Preface

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: information technology, telecommunications, energy, banking and finance, transportation systems, chemicals, agriculture and food, defense industrial base, public health and health care, national monuments and icons, drinking water and water treatment systems, commercial facilities, dams, emergency services, commercial nuclear reactors, materials and waste, postal and shipping, and government facilities. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed.

This book, *Critical Infrastructure Protection*, is the first volume in the new annual series produced by IFIP Working Group 11.10 on Critical Infrastructure Protection, an active international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts related to critical infrastructure protection. The book presents original research results and innovative applications in the area of infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors.

This volume contains twenty-seven edited papers from the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at Dartmouth College, Hanover, New Hampshire, March 19–21, 2007. The papers were selected from fifty-one submissions, which were refereed by members of IFIP Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection.

The chapters are organized into six sections: themes and issues, infrastructure security, control systems security, network infrastructure security, infrastructure interdependencies and risk assessment. The coverage of topics showcases the richness and vitality of the discipline, and offers promising avenues for future research in critical infrastructure protection.

This book is the result of the combined efforts of several individuals and organizations. In particular, we thank Rodrigo Chandia and Mauricio Papa for their tireless work on behalf of IFIP Working Group 11.10. We gratefully

acknowledge the Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College, for nurturing IFIP Working Group 11.10 and sponsoring several of the research efforts whose results are described in this volume. We also thank the Department of Homeland Security and the National Security Agency for their support of IFIP Working Group 11.10 and its activities. Finally, we wish to note that all opinions, findings, conclusions and recommendations in the chapters of this book are those of the authors and do not necessarily reflect the views of their employers or funding agencies.

Eric Goetz and Sujeet Shenoi

Chapter 2

CYBER SECURITY: ARE ECONOMIC INCENTIVES ADEQUATE?

Scott Dynes, Eric Goetz and Michael Freeman

Abstract Protecting national critical infrastructure assets from cyber incidents is an important challenge. One facet of this challenge is that the vast majority of the owners and operators of critical infrastructure components are public or private companies. This paper examines the threats faced by for-profit critical infrastructure entities, the incentives and drivers that influence investment in cyber security measures, and how policy initiatives might influence cyber preparedness in critical infrastructure entities.

Keywords: Information security, economic incentives, government policy

1. Introduction

Critical infrastructures are vulnerable to cyber incidents. According to one study, thirty hackers with a budget of $10 million "could bring the United States to its knees. [Terrorists] are now powerful enough to destabilize and eventually destroy targeted states and societies" [8]. In a government exercise, simulated hackers took control of power grids and 911 systems in nine U.S. cities [12]. *The Washington Post* reported that "U.S. analysts believe that by disabling or taking command of the floodgates in a dam or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real world lives and property" [6].

In launching the National Strategy to Secure Cyberspace [11] in February 2003, President Bush demonstrated the concern about "the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy or national security," noting that "disruption of these systems can have significant consequences for public health and safety," and emphasizing that the protection of cyber systems has become "a national priority" [2].

Dynes, S., Goetz, E. and Freeman, M., 2008, in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 15–27.

President Bush's Executive Order on Critical Infrastructure Protection [1] established the National Infrastructure Advisory Council (NIAC), which was charged with determining the risk terrorists might pose to critical infrastructures and how the government might best reduce those vulnerabilities. In its final report, the NIAC concluded that market forces, where they are free to operate, would be the most effective means to promoting a greater level of information security [10].

Given this desire to raise the general level of information security for critical infrastructures, the question becomes one of how to bring this about. This challenge must be viewed in the context that the vast majority of the owners and operators of critical infrastructure assets are non-governmental (public, non-profit or private for-profit) entities. In all cases, managers face similar incentives and drivers in utilizing limited resources to achieve their business objectives. The question thus becomes to what extent is information security perceived as a business objective. If the investment by businesses does not meet societal needs, government may be required to take regulatory or legislative action. Arguments against stricter information security regulation often cite market forces as being effective societal cyber security drivers, but the evidence does not completely support this position.

