December 2007

The Influence of Regulations on Innovation in Information Security

Lara Khansa
University of Wisconsin, Madison

Divakaran Liginlal
University of Wisconsin

THE INFLUENCE OF REGULATIONS ON INNOVATION IN INFORMATION SECURITY

Lara Khansa and Divakaran Liginlal
Department of Operations and Information Management,
School of Business, University of Wisconsin, Madison
{lzkhansa@wisc.edu; dliginlal@bus.wisc.edu}

Abstract

We postulate that regulatory compliance pressures that have forced information security out of obscurity and into the corporate boardroom provide economic justification for information security firms to innovate. We aim to establish the link between regulations and innovation through the intermediary of demand for information security products and services. First, we show from the results of a pilot study of US firms that regulations do indeed bolster demand for information security products and services. Next, we use time series methods to further confirm these results and to establish a strong correlation between demand and innovation, proxied by R&D expenses. The results show that demand is highly correlated with innovation (correlation of 0.516) and that it significantly increases around the timing of major information security regulations and standards (t-stat of 2.2 at a 95% confidence level). Motivated by these findings, we argue in favor of regulating the IT industry, which includes the information security sector, not through imposing punitive regimes but rather by providing incentives to IT producers, thus stimulating technological, process, and organizational innovations.

Keywords: Regulation, innovation, demand, vulnerability, privacy, information technology.

Introduction

Information security has gained prominence in recent times and has become an integral part of doing business in today's digital world. Three important phenomena provide economic justification for information security firms to innovate. First, organizations have become increasingly vulnerable to newer and more sophisticated methods of malicious attacks, launched with the goal of committing fraud and making illegal profits. Second, the field of information technology has seen radical innovations in telecommunications and computing architectures. Third, regulatory compliance has forced companies to rethink their information strategy and to enforce appropriate safeguards and controls over their IT systems and processes.

Information security and information systems are complementary. Unlike other IT sectors which were initiated by a breakthrough innovation, information security was born out of the need to make vulnerable IT products more secure. This implies that innovation in information security is inherently tied to innovation in information systems. Innovation in information systems, which according to Swanson (1994) encompasses the core technology, administrative, and organizational facets of a business, has been extensively researched. For example, Adner and Levinthal (2001) identified consumer wants as the main driver of IS innovations. They explored how heterogeneous consumer needs influence the product development efforts of firms. This idea of demand-driven innovation conforms to the Schmooklerian school of thought (Schmookler 1966), which advocates that the success of an innovation is intertwined with a strong and growing demand for it. Kim et al. (2006) linked innovation in information systems to the market value of the firm. In particular, they hypothesized that innovations in the context of supply chain can be viewed as firm resources that enhance channel capabilities and improve market performance. Although one may argue that the majority of innovations in information security are demand-driven, this does not preclude technology-push strains in information security innovation. Public Key Cryptography, for example, is a breakthrough innovation that has driven change in technology, which per the Schumpeterian theory (Schumpeter 1934) would lead to demand adjusting automatically to supply. The subtle difference between the technology-push and demand-pull views is that, while a push strategy conjectures that the innovating firm drives market

demand, the pull strategy begins with the consumer who creates demand pressure and defines desirable product attributes. This study examines primarily the demand-pull facets of innovation in information security.

While many researchers have studied different aspects of innovation in information systems, we have not found, in our thorough examination of the literature, any study that clearly and explicitly elucidates the drivers of innovation in information security. In this paper, we fill this gap by focusing on an important driver of information security identified previously, namely regulatory compliance. In particular, we endeavor to first link demand and innovation both conceptually and empirically, showing that they are highly correlated. We then show that regulations have been associated with higher demand and, in turn, indirectly bolster innovation.

The remainder of this paper is organized as follows. Section 2 presents our conceptual framework linking demand, innovation, and regulations and categorizes major information security regulations into five broad categories based on their intent and scope. Section 3 summarizes a pilot study, an empirical study, and a subsequent trend analysis to validate the framework. Finally, in Section 4, we offer additional recommendations concerning the need to regulate the IT industry.

Innovation, demand, and regulations

Regulations may influence innovative activities in two ways. First, they can significantly influence demand and the market structure. Second, in an industry such as IT where standards are very important, public policies serve as a catalyst for developing and enforcing standards. Consequently, policies that influence standardization may have profound effects on the nature and pace of innovation. As evidenced in the conceptual model shown in Figure 1, regulations directly affect the consumers of IT products and services, in turn influencing demand and the market structure, while IT and information security standards are applicable to the firms that produce IT and information security products and services. This producer-consumer paradigm serves as a useful basis to tie regulations to innovation in information security.

