The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare.

Anindya Ghose
Leonard Stern School of Business,
New York University

Uday Rajan
Ross School of Business,
University of Michigan

Submitted to Workshop on Economics of Information Security 2006

March 2006

Abstract

The Sarbanes-Oxley legislation is a mandate that is bringing new attention to IT security as a critical part of the risk management framework for the dual purposes of certifying internal controls and attesting to the accuracy of information. Regulatory compliance, security audits and mandatory information disclosure about internal weaknesses can be very costly from a budget standpoint because internal resources need to be allocated away from critical functions such as innovation and product development into increased investments in technologies that facilitate compliance. We propose a theoretical framework towards analyzing the economic impact of government mandated information disclosure and internal audits on firms' investments in IT security, the optimal levels of industry wide production and the extent of market competition. Our analysis reveals that mandatory investments in regulatory compliance may have several unintended consequences such as reduction in optimal production quantities, decrease in the extent of market competition and an overall reduction in social welfare due to distortions in IT security and internal control investments. In particular, our results highlight that smaller sized firms are more severely affected than larger firms and this process may lead to a severe long term impact on the operations of both capital as well as product markets. Our results are in accordance with recent anecdotal and empirical evidence.

1 Introduction

Today's new era of corporate governance requires higher levels of information disclosure and data integrity due to regulations such as the Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBP) and the Health Insurance Portability and Accountability Act (HIPAA). Each of these laws imposes strict requirements on enterprises to establish or identify, document, test, and monitor "internal control" processes (Schneier 2004). In particular, the SOX Act was formulated to increase companies' compliance with Securities and Exchange Commission (SEC) disclosure laws. In the aftermath of Enron, World Com, Tyco and other high-profile business scandals between December 2001 and June 2002, Congress reacted rapidly to introduce the SOX Act (SOA). What prompted lawmakers to create this provision was the concern that there was a lack of sufficient controls at these scandal-ridden firms. In particular, the SOX Act introduced significant changes to financial practice and corporate governance regulation, including stringent new rules designed to protect investors by improving the accuracy and reliability of corporate disclosures.

Perhaps the part of the Act having the most impact was Section 404. Section 404 requires management to submit to the SEC with the company's annually filed financial statements, an internal control report, which shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. It should also contain an assessment, as of the end of the fiscal year, of the effectiveness of the internal control structure. Such reports should include a description of material weaknesses in such internal controls and financial systems infrastructure.[1] Such information disclosure about internal weaknesses can have serious adverse consequences for firms (described subsequently).

The tenets of SOX specify that corporate governance be responsible for providing transparency, integrity, and accountability over regulated financial data by providing an internal control report in its annual report. Hence, from the perspective of IT security, such govern-

[1] A material weakness is a significant deficiency arising from the lack of adequate internal control infrastructure.

ment mandated regulations create an utmost need for additional information security and technology planning to be successfully screened in information security audits.

One of the most important elements of SOX compliance is providing evidence that the financial applications and supporting systems and services are adequately secured to ensure that financial reports can be trusted. Hence, from an IT security perspective, internal controls cover an enormous range of methods and procedures that an organization employs to ensure it is using resources as intended, preventing fraud, protecting assets from damage and so on. Among those methods and procedures are IT security techniques to thwart hackers, and viruses that might abuse the organization's IT infrastructure. Evidence of slipshod behavior could include a history of Trojan break-ins that caused leakage of high-profile company trade secrets, or a spate of incidents in which hackers hijacked company servers to launch distributed denial of service attacks, or even failure to hire competent IT security staff or to provide resources commensurate with the challenges of safeguarding the company's infrastructure.

Thus, regulatory compliance and information disclosure about internal weaknesses can be very costly from a resource standpoint because internal resources need to be allocated away from regular investments such as innovation and R & D to IT security investments in order to facilitate compliance and eliminate weaknesses that may be revealed during internal audits. This places a special burden on firms, and especially on CEOs (Chief Executive Officer) and CISOs (Chief Information Security Officer). They need to understand which systems, services and processes need to be controlled, which aspects of information security are most critical to compliance and how they should allocate resources between regular investments in innovation, product development or R&D, and investments in security technologies that promote internal control.