To gain a grounded perspective on this issue, we examine the main economic drivers of cyber security and assess how they can improve the security postures of industry and government organizations. The action of these economic drivers, if better understood, could help shape a framework for evaluating cyber security and investments in cyber security. We approach this problem by examining theoretical economic incentives and drivers for public and private firms to invest in information security. We follow with field studies of firms, looking at the actual practice of cyber security investment. We conclude with a discussion of the effectiveness of market forces, and possible policy mechanisms that could drive entities to do better.

2. Cyber Security Investment

This section discusses theoretical and practical approaches to making cyber security investment decisions. These are by no means the only approaches; rather, they are representative of those found in each domain. We begin by framing the issue of what companies hope to achieve through investments in cyber security.

2.1 Cyber Security: What is Adequate?

What does it mean for a firm or other entity to have an "adequate" level of cyber security? A rational approach to defining "adequate" involves identifying the entity's risk by examining the vulnerabilities, the probabilities of successful exploitation of the vulnerabilities, the cost of the outcomes if the vulnerabilities are exploited, and the cost of mitigating the vulnerabilities. The incentives for security arise from the possible costs and other losses that are uncovered.

While the insight into the risk from this process is likely better than that from more heuristic methods, even a strict application of the process can result in an overly narrow and localized view of information security risk.

Consider the security management of a home computer. Most individuals use their home computers to surf the web, send and receive email, and do word processing. From this purely local viewpoint, the incentives for users to protect their machines are to maintain connectivity and to protect the data they value. If a user does not store valued data on his/her machine, no security measures may be adopted until the machine is infected with a virus that interferes with the user's limited use of the machine. There is little incentive to invest in security against viruses, Trojans, worms and other malware unless they affect the user's ability to use the machine. The user is typically not concerned about the probable induction of the machine into a bot network that may cause harm to others.

The Broad View Consider the situation of a global information risk manager of a financial firm. Her focus is not merely on keeping her firm's machines free of viruses and worms; it is also on assuring the availability of her firm's services and on the integrity and security of data as it is being held internally, at business partners, and passed between her firm and other enterprises. She has a much broader view of what is being protected: her firm's business processes, her customers' data, her local machines and network, all of which may be viewed as sources of risk to business processes. Consequently, she invests in information security at a level consistent with this view. Her incentives are different from those of the home user: she needs to protect her clients' data (money) internally, she needs to assure that clients' data is protected by her business partners, and she must ensure that her firm is regarded as a secure entity by other businesses that interact with her firm.

In the case of most firms, the definition of what is being protected lies between these two extremes. We hypothesize that absent external forces such as regulation, the relative information security stance assumed by an organization is correlated with the inclusiveness of what is being protected. For example, within a particular industry sector, some firms would consider that protecting their local machines, applications and data is adequate. Other firms would adopt a more extensive view of what needs to be protected by ensuring that their communications and data transactions with members of their extended enterprise are secure.

External forces such as regulation will affect this correlation. Returning to our financial sector example, regulation can have the effect of making the local good and the sector good the same. This is the result of regulation imposed on industry as well as network effects: if a financial institution's security is inadequate, then other financial institutions will not conduct business with it because they realize that the institution's level of security affects their own level of security. In this case, the minimum acceptable level of security is that which also meets a sector good. This is especially true in a sector that relies

heavily on user trust, which can be eroded across a sector by a security breach at just one institution.

Incentives and Public Welfare So far we have examined what entities might reasonably do in their self interest from the individual firm and sector points of view. What might constitute an adequate level of information security from the viewpoint of a government, and what relationship does this level of security have with the security level that firms might reasonably adopt? Ultimately, the question is: are there adequate incentives for firms to adopt security postures that are in line with the public welfare?

The government is primarily interested in addressing vulnerabilities that would threaten the ability of the infrastructure to deliver critical services and goods to the population [11]. The government is concerned with systemic risks that have not manifested themselves to date. Because of the different nature and low probability of these risks, it may be the case that rational firms will never adopt a level of information security that would address the vulnerabilities that underlie the risks. Put another way, the types of information security desired by the government may be different from those that individual firms might consider. It is reasonable to assume that information security solutions needed for the public welfare are different (and possibly more stringent) than those required by firms.

