Information Security in the Extended Enterprise:

Some Initial Results From a Field Study of an Industrial Firm

Scott Dynes [1,2]
Hans Brechbühl [1]
M. Eric Johnson [1]
[sdynes, Hans.C.Brechbühl, M.Eric.Johnson]@Dartmouth.edu
[1]Glassmeyer/McNamee Center for Digital Strategies
Tuck School of Business at Dartmouth College
[2] Institute for Security Technology Studies, Dartmouth College

Version of April 13, 2005

Abstract

What are the main drivers of private-section investment in information security? How exposed are firms to cyber risks arising from their reliance on the information infrastructure? Initial results are presented from a field study of a manufacturing company and four of its suppliers of different sizes. We find that many managers believe: that information security is less a competitive advantage than a qualifier for doing business; that firms' internal networks are not at additional risk as a result of using the information infrastructure to integrate their supply chains; and that their supply chains are robust to internet outages of up to a week in duration. We discuss their security perceptions and actions in the context of a cost model.

Introduction

As organizations increasingly rely on the internet for their internal and external business processes, each firm's security decisions have an impact on the overall security of the information infrastructure for the thousands of suppliers, collaborators, and channel partners that they interact with as part of that firm's extended enterprise (a collection of firms that design, produce, and market a product or service [Dav2004]).

Each firm in the extended enterprise must have access to critical business information such as product specifications, marketing plans, and vast transactional data on product sales and movement within the supply chain. Managing the security of this sensitive information flowing across the extended enterprise is a significant and under-researched topic. Firms often make information security decisions with very limited information about the threats their systems face, the strength of their systems against these threats, and the efficacy of additional security measures. Outsourcing and globalization present even more difficult security issues; in many industries competition is quickly changing from firm against firm to extended enterprise against extended enterprise.

Understanding the economics of information security within and across firms will necessitate understanding the process by which firms adopt information security

mechanisms; this will expose existing drivers and possible incentives promoting greater information infrastructure security. Separately, understanding the risks referred across the extended enterprise is critical to defining a level of information security to minimize those risks, and is a step towards developing a business case for the security needs of the firm as well as addressing what level of security is needed for the greater public good. Understanding these issues will enable policymakers to make reasoned decisions regarding what policies might be needed for and what policy mechanisms will be effective at promoting an increased level of security in the information infrastructure.

Over time, to the extent the business case is understood, the market might drive enhanced security and help close vulnerabilities, addressing some aspects of current market failures. As a policy matter, serious research into these issues will allow chief executive officers (CEOs) to talk with their peers and government leaders about this issue from a fact-based and theoretically sound foundation and enable CEOs to add significantly to sound policy-making.

While there are a few papers that have studied return on investment (ROI) on information technology (IT) security investments at the firm level ([Bla2001], [Gee2001], [Gor2002], [Soo2001]), little empirical work has been done at the firm level to understand the processes involved in information security. Like the interdependent security risks faced by other business partnerships ([Gun2004], [Kun2002], [Kun2004]), such as baggage handling in the commercial airlines, we hypothesize that information security risks across trading partners exhibit many important risk management challenges.

We have identified three research efforts that address the core information security issues pertaining to the efficacy of economic and other potential drivers of information security, the risks to which critical business infrastructures (supply chains) are being exposed, and to what extent security decisions need to be made with an eye to managing risks beyond one's local organization. These research efforts are:

To understand how firms adopt information security capabilities. How do firms currently make security investment decisions? What are the key drivers? A key objective is understanding the drivers that influence firm's information security investment strategies.

To access interdependency risk magnitude. How large is the real or perceived security problem for the extended enterprise? What are the security risks and how do those risks translate into business risks? Knowing how vulnerable or resilient supply chains and extended enterprises are to security failures of one of their members will directly inform the policy debate about how much information security is needed for the greater public good.

To evaluate the information security gap. Are larger companies only as secure as their least-secure supplier? Are larger firms making better security investments (and better patch management decisions) than smaller firms, creating a security gap in the extended enterprise, which may render all interdependent companies as vulnerable as the weakest critical company in their extended enterprise [Joh2004]? Is anyone managing the risk

across the extended enterprise? Should large, relatively secure firms be concerned about collaborating with smaller, less secure firms?