Prior to Section 404, the audit evaluation of internal control was optional and might have been avoided, for example, for efficiency or size reasons. There was no requirement to disclose publicly the findings from the internal control evaluation. Post-SOX these disclosures are *mandatory.* Recently, a number of trade press articles have voiced for a rollback of portions of the SOA, citing Section 404 as imprudent act of overregulation and called for its repeal. This main goal of this paper is to build a theoretical framework that lays out some consequences to firms that have resulted from the mandatory information disclosure and internal/security audits, and its potential implications on firm profitability, investments in IT security and social welfare.

1.1 Perceived Costs & Benefits

In order to understand the effect of such information disclosure and compliance regulations, it can be useful to get a deeper understanding of the benefits and costs of such laws. Compliance with SOX regulations requires significant, non-recurring costs "upfront" investment. Costs are quantifiable and immediate, whereas benefits are intangible and more difficult to quantify. First, there is a strong learning curve for all registrants and auditors. Audit committees need to spend more time in compliance activities. Then, there are significant fixed costs such as initial documentation, initial remediation of deficiencies (potential deferred maintenance), training efforts, developing overall project and testing plans. None of these processes are stationary though. This implies that the current documentation may change next year as business processes and business controls change from year to year. A company must test each of its controls each year. Intangible costs include delays in decision making due to increase in risk averseness of the top management. And, most importantly, given fixed budget constraints, these mandatory investments in SOX compliance technologies and systems can potentially lead to compromises in the level of IT security spending.

A survey of 224 public companies by Financial Executive International (FEI) in July 2004, found that the average cost of complying with Section 404 is approximately $4 million, and that the average cost varies with firm size. According to a report by the Big Four Accounting firms, the average cost of compliance with Section 404 in 2004 for a fortune 1000 company is $7.8 million. A study by the law firm of Foley and Lardner found the Act increased costs associated with being a publicly held company by 130 percent. Many of the major problems stem from section 404 of SOX, which requires CEOs to certify the accuracy of financial statements.

In addition to the direct cost of implementing a system that achieves compliance with SOX, the workload and risk of directors has increased as a result of the regulation. This, in turn, has lead to an increase in the fees paid to directors. Further, the increase is disproportionately high on small firms. Linck, Netter, and Yang (2005) estimate that, from 2001 to 2004, small firms had to pay higher director fees to the tune of \$0.84 per \$1,000 in net sales, whereas for large firms the corresponding increase was just \$0.07.

While the implementation costs of Section 404 are quite significant, the benefits might be harder to estimate. Specifically, its not quite clear if announcements of material weaknesses by companies are informative to equity investors, creditors and regulatory agencies. Indeed, anecdotal evidence in this regard is quite mixed: A Goldman Sachs study found that 12 % negative stock price reaction to a disclosure of internal control deficiencies by a small-cap firm (Flowserve) but a positive reaction to a disclosure by Eastman Kodak of a forthcoming adverse SOX 404 opinion. The Wall Street Journal (April 14, 2005) reported that the credit rating agency take negative action against about 20% of companies reporting a material weakness.

To be fair, SOA can have a number of expected benefits. First, it could lead to greater accountability, ownership and appreciation of internal control systems throughout all levels of an organization. Second, it can lead to more timely identification and remediation of internal control weaknesses that might not have been detected otherwise. Thus, the benefits of improved corporate controls are expected to be found not only in decreased malfeasance, but perhaps even more so in a substantial increase in corporate data quality, the decrease of instances of erroneous intra- and extra-corporate transactions.

The above discussion then highlights that there are distinct trade offs involved in such mandatory accounting information disclosure regulations. This paves the way for a set of research questions which might of interest to academics and executives alike. Some of these are outlined below.

2 Research Questions

1. What is the impact of mandatory information disclosure about internal controls on the optimal level of investments in IT security? What are the optimal levels of investment in technologies that increase regulatory compliance and information assurance? How should a firm allocate its finite resources between IT security spending that ensure protection of its critical infrastructure and regular investments that promote product development and innovation?