This is not to say that there is no overlap between a sector's interests and the government's interests. It is likely that the financial industry's interests and the government's interests are closely aligned. In other instances, the aims will be different, as in the case of control systems used by power sector companies. The government would like to see more secure control systems, but the companies see little or no economic incentive to upgrade. In our discussion we will address mechanisms that promote the adoption of better security measures in cases such as this.

2.2 Optimal Level of Investment

Every firm will adopt some level of information security. A minimum level of information security investment is required simply to do business and to be credible with potential customers and suppliers. We call this the security baseline β. This baseline level would be different for the various business sectors and, perhaps, for different business sizes.

At or above the security baseline is an optimal level of investment for the firm (see, e.g., [7]). The argument is that the optimum level of cyber security investment is where the marginal costs of increased information security equal the marginal decrease in costs due to events such as virus attacks, hacking and break-ins. This argument represents a definition of the optimal level of investment in information security. Figure 1 graphically relates the minimal level of spending with the local optimal level of spending. Note that the minimal level β will always be less than or equal to the local optimal level of spending O_L. Within an organization, the optimal level of spending occurs when an

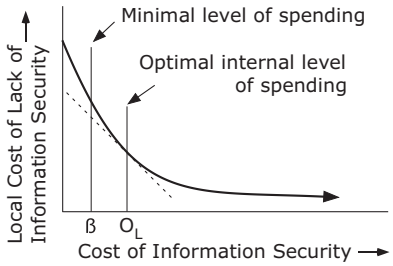

Figure 1. Optimal level of local information security investment O_L (after [7]).

increase in security results in an equal decrease in costs due to security lapses. Taken literally, this optimum corresponds to a largely local view of what to protect. This is because the vast majority of firms have not experienced cyber events that have had significant external costs.

If organizations are to use such a method, they need assessments of the costs incurred due to a lack of information security, their spending on information security, and the marginal rates of return for changes in spending. In reality, while an organization may know how much it spends on cyber security, estimating the true cost of information security lapses is a much more difficult proposition. Some costs are fairly concrete (e.g., the time spent to rebuild systems and recover data); other costs are less tangible (e.g., theft of intellectual property and loss of future business due to brand damage). Surveys such as those done annually by CSI/FBI include such costs, but they are more indicative of trends rather than providing accurate estimates of true economic costs (mainly because survey respondents estimate their losses without applying consistent metrics or guidelines).

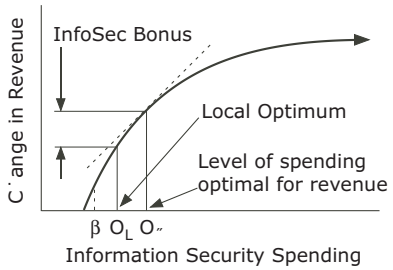

Figure 2. Revenue change as a function of information security investment.

If there are economic incentives for investing at a level higher than that required for a local optimum, what would they look like? Any economic incentive would imply that increasing information security would result in greater profits, either from increased revenue or reduced costs. The case of increased revenue leads to the scenario shown in Figure 2, where the curve in Figure 1 is plotted on new axes to show the change in revenue as a function of investment in information security. Increased revenue (and profits) would result in a new

optimal point reflecting the greater investment. A likely reason for this scenario is that increased information security results in an advantage over competitors with lesser levels of information security. Examples include email providers that offer virus screening as part of their services and banks that offer secure online services.

3. Field Studies

We now turn from intellectual constructs to results from field studies, which have been motivated by a desire to understand how firms actually invest in information security: drivers, incentives, and how risk is identified and managed. The field studies involved identifying a "host" organization, and typically conducting interviews with the CIO, the manager of information security, a supply chain executive, and a supply chain relations manager of the host. We would ask the host to introduce us to a few key suppliers that it interacted with using the information infrastructure; we then conducted similar interviews of the suppliers.

