Information Disclosure and Regulatory Compliance: Economic Issues and Research Directions[1]

Anindya Ghose
Leonard Stern School of Business,
New York University
Tel: (212) 998-0807
E-mail: aghose@stern.nyu.edu

July 2006

[1] I thank Uday Rajan and Martin Loeb for helpful comments.

Abstract

The Sarbanes Oxley Act (SOA) 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. Briefly speaking, it requires management to submit a report containing an assessment of the effectiveness of the internal control structure, a description of material weaknesses in such internal controls and of any material noncompliance. Such mandatory regulations 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. Moreover, the tight coupling between compliance activities, information disclosure and IT investments can have implications for IT governance because of its potential to change relationships between technology investments and business. This article aims to provide some intuitive insights into the trade-offs involved for firms in disclosure of such information, and gives an overview of some research questions that would be of interest to academics, industry executives and policy makers alike.

1. Introduction

The Sarbanes-Oxley (SOX) Act was formulated to increase companies' compliance with SEC disclosure laws. In the aftermath of Enron, World Com, Tyco and other high-profile business scandals between December 2001 and June 2002, Congress rapidly approved the passage of the SOX Act (SOA). What prompted the government to create this provision was a concern stemming from the lack of sufficient controls at these scandal-ridden firms, and the need for firms' financial statements to be accurate and devoid of any kind of accounting manipulation. Thus, the SOX Act required managers to implement controls over the financial reporting process and state whether they were effective.

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 made pursuant to the securities laws. 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 and procedures for financial reporting. It also requires auditors to attest to, and report on the management's assessment of the internal control systems. Such reports should include a description of material weaknesses in such internal controls and of any material noncompliance. Furthermore, where significant deficiencies exist, they need to be identified as required under SOX. For an interesting study that examined the cause of significant deficiencies in internal control that required identification, see Ge and McVay (2005). They found that poor internal control is related to "an insufficient commitment of resources for accounting controls". An example of a statement contained within the internal control report provided by corporations is provided below.

- An evaluation of the effectiveness ….disclosure controls and procedures…was performed… ..with the participation of the Company's Management, … these …are effective to provide reasonable assurance that information required to be disclosed by the Company ..is accumulated and communicated to the Company's Management …to allow timely decisions regarding required disclosure and …to provide reasonable assurance that such information is recorded, processed, summarized and reported within the time periods.
  - *Wal-Mart Stores Inc- March 31, 2005*[2]

Since modern financial reporting systems are heavily dependant on technology and associated

[2] This example was taken from the study by Gordon et al. (2006).

controls, any review of internal controls would not be complete without addressing controls around information security. An insecure system would not be considered a source of reliable financial information because of the possibility of unauthorized transactions or data manipulation, each of which can compromise data integrity. The SOX Act focuses on management accountability and operating efficiencies in firms. Both of these are tightly coupled with investments in IT and the role played by IT professionals. Indeed, sections 302 and 404 indirectly force the scrutiny of information security controls for SOX compliance.[3] The implication of these new regulations is that organizations, especially those dealing with financial information, must establish the appropriate processes and technologies to evaluate data usage requirements for all users and create a data usage control policy that defines how data may be used by each user. They need to record database activity and report on deviations from the data usage control policy. Further, they need to alert management when a deviation from usage control policy might violate data integrity.

There's been a lot of debate about the impact of new government and industry regulations on IT departments, especially in the financial services sector. The financial services sector has long been presumed to practice superior information security, largely because of the preciousness of its assets and the fact that its business is carried out almost entirely on IT systems. A study based on interviews with 100 IT managers in UK financial services companies reveals that given the current level of investment in technologies that help companies comply with regulations such as SOX, around 60% of IT managers from financial services companies believe the demand on IT to deal with compliance issues will increase over the coming three years (Carr 2006). Indeed, the study states that most respondents are not satisfied with their current capabilities to perform tasks necessary for compliance such as document management and archiving. Further, it also reports that "most financial companies are only just beginning to scratch the surface in areas such as the archiving of electronic messages and digitized phone records." This becomes even more important in the face of a recent study that shows how susceptible the financial services industry is to targeted scans and probing attacks (Schneier 2005). Counterpane tracked the thirteen major vertical markets using attack data between January 2005 and October 2005. The study found although the financial industry ranks second highest in attacks, it is actually the most vulnerable to security breach activity—approximately 50% of all targeted scans detected by Counterpane occurred within the financial industry.