This paper presents initial results of a study that explores these questions through field research of firms of different sizes and their supply chains. The results presented relate to the first two points of interest described above.

Methods

The field study consists of a set of interviews with security and supply chain executives and managers at a "Host" firm and four of its direct suppliers (direct meaning that the supplier's product is core to the product of the Host). The interviews were designed to elicit the knowledge and beliefs of the interviewed individuals; security audits of the interviewed firms were not a part of this study. Thus, the results of this study reflect the beliefs of the interviewees without an external check on the validity of certain statements (like the recent AOL/NCSA Online Safety Study [AOL04]). By asking the same questions of different interviewees in the same organization, we were able to look at the internal consistency of information provided in interviews.

The Host firm is a Fortune 500 manufacturing firm with plants and sales worldwide. A series of interviews were conducted with security, information and supply chain executives and managers at both the headquarters level as well as at an individual business unit (BU) level. In all, 13 individuals were interviewed. Interviews were based on a set of questions and conceptual frameworks designed to gain insight into the issues under study for each particular role interviewed. Interviews were conducted in person with one or two researchers, and one to four interviewees. Interviews lasted from 30 minutes to 2 hours. At the start of each interview it was made clear to the interviewees that the interview was anonymous; during the interview every effort was made to build a high degree of trust with the interviewee. Host interviews were conducted July 2004 through February 2005.

As this set of interviews was designed to be the first in a larger study, this study was treated as a pilot study in that the set of questions asked during each interview changed. Specifically, a set of role-dependent core set of questions was asked at each interview; as the series of interviews progressed, additional questions were introduced in an effort to deepen the understanding of the research issues.

With the aid of the Host firm, six candidate supplier participants were selected. These candidates were chosen without regard to their information security capabilities; we had no knowledge of their abilities or their history with the Host firm in that regard. The criteria used to choose the candidates were:

- Candidates had to use some form of electronic communication to manage their supply relation with the Host. This was a requirement.

- Candidates would be a range of sizes in terms of their annual revenue. This was a requirement.

- Candidates would provide products directly used in the Host's products. This was a requirement.

- Candidates should be close to a small set of geographic locations. This was a nice-to-have.

The Host asked the candidates if they were willing to participate in the study. Five of the six suppliers contacted by the Host agreed to participate in the study; of these five, four were interviewed. At the suppliers we spoke with information security and IT executives and managers, and where applicable the account managers of the Host's account. For the four suppliers, nine individuals were interviewed. Supplier interviews consisted of one researcher and 1-2 interviewees. Four interviews were conducted in person; the rest were conducted by telephone. Supplier interviews were conducted December 2004 through February 2005.

In terms of exploring how firms made information security investment decisions, the interview questions were the same as those used for the Host interviews. With regards to the risks developed through supply chain integration, while the original intent was to ask questions only about the Host-Supplier relationship, the discussion at the host and supplier firms covered both supplier and customer relationships for that firm. As with the Host interviews every effort was made to establish a high level of trust with the interviewee. At the start of the interview, it was made very clear that the interview was anonymous, and that the purpose of the interview was informational and not in any way an audit of the supplier's information security capabilities.

Results

We were able to develop a host relationship with a Fortune 500 manufacturing company; the results we present here result from interviews with 13 executives and managers of IT, information security and supply chain at the Host, and with 9 executives and managers of IT and customer accounts at 4 suppliers to the Host. Table 1 gives some particulars about the Host and the suppliers.

	Product	Number of locations	Annual Revenues	Subsidiary?
Host	Conglomerate	many	several billions	No
Supplier A	Metal	many	few billion	Yes
Supplier B	Logistics Services	many	few 100 millions	Yes
Supplier C	Printing/Design	few	few 10 millions	Yes
Supplier D	Metal parts	one	few millions	Yes

Table 1: Properties of Interviewed Firms.

Drivers of Adoption of Information Security

While each firm approaches information security in a different manner, there are some patterns that emerge. InfoSec managers talked about the set of processes that were used to arrive at their existing level of information security in much more nebulous terms than they talked about the drivers of the adoption of additional levels of information security.