2. Can information disclosure on internal controls impede market competition? What are the optimal levels of information about material weaknesses that should be disclosed? What is the impact of mandatory information disclosure on social welfare?

2.1 Prior Literature

Questions on information disclosure, economic incentives, and social welfare, similar to those noted above, have been previously studied in the context of other organizations. This earlier work is able to shed light on building appropriate theoretical frameworks to answer these questions. Of particular relevance, in this regard, is the extensive literature in conflicts where researchers have studied the optimal allocation of scarce resources by firms, given resource constraints (see for example, Hirshleifer 1989, Hausken 2005). An additional stream of literature in accounting has analyzed the trade-offs faced by firms in disclosing and presenting financial information (Hirshleifer and Teo 2003). Earlier work in finance has tried to establish a link between financial reporting and economic consequences (Demski and Feltham 1994, Fischer and Verrecchia 1999). For a good review of the empirical disclosure literature, see Healy and Palepu 2001, and Core 2001). In the past, disclosure in an accounting context has been deemed to very different from that in software vulnerability disclosure. However, the enactment of recent regulations such as the SOX Act have brought forth several interesting developments leading to direct relationship between accounting information disclosure and information security.

The kind of questions asked in this article can build on the recent literature on security information disclosure and sharing, that analyzes the cost and benefits from enrolling in Information Sharing and Analysis Centers (ISACs). Recent papers dealing with the economics of information security and protection of critical infrastructure include Anderson (2001) who discusses various distorted incentives in the information security domain implied by the existence of moral hazard and adverse selection problems. An emerging stream of literature in the economics of information security has also studies issues related to disclosure of security breaches and vulnerabilities. Firms that participate in ISACs are required to reveal information about security breaches and vulnerabilities to a central monitoring organization(Gordon, Loeb and Lucyshyn 2003, Ghose and Gal-Or 2004) and have different incentives for doing so (Ghose and Gal-Or 2005). Arora et al. (2004) provides a decision framework for understanding how disclosure timing may affect vendors decision and in turn, what policy maker should do. Camp and Wolfram (2000) describe a means for creating a market for vulnerabilities in order to increase the security of systems. Cavusoglu et. al. (2005) study what the optimal disclosure policies should be when vulnerability affects multiple vendors and shed light on social welfare implications of an early warning system which provide vulnerability information to some selected users.

3 Model

In the benchmark model, we analyze a market consisting of two firms producing a differentiated product in a two-stage non-cooperative Cournot game (Tirole 1992). In the first stage, firms choose optimal levels of security technology investments such as those which promote information assurance, and internal compliance. The rest of the resources from the budget are plugged back into regular product development investments. In the second stage, they could choose quantities. We consider a subgame perfect equilibrium of this game using backward induction. The demand of each firm depends on its own price and the price of its competitor. In this context, we can examine how the effect of information disclosure on profits and social welfare, is affected by firm and market characteristics. The demand functions for firms 1 and 2 are assumed to be linear in self and cross-price effects. Recent work in the economics of IT security has used similar frameworks to analyze the effect of security information sharing decisions (Gal-Or and Ghose 2005).

Each firm i chooses its own price p_i and its own investment in product development, r_i. Firm i faces a capital constraint, modelled as follows. Suppose firm i spends s_i on "compliance" technologies. These may be interpreted as technologies that increase internal corporate control by providing management with better reports about the details of the firm. Then, firm i can raise a total of $k(s_i)$ from the capital markets, where $k' > 0$, $k'' < 0$, and $k'(s) \to \infty$ as $s \to 0$ from above. The function k represents an unmodeled friction in the capital markets to allow a departure from the Miller–Modigliani (1961) theorem. The friction itself may be bankruptcy or agency costs faced by the firm. Given the structure of the k function, even in isolation firm i will spend a positive amount on compliance. From this point onwards, we will continue to designate the firm under consideration as firm i and its competitor as firm j. As well, in describing the behavior of both firms in terms of a system of equations, we will drop the qualification, $i, j = 1, 2; i \neq j$ for brevity.