Regulatory stimulus and firm response

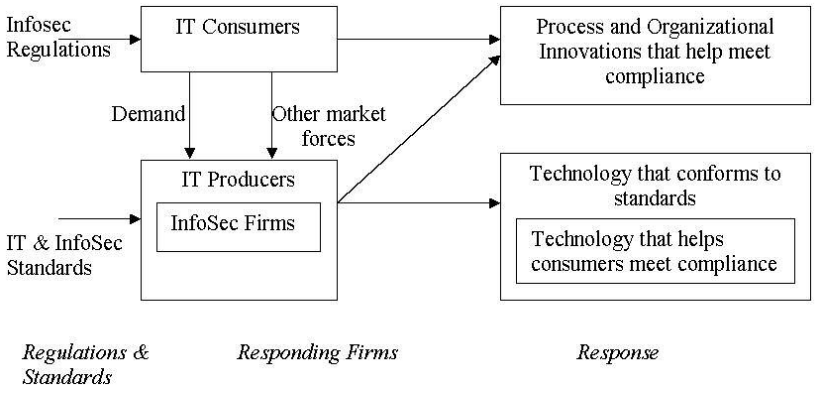

Figure 1. Conceptual model of regulations and their impacts on innovation

The fundamental objective of information security regulations is to ensure that organizations observe due diligence and enforce safeguards and controls on systems and organizational processes in order to protect the confidentiality, integrity, and availability of data. Although technology, process, and organizational innovations are not the intended goals of regulation, they are the primary means by which regulations take effect. In the model shown, security regulations affect consumers of IT products and services directly, while producers of IT (and information security) are affected indirectly through actions by standards bodies and the demand for products and services. We categorize information security regulations and standards based on their intent (corporate governance and privacy legislation) and scope (federal agencies, electronic banking and payment, and sector-wise).

A. Corporate governance

The spate of corporate scandals and mismanagement of corporate finances led to the Sarbanes-Oxley Act (SOX) that affects all public companies (Schultz, 2004). Section 404 of the Act requires management to perform an assessment of internal controls over financial reporting and obtain attestation from external auditors on an annual basis. SOX stimulates all areas of innovation, but particularly emphasizes process and organizational innovations.

B. Privacy legislation: The regulation of the collection, use, and storage of personal information is the fundamental objective of privacy legislation.

a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is targeted at securing patient records and transferring electronic health care information. HIPAA Privacy Rule covers patients' privacy rights and the use and disclosure of protected health information. HIPAA Security Rule requires that administrative, physical, and technical safeguards be instituted to protect data, systems, and processes (http://www.hhs.gov/ocr/hipaa).
b. The Gramm-Leach-Bliley Act (GLBA) requires each financial institution to respect the privacy of its customers and to protect the security and confidentiality of the customers' nonpublic personal information (http://www.ftc.gov/privacy/glbact).
c. The California Information Practice Act or Senate Bill 1386 requires companies that own or have access to personal information of California residents to notify them if their data have been accessed illegally (http://www.privacy.ca.gov). The California Assembly Bill 1950 (AB 1950) further requires that organizations take "reasonable precautions" to protect California residents' personal information from modification, deletion, disclosure, and misuse rather than just report on its disclosure.

Privacy regulations also address all types of innovation with specific emphasis on privacy enhancing technologies and data protection methods.

C. Federal regulations & standards

a. The Federal Information Security Management Act (FISMA) requires federal agencies to develop agency-wide programs to secure data and information systems supporting agency operations and assets, including those managed by other agencies or contractors (http://csrc.nist.gov/policies).
b. The Federal Information Processing Standards (FIPS) requires U.S. federal government agencies to use a cryptographic product that has been FIPS 140 or Common Criteria (CC) validated (http://csrc.nist.gov/cryptval).

D. Guidance and standards for electronic transactions

a. The Federal Financial Institutions Examination Council's (FFIEC) guidance of October 2005 requires that financial institutions and their application service providers (ASPs) deploy security measures to reliably authenticate their customers' high-risk online banking transactions through using multifactor authentication, layered security, and other reasonable controls (http://www.ffiec.gov/pdf/authentication_guidance.pdf).
b. The Payment Card Industry (PCI) data security standard requires organizations that handle bank cards to conform to security standards for protecting access to data in storage and in transit and updating and testing systems regularly among others (http://www.pcisecuritystandards.org).

E. Sector-wise standards and regulations

a. Title 21 of the Federal Regulations Part 11 (21 CFR Part 11), which outlines the US Food and Drug Administration's (FDA) requirements for electronic records and electronic signatures for the

pharmaceutical industry, requires organizations to ensure authenticity, integrity, confidentiality, and non-repudiation of electronic records (http://www.fda.gov/ora/compliance_ref/part11/).

b. The North American Electric Reliability Council (NERC) cyber security standards aim at protecting the critical cyber assets essential to the reliability of the national power grid (http://www.nerc.com/~filez/standards/Reliability_Standards.html).

Table 1 summarizes these different regulations and standards of interest to our discussion.

Table 1. Categorization of information security regulations

	Categories based on intent and scope	**Legislation/Standards**
Information Security Regulations	Corporate Governance	Sarbanes-Oxley
	Information Privacy	HIPAA, GLBA, SB 1386, AB 1950
	Federal Agencies	FISMA, FIPS
	Electronic Banking and Payment	PCI, FFIEC
	Sector-wise	21 CFR Part 11, NERC etc.