First, the primary driver of firm's existing level of information security is the InfoSec manager protecting their firm's internal network and data. The process of how InfoSec managers arrive at their current level of information security was not well-described, likely because it was not the result of an external dialogue, but of a dialogue internal to the InfoSec manager. For deciding on this base level of InfoSec, InfoSec managers use their past experiences, the experiences of trusted colleagues, consultants, trade magazines, web research and other mass media.

While the resulting baseline InfoSec practices differ by company, the results are reported as being the same across all interviewed firms: none has experienced a virus, worm, break-in or web defacement in the last year.

Second, the main drivers for the adoption of additional information security are government regulation and customer requirements. While more than one firm talked about 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.

With one exception, firms had an analogous reaction to customer requests for information security. Every firm interviewed described itself as being responsive to customer requirements for information security; one supplier said that customer requirements would be the big driver of further information security efforts. Within this set of firms, customer demands have mainly come in the form of questionnaires, some of which were quite extensive. Industries that have presented these questionnaires include aerospace, oil, and trucking. The interviewed firms view these questionnaires as representing a qualification for business; with the probable exception of Supplier D, these questionnaires did not affect the level of information security at the firms as the firms already had sufficient information security.

As a group, the interviewed firms made few or no demands on their suppliers for levels of information security, although Supplier B said that they would start having requirements in the near future.

Of the five firms interviewed, four think of information security as a cost and a qualifier. The director of IT at Supplier B thought that information security was a competitive advantage in the sense that customers felt more comfortable in doing business with them as a result of their focus on information security. With this exception, nobody interviewed thought that information security would ever become a competitive advantage.

Risks to Extended Enterprises From Reliance on the Information Infrastructure
Two types of risks were explored in detail: risks to internal IT systems and information as a result of integrating the supply chain using the information infrastructure, and risks to a firm's ability to produce product as a result of supply chain disruptions caused by information infrastructure events.

Information Security Risks
The great majority of the internet-mediated communications the interviewed firms have with their customers and suppliers is via email and web-based applications.

The Host firm communicates with its suppliers using Electronic Data Interchange (EDI, essentially a standardized, codified email format for communicating information about orders), a database-backed web application, a few virtual private network (VPN) connections that are isolated to the server hosting the required application, and email. The security manager at the Host regards web-based applications as the type of connection carrying the highest risk to the Host's internal network, with VPN being second, and EDI and email third.

	Web App	VPN	Electronic Data Interchange	Email
Host	Y	Few	Y	Y
Supplier A	N	N	N	Y
Supplier B	N	N	Y	Y
Supplier C	N	N	N	Y
Supplier D	Y	N	N	Y

Table 2: Types of Connections Firms Utilize with Their Business Partners

Of the suppliers, A and B used EDI and email to communicate with their business partners (customers and supply chain), and did not utilize VPN or web-based applications. Supplier C used only email; D used email with a single supplier having access to information stored in a database using a web-based interface.

None of the firms interviewed had experienced a compromise of security to their internal systems as a result of their electronic integration with their suppliers.

Risks to Supply Chain Continuity
What are the risks to the Host's supply continuity as a result of using the information infrastructure? These discussions were framed around the case of the Host losing the ability to communicate with suppliers via the internet for various periods of time. All firms interviewed said they would use phone, fax and FedEx to communicate with suppliers and customers in cases of prolonged internet outage; none thought that such an

occurrence would result in any lost business.

To understand the level of disruption an internet outage would have on the supply chain of the interviewed firms, an effort was made to understand how the various firms communicated with their supply chain. The results are summarized in Table 3, which shows the division of the types of communications used to order their supplies at the time of the interview.

The business units (BUs) and divisions interviewed at the Host are the largest user of the internet for supply chain management; the use of web applications and EDI accounted for over 3/4 of the orders sent to all suppliers of these BUs and divisions. Executives at each BU said that it is their goal to move 100% of their suppliers to use either a web application or EDI in the near term.

Supplier A, a multi-billion dollar company, uses only phone and fax to order their supplies. Supplier B relies on EDI for 60% of its supply chain communications with the remainder being phone or fax. Supplier C uses email to order 80% of their supplies; they follow up both their email and fax orders with hard copies sent by mail.