It's well known that internal control evaluation and responsibilities are not a new mandate on business in the US. For instance, the US Foreign Corrupt Practices Act of 1977 requires publicly held companies to maintain adequate system of internal control. Further, the evaluation by external auditors has been an integral part of firm audit for many years. However, prior to Section 404, the

[3]For a good survey of how the SOX Act is related to IT Governance, see Damianides 2005.

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 article have voiced for a rollback of portions of the SOX Act, citing Section 404 as imprudent act of overregulation and called for its repeal. This article lays out some potential trade-offs to companies that have resulted from the SOX Act and its implications on firm profits, industry structure and competition, and social welfare.

1.1 Perceived Costs & Benefits

SOX has made companies place more emphasis on the reliability, security and accuracy of their systems. Companies need to understand how their back office systems support financial data processing - and show that they have the right IT governance in place. 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 is 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, SOX Act 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 information 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. ***Sarbanes-Oxley requirements are causing companies to reconsider public status. Is that detrimental for social welfare?***

The SOX Act 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 small public companies. The costs of complying with the SOX Act, however, are borne by all public companies. 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 SOX Act regulations. The added time, expense and managerial hassle to small companies may be tipping the decision away from a public offering.[4]

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 (Lieuz et al. 2004) have shown that the SOX Act maybe the driving force behind the decision of many companies to go 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. 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, Lieuz 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 SOX Act 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 SEC's 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 SOX Act 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 decreases in participation in public markets, or an increase in the number of acquisitions adversely affect welfare? What are the plausible outcomes? The jury is still out on these questions.

2. ***By creating an artificial incentive for firms to merge, is the law impeding market competition?***

According to several CEOs, the SOX Act does stifle intra-industry competition. According to the

[4]One could also argue that SOX could have a negative influence on corporate mergers and acquisitions because acquiring firms may be wary of the financial liability they could assume for the private companies they acquire. Anecdotal or empirical evidence to support this assertion is little or non-existent, though.

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.

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 firm's cost of capital. Hence, by increasing the level of consumer trust SOX Act can mitigate concerns on the cost side as well. However, there are hidden dangers. SOX Act 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 today's economy, an attempt by a firm's 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, not necessarily to recession levels, but to levels well below the economy's 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 the SOX Act. 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.

3. ***Can Sarbanes-Oxley compliance compromise IT security? Given the resource constraints a firm faces, what are the optimal levels of investment in technologies which boost SOX compliance? How should a firm allocate resources between IT security spending, SOX compliance spending and other regular expenditures such as product development/R & D/marketing?***

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 SOX Act specify that corporate governance be responsible for providing transparency, integrity, and accountability over regulated financial data. As with most laws of this type, regulatory compliance only establishes a base line and is just a start to ethical corporate governance and financial conduct. Also, given the high stakes involved firms are also considering outsourcing some of the software systems development to companies that already have the expertise in secure coding techniques. In addition, firms could in principle, also explore the role that application security products could play in reducing time to be compliant.

However, investing in compliance technologies is like a double edged sword. Devoting time and money to SOX Act 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 (more on this later). 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 the SOX Act 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. A recent report by Red Siren (2005) which surveyed Chief Security Officers (CSOs) mentions similar findings. 62% of the participants said they are having to spend more time complying with government regulations such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act, and less time on activities actually protecting their networks. More than one-third ([38%) of the respondents said such mandatory regulations have caused them to either divert or delay new IT security projects. Getronics (2005) reports a similar finding by Gartner Research analysts.

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, won't be undertaken."[5] 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 a result, Section 404 requirements seem to be significantly

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

inhibiting business operations and having an impact on the competitiveness of companies.