Our field studies involved more than fifteen companies and interviews with dozens of people. Details of the case studies are provided elsewhere [3, 5]. In the following, we present pertinent results from the case studies. The results are organized around the drivers of information security investment, the degree of interconnectedness and dependency on the information infrastructure, and the resilience of the organization to cyber events.

3.1 Manufacturing Sector

The host was a manufacturing conglomerate; we conducted interviews at its electrical and automotive business units. The host is very dependent on the information infrastructure to communicate with its customers, and was working to move its supply chain management functions (communications with its suppliers) to be Internet-based as well. The primary driver of the firm's existing level of information security was the need to protect its internal network and data. The process of how information security managers arrived at their current level of security was not well described, likely because it was not the result of a rational process or an external dialogue. To decide on the base level of information security, managers typically use their past experience, input from trusted colleagues, consultants, trade magazines, web research and other mass media.

The main drivers for the adoption of additional information security measures are government regulation and customer requirements. While more than one firm mentioned Sarbanes-Oxley as shining a spotlight on their internal information security procedures, none said that their level of information security increased as a result of Sarbanes-Oxley (although there was frequently a shift in focus or reallocation of resources as a response). On the other hand, every firm described itself as being responsive to customer requirements for improved security. In the manufacturing sector, customer demands mainly come in the

form of questionnaires, some of which are quite extensive. The firms viewed these questionnaires as representing a qualification for business. As a group, the interviewed firms made little or no demands on their suppliers for levels of information security, although one supplier said that it would introduce such requirements in the near future. Most of the firms viewed information security as a cost and as a qualifier. The director of IT at one supplier thought that information security provided a competitive advantage because customers felt more comfortable doing business with them as a result of their information security focus. With this exception, none of the interviewees felt that information security would ever become a competitive advantage in the manufacturing sector. Details of the risk the host faced as a result of using the information infrastructure to manufacture and deliver its products can be found in [4].

3.2 Oil and Gas Sector

The field study host was a mid-sized refiner of specialty petroleum products. Unlike the situation in the manufacturing sector, business operations at the refinery would be largely unaffected by an Internet outage. Supplies are typically ordered by telephone with a lead time of weeks, and product orders, while usually communicated via the Internet, could easily be handled via the telephone as well. However, the plant's process control systems (PCSs) rely on an information infrastructure. PCSs are commonly used in refineries, pipelines and electric power generation and distribution systems; they comprise sensors, actuators and logic systems required to operate and monitor industrial processes. The dependence of the refinery on the PCSs is very high; it is not feasibly to operate a refinery manually.

From interviews with the V.P. of refining and the manager of information security, it was clear that there is little perceived economic incentive to invest in a more secure PCS; the lens that the VP of refining adopted was, "How will a more secure PCS help me make a better product?" There were few if any questions from customers about PCS security; the major driver is long-established regulations related to required redundancies in critical systems. During our interviews, two additional PCS security drivers emerged, both centered on assuring business continuity. The first concerned motivations arising from the threat of PCS cyber incidents. The VP of refining allowed that he was concerned that an event could shut his plant down, but it had never happened before, and he had never heard of such a thing in the industry. As a result, he could not justify investments to mitigate the risk. He emphasized that even if a malicious cyber event were to disrupt operations at a major refinery, he would be reluctant to invest in better PCS security because his was not a major refinery and would not be subject to the same risk. However, he would be inclined to invest in security if similar-sized refineries were to be attacked.

The second driver resulted from a risk mapping exercise conducted under a research project supported by the Department of Homeland Security [13]. This effort focused on creating a mapping between IT and business risk at the refinery. The mapping clarified the business consequences that would result

from various PCS security incidents. As a result of this activity, the VP of refining stated that he understood how investing in security would help him make a better product: he could make more of it due to increased resilience. As a result, we conclude that the economic and market drivers for increasing PCS security at this refiner are low. While latent drivers do exist, a greater level of transparency into actual PCS security incidents at other refineries would be required for these drivers to become effective. The drivers and incentives for major refineries are somewhat different, leading to a more proactive and global view.