	Web App	EDI	email	Phone/Fax
Host BU #1	88% of PO's online		0%	12%
Host BU #2	~77% of PO's online		0%	~23%
Supplier A	0%	0%	0%	100%
Supplier B	0%	60%	0%	40%
Supplier C	0%	0%	80%	20%
Supplier D	0%	?	?	?

Table 3: Percentage of Interviewed Firm's Supply Chain Order Communication by Connection Type

Despite its dependence on the internet for communication with its suppliers, Host interviewees noted that the worst thing that could happen from a supply chain perspective would be for the Host's intranet to go down; this would directly affect plant's abilities to access the Host's internal inter-plant ordering system[1], resource planning systems, and other automated systems supporting the generation and processing of orders. The Host has invested in a backup ISDN system with the intent that all the Host's locations would be able to communicate with each other if the internet were to fail. Supplier B also has invested in a frame-relay backup system that is completely separate from the internet; this would link all their sites.

From the standpoint of the suppliers and supply chain continuity, the impact of lack of

[1] At the Host, the largest suppliers to some plants are other Host plants.

access to the internet is mainly time-dependent: the longer the outage, the greater the effect. Table 4 combines the reported impact that outages of various durations would have on the supply chains of the interviewed firms.

There were several viewpoints expressed during interviews at the Host, including the impact of security on both their supply chain and their participation in the supply chain of their customers. The shortest interruptions that would be noticed were surprisingly short, on the order of 15 minutes. This is due to a requirement of some of the Host's customers that they be notified within 15 minutes of the Host shipping product to the customer; failure to send this advance shipping notice (ASN) is noticed, and is a factor in renewing a supplier's contract. Some executive at the Host were more concerned with the potential impact of short outages than those of longer outages.

As the length of an outage increased, Host interviewees talked about additional variables that affected how an internet failure would impact the Host's business continuity. The overall sense was that the Host would do whatever it took to maintain the ability to produce and ship product; they felt that the element that would suffer most would be invoicing and payment; that would be secondary to the actual ordering of supplies and production of product. When the conversation moved beyond this generality, interviewees talked in greater detail about other factors that would impact the Host.

Internet down for:	An afternoon	1 day	3 days	A week
Host BU #1	No impact	Low volume plants: supply-side pain	Hi volume plants OK	Hi volume plants: shipping issues
Host BU #2	ASN disruptions - impacts customer	Stock available for production	Customers would see slack	Unable to produce all items
Supplier A	No impact	No impact on supply side; "big deal" on customer side		
Supplier B	[confident there would be no impact on supply or delivery of products]			
Supplier C	No impact	No impact	No impact	No impact
Supplier D	No impact	No impact	No impact	No impact

Table 4. Reported impact of an Internet outage of various durations on the supply chains and customers of interviewed entities.

One interviewee talked about plant volume. The Host has high-volume plants that produce substantial quantities of the same product, and other plants that produce small numbers of customized products. From a supply-chain perspective, the high-volume

plants would be able to sustain a 2-3 day internet outage without difficulty; this interviewee expected that around that point the suppliers would start calling the Host; there would be no need for the Host to call the suppliers. He termed this "supply chain learned behavior", and noted that for high-volume plants there is a lot of forecasting information shared between the Host and suppliers, so the suppliers have a good idea of the Host's needs for a substantial amount of time. He thought that if internet connectivity were out for a week, the supply chain would be operating, but the finished products would be piling up on the shipping dock due to the impact of the outage on the Host's ability to interact with its customers and shippers.

Another Host interviewee echoed this theme, noting that the amount of disruption caused within the supply chain is dependent on the number of customers a supplier has: if a high-volume plant ships to only a few customers (think of large potato growers who supply McDonald's: they only have one customer), it is possible to process orders sent by phone or fax. Such relationships would also be involved in forecasting. If the same plant were to have to take orders by fax or phone from thousands of smaller firms, it would be very challenging.

In contrast, the low-volume, custom plants would be affected to a greater extent by an outage. In the example he was using, the custom product requires components with lead times of days; in order for a part to be available to be integrated into the product in a timely fashion, it would have to be ordered today.

Supplier A said that there would be not impact to their supply chain as a result of an outage of the internet, as all their supply chain communications occur via phone or fax.