4. How does compliance affect the security of critical infrastructure assets?

Certain industries are very critical to our nationwide security because of their intimate connection to critical infrastructure assets. According to the DHS (Department of Homeland Security), critical infrastructure includes "cyber assets both technology-based, physical and logical which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic of US citizens." The financial services industry, which is privy to the sensitive information about consumers is also most susceptible to cyber-security breaches. Given the increasing pervasiveness of storing data in digital form and the importance of confidential personal information, a major breach of client data could not only impact a financial services organization's financial performance, but also severely cripple the security of critical infrastructure industries. Publicly traded financial services organizations need to keep extensive records and documentation of internal controls to comply with the SOX Act. A security breach in a critical infrastructure industry, such as banking, may adversely affect producers and consumers in other industries. The shift in management attention from protecting critical cyber-infrastructure to investing in compliance and internal control may derail other IT projects (Agostino 2004) and impinge on the overall security of the industry. The resultant ripple effects can have grave consequences on national security. The management has to have a careful understanding of how to allot resources to different business units in order to balance the various investments.

Related to this is the question of "externalities" which arise when cost and benefits of investments are harder to quantify. This is certainly true of information security investments. For example, while a significant terrorist attack undermines the nation's sovereignty, the costs associated with such an attack may be difficult to quantify. In economics, such an attack is defined as imposing a "negative externality." The presence of this negative externality means that private markets will under investment in security than the socially optimal level. This is because firms deciding how best to protect themselves against terrorism are unlikely to take the external costs of an attack fully into account, and therefore will generally provide an inefficiently low level of security against terrorism on their own (Orzag 2003). Without government involvement, private markets will thus typically under-invest in anti-terrorism measure. In such contexts information sharing may act as a panacea; Gal-Or and Ghose (2005) find that security technology investments and security information sharing act as "strategic complements" in equilibrium. On the other hand, information sharing can also lead to a free-riding problem (Gordon, Loeb and Lucyshyn 2003).

5. How does mandatory information disclosure affect a firm's intellectual property?

SOX can have a major impact on the importance and management of intangible assets such as intellectual property (IP). In fact, among SOX's accounting mandates are specific requirements on companies to report on the value of their IP and to annually audit their IP. Given the intricate interplay between intellectual property and SOX, companies are beginning to appreciate the role of intellectual property in financial performance. Under SOX, firms need to be diligent in disclosing and certifying their tangible and intangible assets in all financial reports. They must identify and list their important IP assets, value them, link those assets to the financial performance and operation of the company, and disclose any impairment to them (Foley and Lardner 2005). IP assets are to be audited annually to determine if there has been any impairment or loss that needs to be accounted for. Patent and trademark portfolios, for example, need to be decomposed and allocated to associated cost and revenue streams. This implies tracking changes in the legal landscape, such as potential claims of intellectual property infringement, changes in competitor intellectual property portfolios, amendments to the scope of patent or trademark applications or patent and trademark validity challenges, and changes in intellectual property law (Blair 2005).

Given these scenarios, measurements undertaken to safeguard IP are part of the controls that must be certified by a company under SOX regulations. In many firms, this is bringing forth a need to formalize and update their IP management processes to better track the IP along with other assets. Rather than having the legal team bear sole responsibility, multidisciplinary teams are being created to review and assess the company's IP-related contracts, including non-disclosure, employment and licensing agreements.[6]

Several questions can arise in this context. For example, how do intellectual property infringers affect the financial prospects of a firm? Or for a given level of information disclosure and investments in compliance, what is the potential for infringement damages and how may that impair current and future intellectual property? What are the potential liabilities if a firm has inadequate controls in place and more importantly, how does one measure such IP related liabilities and reflect the losses in the mandatory periodic reports? Moreover, what are the specific kinds of information that should be disclosed when disclosure is mandatory? Can these disclosures serve the purpose of alerting auditors, managers, and investors?[7]

3. Prior Literature

Questions on information disclosure, economic incentives, and social welfare, similar to those noted

[6]Sarbanes-Oxley and Your Company's. IP 4/19/2006. www.jenner.com/news
[7] I think an anonymous reviewer for suggesting this.