Each firm has a resource constraint R, where R is some function of investments in product development, r and the investments in information assurance technologies that boost internal compliance given by s: $R = f\ (r,\ s)$. So one trade-off firms face is that if r increases, s will have to decrease and viceversa. However, an increase in s also reduces the cost of capital, which in turn can facilitate increased investments in r. So there are two countervailing effects of the increase in r on s.

We model the constraint on funds for total investments, which can be written as

$$R = r_i + s_i \quad = \quad k(q_i, s_i), \tag{1}$$

where k is increasing and strictly concave in both arguments, and the cross partial derivative is strictly positive (so $\frac{\partial^2 k}{\partial q_i \partial s_i} > 0$). In addition, $k(0,\cdot) = k(\cdot,0) = 0$, with k satisfying an Inada condition in both q and k at 0. An example of a function that fills these criteria is

$$k(q_i, s_i) \quad = \quad A q_i^{\alpha} s_i^{\beta}, \tag{2}$$

where A, α, β are all strictly positive.

We assume a linear inverse demand curve,

$$p_i \quad = \quad a_i(r_i, r_j) - b_i q_i + b_j q_j, \tag{3}$$

where $b_1 > b_2$ so that own price effects are greater than cross-price effects. Here the slope b_1 is the elasticity of demand and can be interpreted as the extent to which consumers are price sensitive or "disloyal" to a firm's product. The variable a_i in (1) is the initial intercept of demand facing i. This intercept may shift upward due to the firms' investments in improving information security.

Then, assuming that firms face a linear demand, the optimization problem of a firm can be written as

$$\max_{p_i, s_i} \ \pi_i(p_i, s_i; p_j, s_j) \quad = \quad (p_i - c_i)\,[a_i(r_i, r_j) - b_i p_i + b_j p_j] - (f + {s_i}^2). \tag{4}$$

where c_i is a constant marginal cost of production. Here b_1 and b_2 are the own and cross-price effects. Each of these effects are symmetric, in the sense that firm 1 has the same effect on firm 2 that firm 2 has on firm 1.

The demand intercept a_i facing each firm may shift due to the investments undertaken by both firms. When a given firm increases its investment in innovation and product development, and consumers become informed of this increase, their level of anxiety about transacting with the firm declines, thus enhancing their expected utility and willingness to pay for the product. In contrast, if the competitor increases its level of investment and consumers become aware of it, the firm may experience a negative demand shock and lose some customers(for example, the switchers) since the competitor may now be considered the more reliable and a "higher quality" source of supply. We summarize this net effect of the firms' investments on the demand intercept of firm i in terms of the difference $(r_i - \alpha r_j)$, where $0 \leq \alpha < 1$. Once again, since α is a fraction, own effects of investment exceed cross effects. Hence, the inverse demand curve can be written as

$$p_i = a_i(r_i - \alpha r_j) - b_i q_i + b_j q_j. \tag{5}$$

On the cost side, each firm incurs a fixed cost and a variable cost as a function of its investment in compliance activities. The variable cost component increases at a non-decreasing rate, i.e. it is a convex cost function with $s' > 0$ and $s'' > 0$. For analytical tractability, we use a quadratic cost function. Let this cost be denoted by $F = f + s^2$. Let the marginal cost of production of each firm be denoted by c_i. The profit function of firm i is then

$$\pi_i(q_i, s_i; q_j, s_j) = (a_i(r_i - \alpha r_j) - b_i q_i + b_j q_j - c_i)\ q_i - (f + {s_i}^2). \tag{6}$$

4 Analysis

4.1 Absence of Government Regulation

In the absence of a regulation requiring a minimal level of compliance, the problem faced by firm i can then be written as follows:

$$\begin{aligned} & \max_{q_i, s_i}\ \pi_i(q_i, s_i; q_j, s_j) = (a_i(r_i - \alpha r_j) - b_i q_i + b_j q_j - c_i)\ q_i - (f + {s_i}^2) && (7) \\ \text{subject to :} \quad & r_i = k(q_i, s_i) - s_i. && (8) \end{aligned}$$