The tradeoff between imposing stringent regulations for the purposes of protection and then relaxing them for usability and ease has been amply discussed in prior literature. For instance, many authors have argued against the restrictions of HIPAA and privacy rules. Nosowsky and Giordano (2006) have argued that the privacy regulation issued under HIPAA has had a significant adverse impact on the conduct of clinical research in the U.S., without a substantial corresponding increase in privacy protection for research participants. Cassidy and Chae (2006) have criticized the use of privacy regulations by the U.S. government and commercial sector because it does not correct the market failure that causes this "information externality". The authors propose that market failure can be corrected using either property rules or liability rules and that liability rules at a federal level are likely to be most socially efficient. Other authors have, on the contrary, advocated in favor of regulations. Greenberg et al. (2004) found that, although HIPAA has only had a limited effect on current e-prescribing practices, future electronic prescribing systems would likely fall short of their potential benefits, absent policy refinements designed to encourage clinically appropriate networked sharing of patient health information. Wagner and Dittmar (2006) emphasize that SOX has made accounting procedures more efficient and has improved the quality of financial data. They argue that the benefits of SOX reside well beyond the technical statutory compliance and reach the organizational and shareholder value realms. Similarly, Milberg et al. (2000) studied the trade-offs between open access to information, which enables economic efficiency, and an individual's right to privacy. They concluded that the self-regulatory model of privacy governance may not be sustainable over the long term.

Empirical study

In this section, we first show through a pilot study of US firms that regulations indeed bolster demand for information security products and services. We then use time series methods to further confirm these results and to establish a strong correlation between demand and innovation.

The demand link- Preliminary evidence from US firms

One may argue that information security regulations do not have a direct impact on technological innovation as the production of IT is not directly impacted by information security regulations. However, we hypothesize that demand for information security products, driven by increasing vulnerabilities and malicious attacks and the need for regulatory compliance, leads to higher innovation by information security firms. To study the impact of regulations on firms' demand for information security products, we conducted a pilot study of US firms by interviewing attendees at a major information security conference held in the US, which hosted over 5000 security professionals and researchers from all over the world. We randomly approached 69 subjects of whom 63 agreed to participate. Only 35 of these interviews (51% response rate) yielded usable data that met our criteria for analysis, such as all information items answered, managerial role in the IT or information security areas, and acquaintance with overall security policies of the enterprise. Each interview lasted for an average of fifteen minutes and consisted of an unstructured first phase and a structured second phase. In the first phase, the interviewer explained the purpose of the study, the interviewing protocol, and ascertained the subject's willingness to participate. Once the subjects agreed to participate, their reasons for attending the Conference (purely research, for

organizational decision making, or to learn about new products and processes, etc.), and their general perception about information security regulations were elicited.
The structured phase involved asking nine questions broken into three sections. The first section consisted of questions such as the number of years of experience in their field of expertise, the nature of business of the firm they represented, the size of the firm, and the relationship between the information security and IT departments within the overall organizational hierarchy. The second section aimed at determining the specific information security regulations applicable to the firm, the evolution of top executive support for the information security program, and the processes that were most impacted by information security regulations. The last section was designed to determine the firm's resource allocation for information security and to understand the decisional processes underlying investment in information security.

The respondents had an average of around 17.5 years of experience with a median of 15. The maximum number of years of experience amounted to 36, the minimum to 6, and the standard deviation to around 8.5 (See Figure 2). They were employed in firms covering a wide range of industries and governmental organizations spanning 3 large (over 10000 employees) firms, 15 medium firms (between 1000 and 10000 employees) and 17 small firms (below 1000 employees) (See Figure 3). The sectors included Information Technology (11), finance and banking (7), publishing (1), healthcare and pharmaceuticals (3), manufacturing (2), consulting services (2), retail (1), and others (8).