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). There is no empirical agreement on whether firms are more likely to disclose good news or bad news. Indeed depending on size, firms use different disclosure strategies if the costs and benefits associated with disclosure and nondisclosure vary with firm size. For example, class action law suits are more probable and more costly for large firms as a result of the method of legal damage estimation (Skinner 1997; Beaver and Marlernee 1990). Based on this observation, Tucker and Zorowin (2006) argue that larger firms are more likely to predisclose bad news. On the other hand, Diamond and Verrecchia (1991) show that the marginal benefit of increased disclosure increases with firm size. The intuition is that increased disclosures are expected to increase market depth and thereby attract large-traders, who are often associated with larger firms. Their theory predicts that irrespective of the kind of news, larger firms are more likely to make disclosures than are smaller firms. For a detailed review of the empirical disclosure literature, see Healy and Palepu (2001), and Core (2001).

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). The U.S. federal government has encouraged the formation of ISACs, with the goal of helping to protect critical infrastructure assets that are largely owned and operated by the private sector. This has been witnessed in variety of industries such as IT, chemicals, oil & gas, electricity, transportation etc. For instance, members of the Financial Services Information Sharing and Analysis Center (FS/ISAC) receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats. ISACs provide “vertical” systems for exchange of sector-specific information and ideas within Critical Infrastructures (CI). Companies that participate in ISACs work with their Sector Coordinating Councils (SCCs) and the Sector-Specific Agencies (SSAs) and are required to reveal information about security breaches and vulnerabilities to a central monitoring organization (Gordon, Loeb and Lucyshyn 2003, Gal-Or and Ghose 2003, Gal-Or and Ghose 2005). The underlying assumption is that such centrally coordinated information sharing organizations would facilitate the alignment of goals for both the private sector and the federal government, which in turn would improve the security of cyber-infrastructure assets (Gal-Or and Ghose 2003).

The interesting parallels can be drawn with compliance regulation because of the underlying nature of internal vulnerability and weakness reporting. Gal-Or and Ghose (2005) show that security information sharing alliances yield greater benefits in more competitive industries. Firms generally respond to increased competition with aggressive price cuts. In order to alleviate such aggressive price competition, firms have greater incentives to invest in mechanisms that alleviate price competition. Since increases in information sharing may help in mitigating price competition, firms decide to raise the extent of information sharing and investments when the degree of competition between them increases. Gal-Or and Ghose (2005) also highlight that the benefits from such information-sharing about internal security breaches and vulnerabilities increase with the size of the firm. Arora et al. (2004) provides a decision framework for understanding how disclosure timing may affect vendor's decision and in turn, what policy makers should do. They show that vendors always choose to patch after disclosure, and that the social planner can optimally shrink the time window of disclosure to push vendors to deliver patch in a timely manner. 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.

On the empirical front, a number of studies have demonstrated the adverse effect of security breach disclosure on the stock market prices of firms and vendors (Campbell et al. 2003, Cavusoglu et al. 2004, Telang and Wattal 2005). The insights from these studies can be used to predict the possible consequences of disclosing internal vulnerability on stock prices. Perhaps the most relevant paper to this article is Gordon et al. (2006) who empirically examine the impact of the Sarbanes-Oxley Act (SOX) of 2002 on the voluntary disclosure of information security activities by corporations and find evidence that clearly indicates that SOX is having a positive impact on such disclosure. Although, an increase in voluntary disclosures of information security activities by corporations does not prove that the activities have actually increased (since activities could remain the same, while the disclosures of such activities have increased), it provides indirect evidence that such activities are receiving more focus since the passage of SOX (Gordon et al. 2006).

