services," 13 (suppl) *Auditing: A Journal of Practice and Theory* 128–142.
- Soare, Lorie. 1988. "The Big Eight Management Consulting and Independence: Myth or Reality," 61 *Southern California Law Review* 1511–1553.
- Stewart, Thomas A. 1997. *Intellectual Capital: The New Wealth of Organizations*. New York: Doubleday/Currency.
- Stole, L., 1990. "Mechanism Design Under Common Agency," mimeo, MIT.