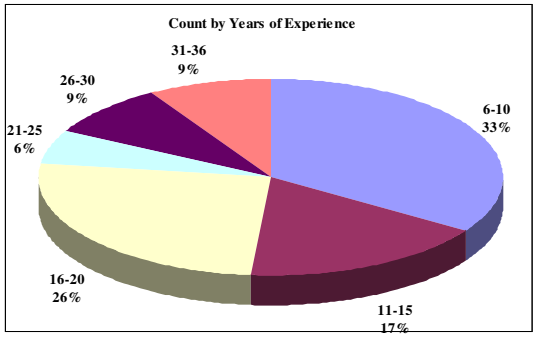

Figure 2. Count by years of experience

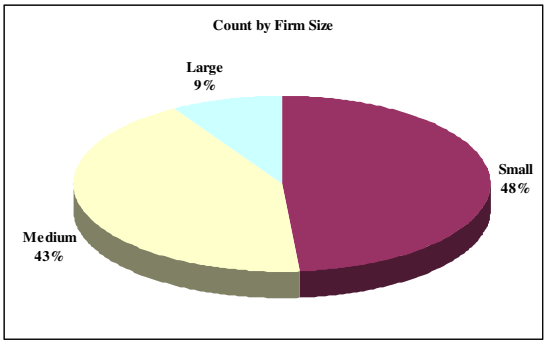

Figure 3. Count by firm size

Only nine of the firms, according to the respondents, have an information security department distinct from IT, while the remaining firms have information security either compactly integrated within IT or distributed across different IT sections. Almost all respondents felt that, regardless of whether they belonged to the public or private sector, their firm's information security strategy has been significantly influenced directly or indirectly by SOX. In particular, they felt that SOX has had a major influence on executive awareness and concern for information security, resulting in better resource allocation, enforcement and monitoring of controls, risk management programs, and auditing. This last result is consistent with prior literature (von Solms 2006; Foote and Neudenberger 2005; Schultz 2004) that has recognized the importance of SOX in creating a fourth wave in the development of information security, namely that of information security governance. The other regulations that mattered depending on firm type included HIPAA, GLBA, SB1386, FISMA, and FFIEC. The majority of respondents (54%) have also indicated that top executive support for information security investment has been significantly increasing driven by regulations and the compelling need to safeguard brand name and image and to avoid litigations. A significant number of respondents (40%) have also recognized that support has only been moderate, while the remaining 6% observed that managerial support has been static mainly due to cost considerations (See Figure 4). Several respondents felt that information security driven by regulations has evolved from primarily perimeter-based protection to internally-focused. Identity and access management was identified by a significant number of respondents (60%) as the technology area that has seen major growth and emphasis over the last three years. They considered it a future priority area too. Prior literature has similarly shown the importance of authentication to the financial sector (Anon 2006), the medical sector (Ulieru 2006), and many other areas. Methods for safeguarding and protecting the confidentiality of data in storage and in transit were identified as the other technology area of high priority from a compliance perspective. Lastly, upon answering questions related to the influence of regulations on resource allocation the results were as follows. Around 63% of respondents indicated that resource allocation for information security investment has significantly increased, while 29% recognized the increase has been moderate. The remaining 8% of respondents acknowledged that management's resource allocation towards information security has been static (6%) and even moderately decreasing (3%) as shown in Figure 5. Investment decisions in a majority of companies (more than 57%) were driven by technical requirements and integration issues clearly indicating that technological innovation is influenced by regulations. Other significant decision factors included business needs and policy

mandates (8), vendor reputation (3), risk (2), and liabilities (2). The majority of respondents felt that cost did not play a significant role in investment decisions.

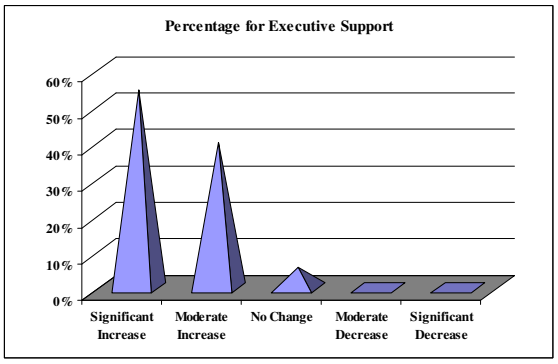

Figure 4. Percentage for executive support

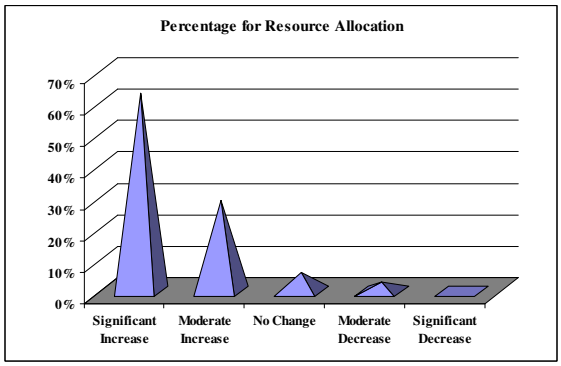

Figure 5. Percentage for resource allocation

Analysis

Quantifying innovation in information security

Prior research has employed various proxies to quantify innovation. Some authors have used patent-related indicators of innovation activity and credit ratings while others have used R&D expenses. Hall et al. (2005) showed that patent count is a noisy indicator of R&D success. Instead, they argued that the number of subsequent citations received by those patents is a better measure of innovative success. Aghion et al. (2005) also used a patent-related measure of innovation. In particular, they measured the intensity of innovation using the average number of patents established by firms in a particular industry.

We commenced this study by performing patent analysis. For that, we searched for patents in the database of the US Patents and Trademark Office[1] under class 726, which corresponds to information security and includes 36 subclasses listed at different hierarchical levels encompassing data protection methods, antivirus techniques, network related security such as firewalls and intrusion detection, security protocols, policies, and vulnerability assessment, etc…We found that few patents were filed prior to 1998. In addition, many recent patents that are still under review do not show in the database because patent descriptions are accessible to the public only after they are accepted. The time series representing the number of patents (Figure 6) clearly shows that the number of patents filed has steadily increased until the peek of the Internet bubble in 2000 and has dropped since then. However, sufficient information is not available to reach a rational conclusion about patent trend because it is typical for patents in information security (as well as IT) to take 4 to 6 years to complete the review process. Therefore many patents that have been filed but have not yet been accepted do not appear in the dataset.

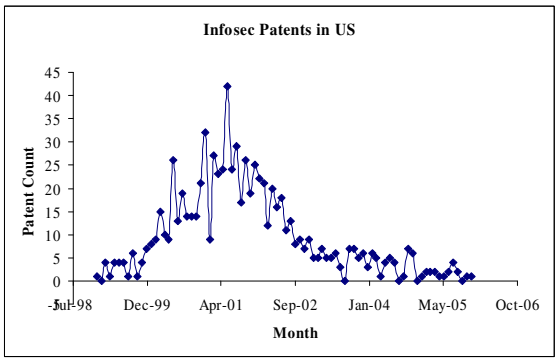

Figure 6. Count of information security patents in the US

[1] http://www.uspto.gov/patft/

Given that patent analysis provides inconclusive evidence for the period under consideration, we resorted to another measure, namely the R&D expenses of major security firms.