4. Economic Modeling of the Problem

Several of these questions are inherently empirical in nature. And some of these empirical studies can be complemented by looking at specific case-studies. On the other hand, analytical models can also be built towards providing many interesting and intuitive insights into these issues. How can one model these phenomena and answer the above questions? It is probably too ambitious to hope that a single model can provide suggestive answers to all of them. Instead we focus on a subset of problems. Let us take an example. Suppose one is interested in issues pointed out in (3). In the simplest possible

formulation, one can analyze a market consisting of two firms producing a differentiated product in a two-stage non-cooperative game as in the standard model of Cournot or Bertrand competition (Tirole 1992). In the first stage, firms choose optimal levels of SOX compliance technology investment and material weakness disclosure levels, such that the rest of the resources from the IT budget are plugged back into IT security investments. In the second stage, they could choose prices or quantities. Firms face a linear demand curve, with the demand of each firm depending on its own price and the price of its competitor. The demand functions for the firms can be assumed to be linear in self and cross-price effects. In this context, we can examine how the effect of information disclosure on profits and social welfare, is affected by firm and market characteristics. 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, Ghose and Rajan 2006, Ghose and Hausken 2006).

The demand function should have two components: a benefit function, *B* and a cost function, *C*. Both the benefit and the cost components should be some function of investments in innovation and investments in SOX compliance. The benefits could be interpreted as increased customer confidence which helps in product markets by boosting demand and decreased cost of capital. On the cost side, there needs to be a fixed component and a variable component which increases with firm size but at a decreasing rate. The framework should also incorporate indirect costs which maps the loss in economic productivity or innovation levels for firms due to diversion of resources from those activities into compliance activities.

Each firm has a resource constraint *C*, where *C* is some function of investments in productivity or innovation, *I* and the investments in SOX compliance X: $C = f(I, X)$. So one trade off the firms face is that if *I* increases, *X* will have to decrease and vice versa. However, an increase in *X* also reduces the cost of capital, which in turn can facilitate increased investments in *I*. So there are two countervailing effects of the increase in *X* on *I*. Additionally, one would need to model a trade off between investments in capital markets and product markets (Evans and Sridhar 2002). Further, it might be important to incorporate a parameter which models the "maturity" of the industry. For instance, the impact of SOX on the bio-tech industry will probably be different than that from a more mature industry such as oil & gas. This parameter will map whether the industry is more prone to IPOs, start-ups, and whether it is more susceptible to acquisitions & mergers.

5. Conclusion

In hopes of restoring investor's faith in corporate America, SOX established significant changes in both management's reporting responsibilities. An unanimous consensus is that regulations such as the SOX, California SB 1386, and the GLB amongst others, are having an enormous impact on

organizations. To meet the aggressive deadlines of these regulations, firms in several industries, including financial services, have invested significantly in consulting, auditors, and new business processes to foster disclosure of material weakness and ensure internal control. A number of recent studies have shown that SOX compliance comes with a high price tag. Companies face both direct (quantifiable) and indirect (non-quantifiable) costs such as increased D&O insurance premiums, higher directors fees as a result of greater time commitments and responsibilities, larger expenses related to internal control software and higher costs relating to consulting fees. An important aspect of these costs is that they are not proportional to the size of the organization. Consequently, smaller firms are being more adversely affected than larger firms.

There is no question that SOX is having a big impact on IT governance. While corporate executives agree that restoring investor confidence is in the best interest of the economy, they disagree on the actual cost and benefits of SOX compliance. The regulations accruing from the SOX Act have forced companies to undertake a series of dramatic changes in the way they appropriate resources to key activities such as IT security. In many firms, critical resources are being diverted away from regular projects to expedite compliance, and several business units are reeling from its impact. Moreover, critics argue that although SOX has raised the level of disclosure, the readjustment of costs affects a company's global competitiveness (Lowengrub 2005). If firms end up passing their compliance costs onto customers by increasing prices, it will make them less competitive in the marketplace, especially with respect to foreign firms that are not subject to SOX. Furthermore, it is plausible that restraints from internal controls reduce the flexibility to respond to customer concerns. Moreover, the tight coupling between compliance activities, information disclosure and IT security, can have implications for IT governance because of its potential to change relationships between technology investments and business. Thus, such mandatory regulations 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.