The corresponding first order conditions are:

$$\begin{aligned} \frac{\partial \pi_i}{\partial q_i} = 0 &\implies a_i(r_i - \alpha r_j) - 2b_i q_i + b_j q_j - c_i + q_i \frac{\partial a_i}{\partial r_i}\frac{\partial k}{\partial q_i} = 0 && (9) \\ \frac{\partial \pi_i}{\partial s_i} = 0 &\implies q_i \frac{\partial a_i}{\partial r_i}\frac{\partial r_i}{\partial s_i} - 2s_i = 0 \end{aligned}$$

Analysis of the above conditions leads to the following result.

Proposition 1 *An increase in firm size leads to an increase in the investment in security and information assurance technologies. Hence, in the absence of any government enforced* *regulation on information disclosure, larger firms invest more in technologies which promote internal control and compliance.*

Next we discuss the two ways in which an act like Sarbanes-Oxley impacts firms.

5 Presence of Government Regulation

According to anecdotal evidence, many firms believe that investing in regulatory compliance technologies is like a double edged sword. Devoting time and money to compliance limits other activities for which those resources could have been used for instance, in critical technology investments and infrastructure protection which boost IT security. Additionally, as companies scrutinize their internal controls and become more conscious of the processes used to make decisions, they may become more risk-averse and slower to seize opportunities (HRO Alert 2005). The pressures of dealing with SOA are forcing most firms to divert their spending away from security, according to a report released by the Internet Security Forum (ISF). ISF surveyed several Fortune 500 firms, and found that a majority of the firms are decreasing their security budgets to ensure SOX compliance.

In order to capture this real world phenomenon, we model the impact of regulation as the presence of a constraint that requires $s_i \geq X(q_i)$, where $X(\cdot)$ is an amount that the firm must spend on internal controls in order to comply with government mandated regulation. We assume that $X' > 0$ and $X'' > 0$ (so X is convex). This leads to the following result:

Proposition 2 *Let (q^*, s^*) be the optimal quantity and the optimal investment in internal control. When $s^* > X(q^*)$, then the government regulation has no effect. When $s^* < X(q^*)$, then regulation forces firms to decrease investments in security technologies s and reduce the optimal quantities q.*

5.1 Impact of Market Reaction

Its well known and often seen that firms that fail to comply with mandated government regulations are not desirable to investors and banks, and thus find it harder to raise low cost funds in capital markets. In this case we model this constraint on funding as a downward shift of A, the constant in the $k(\cdot)$ function. This implies that when the firm spends s for compliance, the amount left over for product development, $k(q, s) - s$, falls.

Proposition 3 *The market reaction to mandated information disclosure about internal controls leads to reduction in the optimal production in the industry q and a reduction in the optimal investment in technologies that promote internal control and compliance, s. Under some circumstances, this can also lead to a reduction in investments in product development and innovation.*

Recall that the amount of capital, k a firm can raise is dependent on both its size (which in our case is the total production quantity, q_i) and its investments in compliance and internal control s_i. While the direct effect of a reduction in investments in security technologies is to increase investments in product development and innovation, the indirect effect of a reduction in s_i, leads to a reduction in r_i through a reduction in R.

It has been reported in the media that SOX regulations create fear among management that they are exposing themselves to second-guessing when making business decisions, raising the hurdle for businesses to make investments. And raising the hurdle rates implies that "some investments that should have been undertaken, that would have been good for society, good for investors, good for shareholders, and good for the economy's growth, wont be undertaken."[2] Moreover, many companies are delaying the implementation of significant IT projects by six to nine months solely because of the documentation and testing requirements of Section 404. Many firms also expect this problem to persist, and predict that they will be able to make major systems changes only in the first half of their fiscal years going forward. As as result, Section 404 requirements seem to be significantly inhibiting business operations and having an impact on the competitiveness of companies.