Analysis of the R&D expenses time series

Another measure of innovation that has been widely used in the literature (Kee Ho et al. 2005) and does not suffer from data insufficiency is R&D expenses. To build an R&D expenses time series and study the trends in information security innovation, we chose a representative sample of public information security firms with a significant share of the information security market. The sample consists of firms with varying market capitalizations, including Symantec, McAfee, Trend Micro, Check Point Software, Verisign, Aladdin, and Authentidate. Three firms in the sample, RSA Security, Internet Security Systems, and Watchguard Technologies were respectively acquired by EMC, IBM, and Francisco Partners, a US-based private equity fund in 2006. We included these firms in the sample up until the completion of their respective acquisitions. Other IT firms, such as Cisco, IBM, Microsoft, etc… whose main line of business encompasses other than information security were not included in the sample so as not to skew the results. These IT firms get revenues from the sales of other than information security products and services and their revenues are seldom categorized into security related and non-security related. Figures 7 and 8 respectively show firm count by market capitalization, as an indication of firm size, and percentage of firms by market segment.

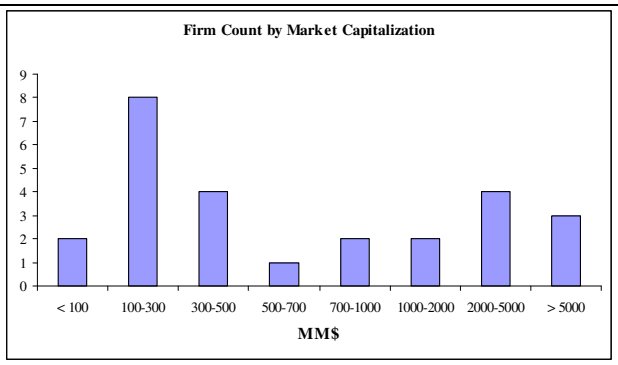

Figure 7. Firm count by market capitalization

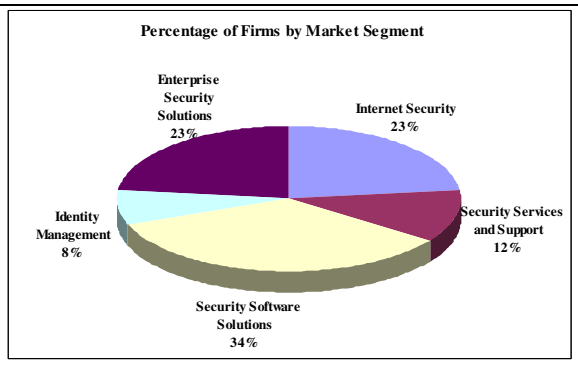

Figure 8. Percentage of firms by market segment

Since the prior patent count analysis showed no major activity in information security innovation prior to 1998, our analysis covers the period from 1998 to 2005. We gathered quarterly R&D expenses from the income statements of the information security firms in the selected sample and constructed the time series shown in Figure 9.

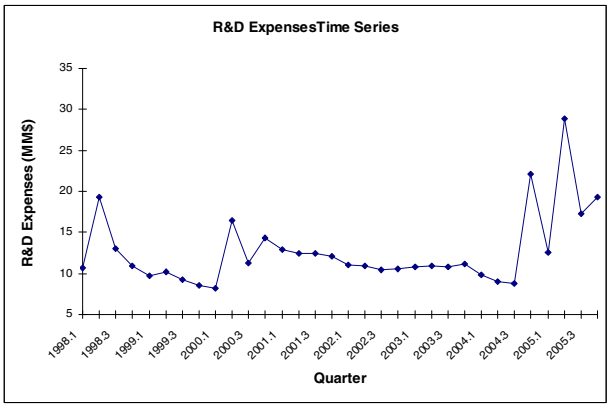

Figure 9. Quarterly R&D time series (MM$)

Figure 9 shows a period of significant volatility in R&D spending near the end of 2004, which coincides with increasing consolidation in the information security industry.

Prior to analyzing the trend of the R&D time series and relating it to demand, we checked whether it exhibited any seasonality. A useful method to study serial dependencies is to examine the partial autocorrelation function (PACF). The PACF indicated no apparent autocorrelation (The first-order autocorrelation amounted to 0.23 and the higher-order autocorrelations were even lower).

Establishing the link between demand and innovation

Data quantifying demand for information security products are not readily available because no firm is willing to expose its strategic information to the public. We therefore propose the revenues of the selected sample of information security firms as a measure of demand for information security. Since revenues of information security firms represent the total amount of income from the quarterly sale of information security-related products and services, we argue that the revenues of information security firms in the US adequately quantify demand. The pre-analysis of the demand time series indicated a first-order autocorrelation of 0.774, while higher-order autocorrelation were found insignificant.

After performing lag 1 differencing to remove first-order autocorrelation from the demand time series, we computed its correlation with the R&D time series. The lag 0 correlation of 0.516, shown in the cross-correlation plot of Figure 10, establishes that demand and innovation are highly correlated.