While EDI was a very significant part of Supplier B's communications with its supply chain, the interviewees felt that there would be very little impact if they were unable to access then internet. Supplier B felt the biggest impact would be on invoicing and payment.

Supplier C, the printing and graphics design firm, was confident that an internet outage would not affect either their supply chain or their ability to produce product for their customers. In explaining their supply process, it came out that even when they use email for ordering, the email is essentially a follow-up of a phone call; the email is followed up with a print-out that is mailed to the vendor. They feel the volumes of supplies ordered is small enough such that they would be easily be able to manage their supply and direct customer needs with phone, fax and FedEx.

Supplier C thought the largest impact would be in maintaining their customer relations; they like to maintain a close relationship with their customers using email. An internet outage would greatly affect this.

Discussion

Drivers of Information Security

The cyber security issue is both an economic and a technology issue. The technologies within the enterprise, between enterprises, and across the internet, all sit in markets. Therefore, the issue of vulnerabilities throughout the system sits within the context of the existing market structure and the various technical, competitive, policy and legal factors. This market is often thought of as being a classic "public goods" market – that is, that the market under current conditions leaves a certain amount of economic welfare unaddressed, and that loss of welfare is defined as a market failure. In this market, we may pay for security on our own systems, although there is evidence that we do not know exactly what the cost-benefit analysis is, but we may not pay to protect others who connect with us or the internet – those are "externalities" (things that happen to other people) that we won't easily internalize. As the issue sits in the market place now, we know that there are vulnerabilities throughout our networks of networks.

In the face of market failures impacting the economy or the national security, there are traditionally two approaches: private and public. Private approaches can include new business models that change the market, innovation, the effects of increased transparency and information, voluntary standard setting, best practices, contracts between parties, insurance, corporate good citizenship, and the like. Public responses can include changes in research and development funding, liability, regulation, mandatory standards, tax policy, government procurement and standards, and the numerous other ideas that have been discussed by the government.

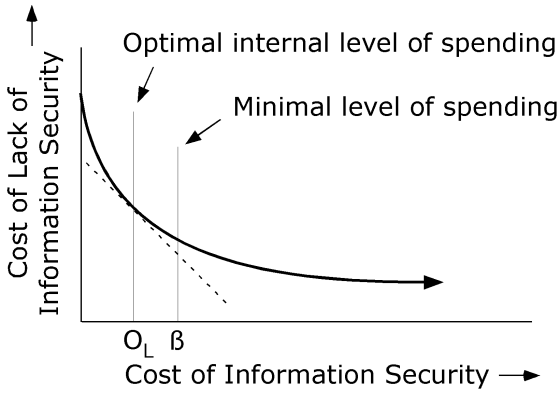

Figure 1. Optimal level of local information security investment O_L. Within an organization, the optimal level of spending will occur when an increase in information security results in an equal decrease in costs due to information security lapses. β is the spending level that firms adopt in the absence of external forces. After [Gor2002].

In this context, Freeman [Fre2004] argued that there are four classes of drivers for increased information security: market forces, government regulation, government spending, and litigation. Do our results provide any insight into the effectiveness of these drivers?

Government Regulation

The interviewed firms certainly pay attention to government regulation; 'government regulations' was mentioned more than once as one of the top three information security drivers. While they might pay attention, in general they do not think that government regulation would be the best manner for promoting effective information security, a view shared by others [Dyn2004]. More than one of the study participants had recently

completed a Sarbanes-Oxley audit. Sarbanes-Oxley, while not specifically about information security, has some impact on firm's information security practices. While one of the interviewees felt that Sarbanes-Oxley improved their information security, he also said that he thought the effect of Sarbanes-Oxley was to move the focus of attention from important security issues to less-important issues.

Market Forces

Every firm will adopt some level of information security, either deliberately or through neglect. In a 2002 paper, Gordon and Loeb developed a model to explain the optimal level of investment in information security. Here we embrace and complement their model to provide a context in which to understand our results. These authors argue that the optimum level of cybersecurity investment is where the marginal costs of increased information security equal the marginal decrease in the costs due to events such as virus attacks, hacking, break-ins, etc. As written, these arguments represent a definition of the optimal level of investment in information security for the organization's good. Implicit in this optimal level is a definition of what is being protected; the optimal level of investment will likely differ if a firm is trying to protect their internal IT infrastructure, or their external dependence on the information infrastructure. We label the level of information security investment optimal for their local good (their internal IT systems) as O_L in Figure 1.