[2] A Sense of Siege. *MSNBC* (January 7, 2005)

6 Market Competition

Proposition 4 *Mandatory investments in internal control induced by government regulation can lead to a decrease in extent of competition between firms.*

According to several CEOs, SOA does indeed stifle intra-industry competition. While the federal government acknowledges the ways in which SOX raises the costs of doing business, they also feel these costs are more than offset by the benefits of improved accounting practices and greater public trust in the corporate world. A lack of public trust tends to boost a firms cost of capital. Hence, by increasing the level of consumer trust SOA can mitigate concerns on the cost side as well. However, there are hidden dangers. SOA requires top managers to certify the veracity of their financial statements. The additional liabilities imposed on managers can increase agency costs by forcing executives to invest effort in less monitored activities. In the context of todays economy, an attempt by a corporations management to exercise an extra degree of prudence in equipment spending and hiring behavior will, in the end, if practiced widely enough, produce a more risk averse top management. Hence, it may reduce production and innovation throughout the economy.

It is reasonable to hypothesize that business activity will be reduced, to levels well below the economys underlying dynamic potential (were corporate behavior less risk averse). Indeed Cohen et al.(2004) hypothesize and find that there was a significant decline in research and development expenses and capital expenditures made by CEOs after the passage of SOX. Related to the above point, if some companies were to pass their administrative costs of SOX compliance to customers by increasing prices, it might end up making the company less competitive in the marketplace, thereby having negative consequences on social welfare.

7 Social Welfare

Let the inverse demand functions be denoted as $p_i = F_i(q_i, q_j)$. Let $q_1 = q_2 = q^*$ denote the equilibrium quantity determined by the market. Focusing on a symmetric environment, where the government sets $r_1 = r_2 = r$, $s_1 = s_2 = s$ and $F_1(q, q) = F_2(q, q) = F(q, q)$, social welfare can be written as follows :

$$SW = 2\int_0^{q^*} F(q,q)\,dq - 2(f + s^2) = 2\int_0^{q^*} \frac{a-q}{b_1 - b_2}\,dq - 2(f + s^2) \tag{10}$$

Proposition 5 *Mandatory investments in internal control and security induced by government regulation can lead to a decrease in social welfare.*

The SOA was designed to restore investor confidence and prevent the type of corporate malfeasance that has plagued the U.S. capital markets in recent years. While few would argue with the assertion that the SOX regulations have increased corporate transparency and enhanced corporate governance, it has become increasingly clear that these improvements are creating a disproportionately heavy burden on smaller size companies. The costs of complying with mandatory government regulation, however, are borne by all public companies.

According to the AeA, the largest trade association for the high-technology sector, Section 404 has become problematic because the cost burden amounts to a major regressive tax on small business, given that the cost is not directly proportionate to revenue (AeA 2005). For multi-billion dollar companies, the cost may run at approximately 0.05 percent of revenue, but for small companies with revenues below \$20 million, the costs can rapidly approach three percent of revenue. At the micro level, anecdotal evidence reveals that for a large company the cost of Section 404 is approximately \$400 per employee, whereas, for small companies, the cost in many instances approaches \$4,000 per employee. However, external auditors have generally adopted a "one size fits all" approach to Section 404. This means that a small company (in terms of revenue) and a relatively simple organizational structure essentially is being held to the same standard as a large multi-billion dollar company with a very complicated organizational structure. The SEC believed there would be "a direct correlation between the extent of the burden and the size of the reporting company, with the burden increasing commensurate with the size of the company." But the opposite appears to be true.

Thus, it seems to have a major negative impact as well: namely reduction in companies going public with their IPOs and increase in acquisitions. Indeed in 2005, 33% of the 18 withdrawn stock offerings – including IPOs, secondary offerings and convertible-stock deals – were put on hold because the issuers began discussions to be acquired instead (Dealogic 2005). That has increased from 2004, when 18% of the 97 withdrawn deals were due to acquisition discussions, and 2003, when 16% of 67 deals were pulled for that reason. Thus, the backlash from the legislative penalty may be worse than the crime it was intended to prevent. One explanation for the exodus from the public market and increase in acquisitions is to avoid the burden of complying with the SEC regulations. The added time, expense and managerial hassle to small companies may be tipping the decision away from a public offering.