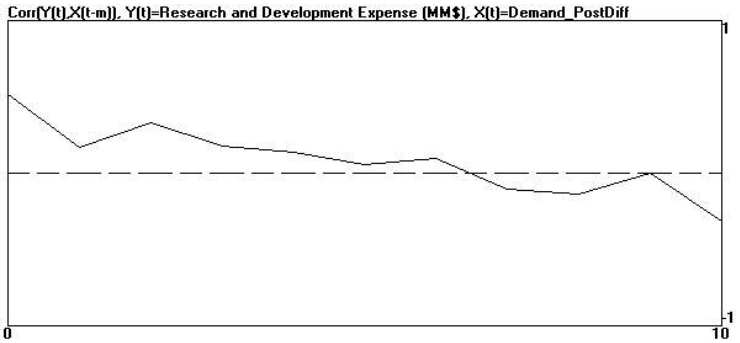

Figure 10. Cross-correlation between innovation and lagged demand

Establishing the link between demand and regulations

We mapped the timing of the various regulations that we have previously identified to the demand curve to assess how demand has fared in relation to regulatory requirements. Although Figure 11 shows an obvious overlap between the effects of various regulations, our goal is to establish a correlation between overall cumulative regulation effect and demand. Table 2 shows a significant positive increase in demand around the timing of important information security regulations and standards. In particular SOX seems to have the highest impact on demand consistent with our findings from the pilot study. In fact, statistics showed that information security spending increased considerably in 2004 and 2005. An estimated $5.5 billion was spent on SOX compliance in 2004 and $5.8 billion in 2005 due to the combination of smaller companies meeting their later deadline, as well as larger companies refining their compliance methodologies[2].

[2] Source: AMR Research, www.amrresearch.com

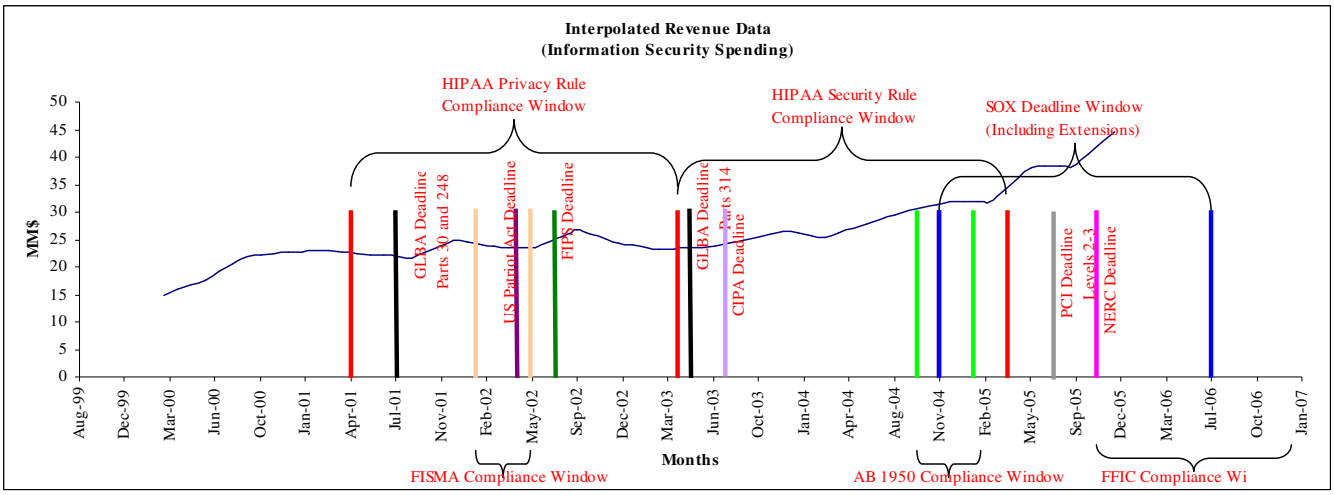

Figure 11. Mapping of major regulations on demand curve (MM$)

Table 2. Demand change over various compliance windows

Regulation	Perecent Change over Compliance Window
HIPAA Privacy Rule	2.378%
HIPAA Security Rule	45.525%
GLBA (Parts 30 and 248)	48.203%
GLBA (Parts 314)	57.082%
FISMA	-3.9170%
FIPS	11.354%
AB 1950	5.605%
CIPA	5.747%
NERC	31.942%
PCI- Levels 2 and 3	33.871%
SOX	20.661%
US Patriot Act	-1.252%
Average	21.433%
% Positive	83.333%
Confidence Interval	[0.079521 0.349143]
t-stat	2.200985

Discussion

We have shown that, as hypothesized in our conceptual and analytical frameworks, demand for information security products has significantly increased (t-stat of 2.2 at a 95% confidence level) around the timing of major regulations, especially over the past 36 months when major regulations such as SOX came into effect. The results of our pilot study also established the direct link between regulations and demand for information security. This reinforces our claim that regulations are linked to an increase in demand for information security for compliance purposes. In addition, we have shown that demand for information security is highly correlated with innovation. The combination of both results establishes an indirect link between regulations and innovation.

Towards new regulatory policies to stimulate innovation

Based on our observations from the trends in regulations and their impacts on innovation in information security, we next discuss the need for new regulations. Much of the mindset of policy bodies, as evidenced in our review of regulations, is

focused on protecting either consumer privacy or organizational assets while very little effort is being made to introduce new policies and legislations designed at fostering technological change. In addition, the dynamics of the information security domain, with rapid increase in computing power and network effects, also require standards bodies to innovate.

Vulnerabilities and the Need for IT Regulations

Figure 12, which is based on the CERT vulnerabilities database (http://www.kb.cert.org/vuls), shows that vulnerabilities have been increasing at an exponential rate over the past six years.