The aim of this article is not to criticize such regulations. Rather, this article aims to provide some intuitive insights into the trade offs involved for firms and lays the ground for some research questions that would be of interest to academics, industry executives and policy makers alike. It would be interesting to address some of these questions in future research, and we hope that it also spurs some more new exciting research along the way.

References

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

[2] Agostino, D., Perspectives: Early Adopters - If they only knew then what they know now. *CIO Insight*, 2004. 1(39).

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

[4] Beaver, William H. and James K. Malernee. 1990. Estimating damage in securities fraud cases. Cornerstone Research.

[5] Blair, J. 2005. Sarbanes-Oxley and IP Management -Or- What do I gotta tell 'em about my IP assets? from http://www.mcgarrybair.com/viewNewsletter.asp?ID=20

[6] Campbell, K., L.A. Gordon, M. P. Loeb and L. Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security* , Vol. 11, No. 3, 2003

[6] Carr, S. (2006). Are compliance headaches only just beginning? from http://www.silicon.com/research/specialreports/compliance/0,3800003180,39156600,00.htm

[7] Cavusoglu H., Mishra B., and S Raghunathan (2004) 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' *International Journal of Electronic Commerce*, 9(1), 69.

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

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

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

[11] Damianides, M. (2005). Sarbanes–Oxley And IT Governance: New Guidance on IT Control and Compliance. *Information Systems Management*. Winter 77–85.

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

[13] Diamond, Douglas S. and Robert E. Verrecchia. (1991). Disclosure, liquidity, and the cost of capital. *Journal of Finance* 36 (4) (September): 1325-1359.

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

[15] Foley and Lardner. (2005). Intellectual Property Metrics Today: It Can Be Done. Global Intellectual Property: *Asset Management Report.* 7(6). 1–7.

[16] Gal-Or, E., and Ghose, A. (2003). The economic consequences of sharing security information. Proceedings of the *Second Workshop on Economics and Information Security*, May, University of Maryland.

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

[18] Getronics (2005). Security Compliance: Practical Strategies to Alleviate Regulatory Frustration.

[19] Ge, W. and S. McVay. 2005. The Disclosure of Material Weaknesses in Internal Control

after the Sarbanes-Oxley Act. Accounting Horizons 19 (3): 137-158

[20] Ghose, A, and Rajan, U. (2006). The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare. *Proceedings of the Fifth Annual Workshop on Economics and Information Security (WEIS06)*. June, Cambridge, UK.

[21] Ghose, A. and K. Hausken. 2006. Information Sharing among Cyber Attackers Attacking one Firm. Working Paper, New York University.

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

[23] Gordon, L., Loeb, M., and Lucyshyn, W. and T. Sohail (2006). The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. Forthcoming, *Journal of Accounting and Public Policy*, (25: 5), 2006.

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

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

[26] Hirshleifer, D. and Teoh, S. (2003). Limited attention, information disclosure, and financial reporting. *Journal of Accounting and Economics*. 36. 337–386.

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

[28] HRO Alert. (2005). At What Cost? February 7.

[29] 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.

[30] 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.

[31] Lowengrub, P. (2005). The Impact Of Sarbanes Oxley On Companies, Investors, and Financial Markets. from www.s-ox.com/feature/detail.cfm.

[32] Orzag, P. (2003). Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives. www.brookings.org

[33] Redsiren. 2005. 2005 IT Security Management Survey Results. December 21.

[34] Schneier, B. (2005). 2005 Attack Trends: Beyond The Numbers. *A Report by Counterpane Security Systems.*

[35] Skinner, Douglas J. (1997). Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics* 23: 249-282.

[36] Telang, R. and S. Wattal. (2005) Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis. *Proceedings of the Fourth Annual Workshop on Economics and Information Security (WEIS06).* Boston, June.

[37] Tirole, J. (1989). The Theory of Industrial Organization, MIT Press, Cambridge.

[38] Tucker, J. and P. Zarowin. (2006). Timeliness of Firms' Voluntary Disclosure of Good and Bad News. Working Paper.

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