3.3 Financial Sector

The field study involving a financial institution is not yet complete; however, we have interviewed multiple CIOs and global risk managers of firms in the financial sector. There are two main information security drivers in financial firms: government regulations and internal concern for brand and reputation. Unlike firms in the manufacturing and oil and gas sectors, the reputation of financial firms for being secure is of critical importance, both for the firm and its customers. Financial firms are also prime targets for break-ins; Willie Sutton famously said that he robbed banks because that's where the money is [14]. Financial institutions have a very large economic incentive to assure the security of their information. As a result, financial firms are very proactive about security and business continuity. Global risk officers think quite broadly about risk. For example, one risk officer mentioned that his biggest concern regarding cyber security was a lack of imagination: he and his staff cover known cyber risks, and spend serious effort on "blue sky" thinking about what is possible, but he is concerned that he is not clever enough. The attention to detail extends to business partners. Whereas the manufacturing firm above depended on business partners to have "reasonable" levels of information security, and not be proactive about assuring that this was the case, the financial institutions we interviewed were very proactive. The institutions had a set of security practices that they expected their business partners to adhere to, and they ensured that the partners adhered to the practices by conducting audits. This practice is not industry wide, as indicated by a recent data theft case involving a third-party processor for Visa [9].

Finally, financial institutions are completely reliant on the information infrastructure. Trillions of dollars are transferred electronically each day, and the vast majority of customer cash withdrawals occur via ATMs. Without electronic communications, banking activities would be severely disrupted.

3.4 Investment Practices

Based on our interviews, we have identified three approaches that firms employ to make cyber security investments.

Sore Thumb Paradigm In this paradigm, decision makers prioritize their information security efforts and investments based on the attacks and incidents that cause the organization the greatest "pain" (i.e., costs in terms of dollars and manpower). Security investment decisions are generally made based on incomplete risk information (e.g., from industry publications and peer groups) and not on detailed risk assessments. The sore thumb approach is common in smaller companies (where there may be close personal relationships between information security managers and the executives who authorize security spending) and in sectors that are less reliant on IT for business operations. This mainly reactive approach provides many opportunities for improvement.

IT/Business Risk Paradigm This paradigm involves a certain degree of implied risk management methodology to rank information security initiatives, with the goal of reducing the risk to IT components and processes. The information for these efforts typically comes from IT managers and staffers within the organization who relay security issues that they have identified internally or from other industry sources. The director of information security then prioritizes responses based on estimates of the likelihood and cost of successful attacks, and the cost to mitigate vulnerabilities. Directors use this process to varying degrees of rigor. The IT risk portion of the paradigm seeks to protect the network, servers, desktops, i.e., hardware devices. This is not directly a risk management approach, although elements of managing risk – identifying costs and potential consequences of incidents – are employed. The business risk portion explicitly examines how information security risks might impact business processes. The assets protected might include the ERP system and the customer order system, i.e., business processes. The security initiatives, therefore, relate to ensuring business continuity. The IT/business risk paradigm can be reactive and/or proactive.

Systemic Paradigm This paradigm is sufficiently different that it cannot be placed on a continuum that encompasses the above strategies. In this paradigm, information security efforts are inseparable from business strategy. Decision makers incorporate information security at every step of IT process development to enable a business strategy. In fact, it makes no sense to even think about IT-enabled business without having information security baked in; it also makes no sense to have "naked" information security initiatives that are not developed as part of some business process. The prioritization and funding of information security initiatives are not treated separately; budgets for IT projects automatically include security considerations. This paradigm is clearly proactive.

The first two approaches could all be present in an organization. The sore thumb approach is often a tactical response to security incidents such as a virus infection. The presence of the IT risk and business risk strategies in firms is more subtle. As a firm's view of information security matures, it is also possible

to move a firm from IT risk to business risk, possibly through an exercise that maps IT risk to business risk.

4. Are Economic Incentives Enough?

If we adopt the theoretical treatment of economic drivers discussed earlier, where economic drivers are defined by increased net revenue, the results of our field studies suggest that the role economic factors play in information security varies from sector to sector and within sectors. In general, economic factors are more prevalent in investment decisions in the financial sector than in the manufacturing sector. The motivation for companies to invest in information security comes from best practices, government regulations, brand/reputation protection and customer demands. Best practices are derived largely from trade publications, industry associations and from regulations. A subset of these best practices forms a baseline for information security investment; managers can invest in this baseline set of security capabilities without further conversations with higher management. This is regarded as a cost of doing business.