In a number of press releases announcing the decision to deregister a firm's stock, managers typically cite the high costs of reporting as the key motivation for "going dark" as it is quite commonly known. Additionally recent empirical studies (Leuz et al. 2004) have shown that SOX maybe the driving force behind the decision of many companies to deregister or go dark. A major finding in their paper is that smaller firms for which reporting costs may be particularly burdensome, are more likely to take such steps. Thus this anecdotal evidence supports our theoretical prediction that smaller size firms are likely to be hurt more than larger firms. Moreover, if the market views the deregistration decision as conveying additional information about a firm's weak future growth prospects, this can become a vicious cycle where investors pull out their stocks even more quickly. In fact, Leuz et al. (2004) note that shareholders might even turn skeptical, if they start viewing deregistration as a tool for management to hide poor performance to protect themselves from legal liability (especially post SOX).

These trends demonstrate that the SOA may even be altering the operation of capital markets. This may not only affect US firms directly but may also have an impact on the number of foreign investors in US markets. In fact, given these mandatory regulations, many foreign firms may not be willing to enter or stay in the US markets (HRO Alert 2005). Even with the SECs partial exemption of the compliance requirements of foreign companies, some of them may stay away from US markets because of the tougher accounting rules and heightened emphasis on corporate governance. Thus, the SOA throws up interesting implications of this act on the net social welfare generated not just from product markets but also from the interactions with capital markets. Does a decrease in participation in public markets, or an increase in the number of acquisitions adversely affect social welfare? What are the plausible outcomes? Our ongoing research also aims to examine these questions.

8 Conclusion

The SOX legislation is a mandate that is bringing new attention to IT security as a critical part of the risk management framework for the dual purposes of certifying internal controls and attesting to the accuracy of financial information. As organizations evaluate their capabilities to meet SOX compliance requirements, they must ensure that the infrastructure supports secure identity management with controls implemented, such as information assurance and policy-based access controls. Given that most organizations have a finite annual budget that is allocated to all investments, the regulations accruing from the SOX Act have forced companies to undertake a series of dramatic changes in the way they appropriate resources to activities such as IT security and internal control. This can have some broader ramifications on firm profitability, market structure and social welfare, many of which were unintended when policy makers first formulated this Act. This article is an attempt to provide some insights into the trade offs and unintended consequences that would be of interest to academics, industry executives and policy makers alike.

Our analysis reveals that mandatory investments in regulatory compliance may have several unintended consequences such as reduction in optimal production quantities, a decrease in the extent of market competition and an overall reduction in social welfare. In particular, our results highlight that smaller sized firms are more drastically affected than larger firms and this process if unchecked, may lead to a severe long term impact on the operations of both capital as well as product markets. Because small cap firms are an important engine of economic growth and technological innovation, the ripple effects of regulations like the SOA will be felt throughout the economy. One major implication of this is that some changes in regulations need to be enforced sooner than later by the federal government.

In our ongoing research, we will extend this theoretical model to look at the optimal levels of information about material weaknesses that should be disclosed by firms in the presence of legislation through entities like SEC and verification through intermediaries such auditing firms. In order to model this, we will add a third stage between stage 1 and stage 2, i.e., after firms have invested in security and internal control technologies but before they have chosen the quantities.

CEOs and boards of directors now care, more than ever, about software and systems that will help them comply with SOX. Specifically, the tenets of SOA specify that corporate governance be responsible for providing transparency, integrity, and accountability over regulated financial data. Given the high stakes involved it may be appropriate to outsource some of the software systems development to companies that already have the expertise of both the regulation as well as secure coding techniques, and this trend of outsourcing to managed service providers will probably increase over the years. In such situations, it would be important to include regulation compliant security requirements in contracts with vendors and outsourcing partners. What should optimal outsourcing contracts with managed security services providers be when the burden of regulatory compliance still rests on the firm itself? In addition, firms could in principle, also explore the role that application security products could play in reducing time to be compliant with government regulation. We plan to address some of these questions in future research, and hope that it also spurs some more new exciting research along the way.[3]

[3] Proofs of all results are omitted for brevity but will be included in the final version if accepted.