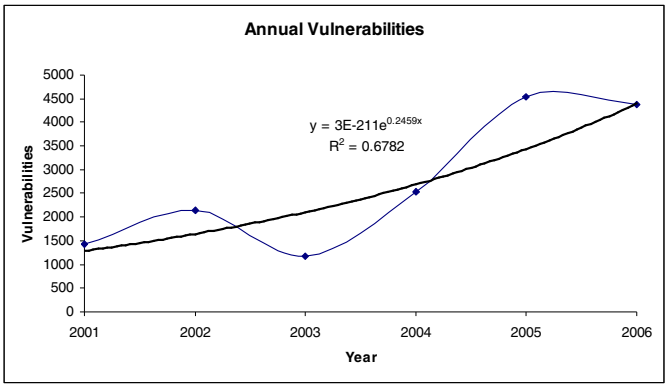

Figure 12. Yearly reported vulnerabilities

Similarly, Figure 13 shows that malicious attacks that exploit these vulnerabilities have also been increasing at an exponential rate from 2000 to 2005 (Data source: http://www.symantec.com/enterprise/security_response/definitions.jsp).

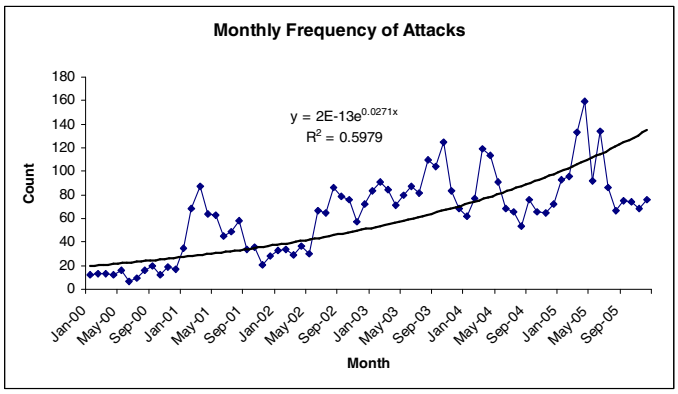

Figure 13. Monthly frequency of malicious attacks

The notion of adding security instead of building it in is the antithesis of basic software engineering principles that advocate simplicity in design and deployment. Indeed, we emphasize the need for more innovation in IT, whether in products, architecture, or processes, with the objective of reducing vulnerabilities through good design. While Arora et al. (2006) show that it is optimal for software firms to "sell first and fix later", we maintain that the continuous innovation by malicious attackers necessitate more forward-looking innovation on the part of IT producers. This leads us to the fundamental question of whether regulating IT will help in stimulating innovation.

The need for regulating the IT industry, given the spate of poorly designed software and security products, has been discussed in many security conferences, such as RSA 2005, and by industry experts, notable among them being Bruce Schneier (http://www.schneier.com/blog). If legislations are intended to enforce strong punitive measures that would mean stifling innovation, with IT companies ending up getting sued for every flaw in a software product, similar to the malaise in the healthcare sector. This warrants the need to use incentives so firms agree to willingly make an effort to reduce the

associated social costs. For instance, providing tax breaks to companies that provide good cyber security is a measure that is being strongly considered by Congress. The mechanics of implementing this are not easy as companies tend to enforce security only when it makes economic sense. For instance, the Internet Security Alliance (http://www.isalliance.org), a collaboration of the Electronic Industries Alliance and Carnegie Mellon's CyLab, has advocated the need to abandon old regulatory approaches in favor of incentives like cybersecurity insurance, awards programs, and caps on legal liability for companies that adopt cybersecurity best practices. Industry-led standardization efforts would foster process and organizational innovation and the diversity of security practices across various industries would make it more difficult for attackers to penetrate systems. Another problem would be in providing incentives and not instituting liabilities if a company were to produce a faulty security tool. This would be akin to being protected if you produced an innovative drug with potential positive features but instead you ended up with disastrous consequences. Therefore, any new regulations that are aimed at command and control of the IT sector, including punitive measures, must be done carefully so as not to impact market innovations.

Privacy breaches and privacy legislation

In order to analyze whether breach notifications and other privacy legislations have helped in reducing the number of incidents, we analyzed the trend in the number of data breaches reported since January 2005. The raw data were compiled by the Privacy Rights Clearinghouse (http://www.privacyrights.org/ar/ChronDataBreaches.htm), a nonprofit consumer rights organization, from a number of sources including mailing lists such as attrition.org and news articles. Figure 14 clearly shows that the reported privacy breach incidents have been increasing in frequency.

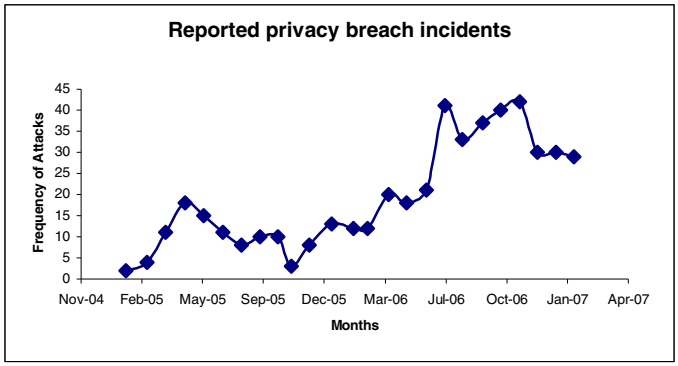

Figure 14. Reported privacy breach incidents since January 2005

The plethora of oft-conflicting state laws with variations in specific provisions, clearly point to the need for Congress to devise a national standard that extends beyond breach notification and to promote industry-developed best practices to reduce the risk of security breaches. Such federal laws should cover the timely disclosure of information to consumers when a security breach poses a significant risk that personal information will be accessed and stolen. Unlike the California law, these laws should go beyond encryption to include other effective industry-developed security measures.