While firms comply with government regulations, the great majority of them believe that existing regulations have a negligible effect on the quality of information security. In fact, many feel that the efforts spent on complying with Sarbanes-Oxley and similar regulations detract from efforts to develop effective security capabilities. One director of information security commented that he now has to spend time assuring that the door to his data center is of a certain thickness rather than working on business continuity planning.

Protecting brand and reputation is an important driver at larger firms. This is an economic driver as brand and reputation are related to the viability of the firm. The drivers behind brand and reputation protection offer insight into the differences in the stature of information security in various industry sectors. Manufacturers gain their competitive advantage from pricing, speed of design and development, and reliability in meeting schedule commitments. While information systems play an important role in creating these advantages, an information security failure at a supplier does not necessarily impact the level of trust customers have in the supplier (there are exceptions, e.g., the intellectual property of customers held by suppliers is of critical importance to the customers).

In the financial sector, brand reputation for security is paramount, and financial firms invest accordingly. One information risk manager we interviewed said his firm would invest essentially unlimited funds to make the information security risk disappear. The last element, responsiveness to customer requests, is interesting from several perspectives. First, the willingness of a firm to modify its information security practices for a potential customer is likely to be a competitive advantage, which is an economic incentive. Next, responsiveness to customer requests gives customers influence over the information security environment in which they operate. As noted above, most firms regard these customer requests as qualifications. For example, potential suppliers to a major oil company must complete a questionnaire about their information security

practices. Interviewed firms said they regard these questionnaires as a set of qualifications, and strive to meet all the qualifications. This mechanism can (and should) be used by firms to manage the risks they face due to their interdependencies with other firms.

4.1 Systemic Risk Management

A central theme of our field studies was the emergent risk due to the interdependencies of Internet-mediated business processes. As noted above, the ability of business sectors and critical infrastructures to provide quality services is dependent on the availability of the information infrastructure. With the exception of the financial sector, the field studies indicate that firms generally do not consider inter-firm risk. Examining the systemic risk of their dependence on the information infrastructure enables organizations to better address their risk. The risk can be reduced by addressing the vulnerabilities and/or by increasing the resilience of business processes in the face of cyber events. For intra-firm processes, this would require interactions with partners in the extended enterprise, along with joint actions to address the systemic risk that emerges from business interdependencies. It is clear that this can be accomplished. The willingness of firms to accommodate customer requests for particular information security practices indicates that firms would be receptive to addressing shared risks with customers and potential customers. The enabling activity is for the customer to communicate the desired action to the vendor; the precursor to this is the customer taking a systemic view of its cyber risk.

Unfortunately, understanding the systemic risk may not be enough. In the case of the VP of refining at our field study partner, the realization of a risk was not enough to cause an investment to mitigate the risk. He was challenged to see the rationale of investing against a threat that to his knowledge had never occurred; moreover, even an attack against a large refinery might not drive him to action. This point of view was reflected in other interviews: managers are disinclined to invest against hypothetical threats. Investing in physical security is reasonable because break-ins and physical theft are common; the threats are tangible. Investing in PCS security is much harder as the threats are less tangible and it is unclear to some managers whether the threats are real. This is not to say that attacks do not occur: according to Eric Byres, there have been more than 150 PCS security incidents. The reason that this is not well-known is that there are incentives to not share this information; knowledge that a firm has experienced a PCS attack could damage its reputation. The same situation is true for other types of cyber events. Managers would be much more apt to invest against threats that they knew had been exploited or are in a class that had been exploited. Processes that determine systemic risk will certainly detail how to rationally invest in information security to reduce the exposure to largely intangible risks. Knowledge of the range of actual attacks would make important risks more tangible, and more likely to be mitigated.