References

[1] AeA 2005. Sarbanes Oxley Section 404: The Section of Unintended Consequences and its Impact on Small Business. Technical Report, February.

[2] Anderson, R. 2001. Why information security is hard : An economic perspective. *Proceedings of 17th Annual Computer Security Applications Conference*, December.

[3] Arora, A., R. Telang and H. Xu. 2004. Optimal Policy for Software Vulnerability Disclosure. The Third Annual Workshop on Economics and Information Security (WEIS04). Minneapolis, MN, May 2004.

[4] Camp, L. and Wolfram, C. 2000. Pricing Security. In Proceedings of the CERT Information Survivability Workshop, Boston, MA October.

[5] Cavusoglu, H., H. Cavusoglu and S. Raghunathan. 2005. Emerging Issues in Responsible Vulnerability Disclosure. The Fourth Annual Workshop on Economics of Information Security (WEIS 2005), Harvard University.

[6] Cohen, D., A. Dey and T. Lys. 2004. The Sarbanes Oxley Act of 2002: Implications for Compensation Structure and Risk-Taking Incentives of CEOs, Working Paper. *(available at ssrn.com)*

[7] Core. 2001. A Review of the Empirical Disclosure Literature: Discussion. *Journal of Accounting and Economics*. 31. 441–456.

[8] Demski, J., and Feltham, G. 1994. Market response to financial reports. Journal of Accounting and Economics 17 3-40.

[9] Evans, J., and S. Sridhar. 2002. Disclosure-Discliplining Mechanisms: Capital Markets, Product Markets, and Shareholder litigation. *The Accounting Review*. 77(3). 595–626.

[10] Fischer, P., and R. Verrecchia. 1999. Public information and heuristic trade. Journal of Accounting and Economics 27 89-124.

[11] Gal-Or, E. and A. Ghose. 2004. The Economic Consequences of Sharing Security Information. Camp and Lewis (Eds), *The Economics of Information Security*, Kluwer, July, 95-104.

[12] Gal-Or, E. and A. Ghose. 2005. The Economic Incentives for Sharing Security Information. *Information Systems Research.* 16(2). 186-208.

[13] Gordon, L. A., M. Loeb, and W. Lucyshyn. 2003. Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy* 22 (6).

[14] Hausken, K. 2005. Production and Conflict Models Versus Rent Seeking Models. *Public Choice* 123, 59-93.

[15] Healy, P. and K. Palepu. 2001. Information Asymmetry, Corporate Disclosure and the Capital markets: A Review of the Empirical Disclosure Literature. 31. *Journal of Accounting and Economics*. 405–440.

[16] Hirshleifer, D. and S. Teoh. 2003. *Journal of Accounting and Economics*. 36. 337–386.

[17] Hirshleifer, J. 1989. Conflict and Rent Seeking success functions. Ratio vs. Difference Models of Relative Success. *Public Choice*. 63. 101–112.

[18] HRO Alert. 2005. At What Cost? February 7.

[19] Linck, J., J. Netter, and T. Yang. 2005. Effects and Unintended Consequences of the Sarbanes-Oxley Act on Corporate Boards. Working Paper, University of Georgia.

[20] Leuz, C., A. Triantis, and T. Wang. 2004. Why Do Firms Go Dark? Causes and Economic Consequences of Voluntary SEC Deregistrations. Working Paper. University of Pennsylvania.

[21] Schneier, B. 2005 Security and Complaince. IEEE Security and Privacy. July/August.

[22] Tirole, J. 1989. The Theory of Industrial Organization, MIT Press, Cambridge.

[23] Zhang, I., X. 2005. Economic Consequences of the Sarbanes Oxley Act of 2002. Working Paper, University of Rochester.