Finally, it is to be noted that self-regulation is a viable option that has not worked well so far. In the case of online consumer privacy, for example, many online policy statements are often lengthy but provide no real privacy protection (http://www.epic.org/reports/decadedisappoint.pdf). Although one may argue that privacy legislations could address these drawbacks, industry advocates have urged Congress to hold back and give businesses more time to develop good privacy practices. If Congress mandates explicit consumer consent in order to share data with third parties, many business models would suffer.

Conclusion

In this paper, we have developed a conceptual model that links demand, innovation, and regulations in information security and have qualitatively and quantitatively tested the veracity of our model and our hypotheses. To conclude, we offer three important recommendations based on our study. First, regulatory bodies need to recognize the importance of information

security to the continued sustenance and stability of the IT sector. Second, in all regulatory efforts, there should be a commitment to highlight the impact on the information infrastructure, which is the backbone of the nation's digital economy. Finally, policies designed to address both IT consumers and IT producers are required. Such policies should not just be focused on a punitive regime. Rather they should be designed to provide social incentives to innovate and to stimulate competition among IT firms.

Acknowledgements

We thank Michael Whitman, the Mini-Track Chair, and the anonymous reviewers for their valuable comments. Their suggestions were instrumental in improving the paper.

References

Adner, R., and Levinthal, D. "Demand Heterogeneity and Technology Evolution: Implications for Product and Process Innovation," Management Science (47), 2001, pp. 611-628.

Aghion, P., Bloom, N., Blundell, R., Griffith, R., and Howitt, P. "Competition and Innovation: An Inverted-U Relationship," Quarterly Journal of Economics (120:2), 2005, pp. 701-728.

[Anon] "Financial Institutions Move Toward Strong Authentication," Computers and Security (25:2), 2006, pp. 86-87.

Arora, A., Caulkins, J.P., and Telang, R. "Research Note- Sell First, Fix Later: Impact of Patching on Software Quality," Management Science (52:3), 2006, pp. 465-471.

Cassidy, C.M., and Chae, B. "Consumer Information Use and Misuse in Electronic Business: An Alternative to Privacy Regulation," Information Systems Management (25:3), 2006, pp. 75-87.

Foote, P., and Neudenberger, T. "Beyond Sarbanes-Oxley Compliance," Computers and Security (24:7), 2005, pp. 516-518.

Greenberg, M.D., Ridgely, M.S., and Bell, D.S. "Electronic Prescribing and HIPAA Privacy Regulation," Inquiry-the Journal of Health Care Organization Provision and Financing (41:4), 2004, pp. 461-468.

Hall, B.H., Jaffe, A., and Trajtenberg, M. "Market Value and Patent Citations," Rand Journal of Economics (36:1), 2005, pp. 16-38.

Hauser, J., Tellis, G.J., and Griffin, A. "Research on Innovation: A Review and Agenda for Marketing Science," Marketing Science (25:6), 206, pp. 687-717.

Kee Ho, Y., Tat Keh, H., and Mei Ong, J. "The Effects of R&D and Advertising on Firm Value: An Examination of Manufacturing and Nonmanufacturing Firms," IEEE Transactions on Engineering Management (52:1), 2005

Kim, D., Cavusgil, S.T., and Calantone, R.J. "Information System Innovations and Supply Chain Management: Channel Relationships and Firm Performance," Journal of the Academy of Marketing Science (34:1), 2006, pp. 40-54.

Milberg, S.J., Smith, H.J., and Burke, S.J. "Information Privacy: Corporate Management and National Regulation," Organization Science (11:1), 2000, pp. 35-57.

Nosowsky, R., and Giordano, T.J. "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: Implications for Clinical Research," Annual Review of Medicine (57), 2006, pp. 575-590.

Schmookler, J. Invention and Economic Growth, Cambridge: Harvard University Press, 1966.

Schultz, E.E. "Sarbanes-Oxley - a Huge Boon to Information Security in the US," Computers and Security (23:5), 2004, pp. 353-354.

Schumpeter, J. A. The Theory of Economic Development, Cambridge: Harvard College, 1934.

Shah, S.K. "Motivation, Governance, and the Viability of Hybrid Forms in Open Source Software Development," Management Science (52:7), 2006, pp. 1000-1014.

Swanson, E.B., and Ramiller, N.C. "Innovating Mindfully with Information Technology," MIS Quarterly (28:4), 2004, pp. 553-583.

Ulieru, M., and Ionescu, D. "Privacy and Security Shield for Health Information Systems (e-health)," Computer Systems Science and Engineering (21:3), 2006, pp. 215-221.

von Solms, B. "Information Security - The Fourth Wave," Computers and Security (25:3), 2006, pp. 165-168.

Wagner, S., and Dittmar, L. "The unexpected Benefits of Sarbanes-Oxley," Harvard Business Review (84:4), 2006, pp. 133.