4.2 Proper Policy Role

We have noted that the government is promoting the development of protection against information attacks that have been hypothesized, but have never been seen. The government is trying to manage the risk by proactively reducing the vulnerabilities prior to suffering any consequences. The difficulty is that most firms are averse to making security investments against events that have never occurred, even if they might worry about them. Many firms are reactive in their investments, responding to actual vulnerabilities. Implicitly, they are not managing risk, but closing known vulnerabilities.

One recent policy effort to remedy this was taken in California, which passed a data breach notification law (AB 700, better known as SB 1386) that required the notification of persons whose personal information was or may be accessed inappropriately. Prior to this law, personal data theft was not broadly reported, resulting in an environment where security investments were not a priority. Since the enactment of the law there have been many reports of data breaches, which have resulted in greater awareness of the issue and in investments to protect against such breaches. Essentially the data breach notification law resulted in the sharing of information that transformed what was for many a hypothetical threat into a known reality. This is certainly a proper role for government policy.

5. Conclusions

Our studies indicate that latent market forces exist for increased cyber security in critical infrastructures. Firms are incented to assure that their business processes are resilient in the face of cyber events, internally as well as externally. By adopting methods for examining their systemic risk to cyber events, firms can become aware of the risks they face due to their interdependencies with other firms. Acting to address these risks will make their own business more resilient; as a result, their business sector will also become more resilient. Thus, latent market forces result in the protection of critical infrastructures.

The government has at least two roles to play. First, by enacting policies that result in disseminating information about cyber incidents, the government can help activate the latent market forces. Secondly, market mechanisms will serve to address the government's concern about critical infrastructures only to the extent that these concerns are aligned with business concerns. If the government is concerned about risks that are not concerns of individual firms, endogenous economic forces are not present, and the government will have to address these risks in other ways.

Acknowledgements

This work was partially supported by the Institute for Information Infrastructure Protection (I3P) under Award 2003-TK-TX-0003 from the Science and Technology Directorate of the U.S. Department of Homeland Security.

References

[1] G. Bush, Executive Order on Critical Infrastructure Protection, The White House, Washington, DC (www.whitehouse.gov/news/releases/2001/10/20011016-12.html), October 16, 2001.

[2] R. Dacey, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report GAO-04-628T, U.S. General Accounting Office, Washington, DC, 2004.

[3] S. Dynes, Information security and health care – A field study of a hospital after a worm event (mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecHealthCare.pdf), 2006.

[4] S. Dynes, E. Andrijcic and M. Johnson, Costs to the U.S. economy of information infrastructure failures: Estimates from field studies and economic data, presented at the *Fifth Workshop on the Economics of Information Security*, 2006.

[5] S. Dynes, H. Brechbühl and M. Johnson, Information security in the extended enterprise: Some initial results from a field study of an industrial firm, presented at the *Fourth Workshop on the Economics of Information Security*, 2005.

[6] B. Gellman, Cyber-attacks by al Qaeda feared, *The Washington Post*, June 27, 2002.

[7] L. Gordon and M. Loeb, The economics of information security investment, *ACM Transactions on Information and System Security*, vol. 5(4), pp. 438–457, 2002.

[8] J. Lewis (Ed.), *Cyber Security: Turning National Solutions into International Cooperation*, CSIS Press, Washington, DC, 2003.

[9] L. Loeb, CardSystems solution becomes a cautionary tale, *eWeek*, July 21, 2005.

[10] National Infrastructure Advisory Council (www.dhs.gov/xprevprot/committees/editorial_0353.shtm).

[11] National Infrastructure Advisory Council, The National Strategy to Secure Cyberspace, The White House, Washington, DC (www.whitehouse.gov/pcipb/cyberspace_strategy.pdf), 2003.

[12] Public Broadcasting Service, PBS Frontline: Hackers (www.pbs.org/wgbh/pages/frontline/shows/hackers), 2001.

[13] J. Watters, Analyzing corporate risks with RiskMAP, presented at the *Second I3P Process Control Systems Workshop*, 2006.

[14] Wikipedia, Sutton's Law (en.wikipedia.org/w/index.php?title=Sutton%27s_law&oldid=119669553).