For any firm, there is a level of information security investment that is adopted; we will call this the security baseline β. This level reflects decisions made within the firm about what they are protecting: some firms may take a very local view and only think of their internal IT infrastructure; others will take a more global view and also think about business processes linking them with their extended enterprise. As drawn in Figure 1, β is to the right of O_L, reflecting our belief that some of the interviewed firms were investing

Top concerns of security managers:	
External break-ins Internal information Business continuity Disaster recovery InfoSec posture of vendors	Internal employees Process security (do applications behave as expected?) Redundancy Spyware
Practically of no concern:	
Infosec posture of vendors Data corruption Data obfuscation Insider attacks Internal systems	

Table 5: Information security manager's reactions to selected security issues. The numbers in parentheses indicate the number of respondents reacting to the issue.

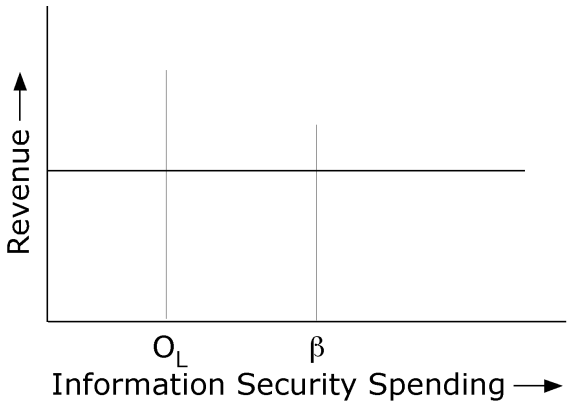

Figure 2. Increased information security has no effect on revenue. This will be the case if information security is not important in selecting suppliers. O_L and β are shown for continuity.

in security at a level greater than that required for the local optimum. This belief is based on the fact that they could identify few costs associated with a lack of information security.

This investment at a level greater than O_L could indicate, among other possibilities, that the interviewed firms are explicitly adopting a more expansive view of their security boundary than that of their local good, or that they value freedom from successful attacks higher than is strictly economically justified. Based on the reactions of interviewed security managers to issues of internal and external security concerns (shown in Table 5), we posit that although security managers are mainly concerned with internal risks (a local viewpoint), they are not titrating to find the optimal investment point O_L but are investing to eliminate all successful attacks. In order for organizations to find the optimal level of spending they need to accurately know the costs incurred due to a lack of information security, their spend on information security, and have a good idea of what the marginal rate of return would be for a change in the spend. In reality, it is relatively easy to know what an organization spends on cybersecurity; knowing the true cost of information security lapses is a much more difficult question. There are fairly concrete costs, such as the time that is spent rebuilding systems and recovering data, and less tangible costs such as the costs of intellectual property losses or loss of future business due to brand damage. Well-known surveys such as the CSI/FBI survey include such costs, but it is acknowledged that they are more indicative of trends rather than accurate estimates of true economic costs.

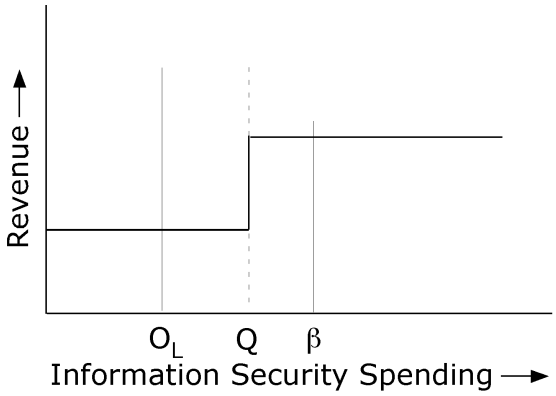

Figure 3. Information security is a qualification for doing business; a certain level Q must be invested to realize this additional revenue. Q is shown as being to the left of O_L; it could be to the right of O_L and still be consistent with our results.

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 a greater profit, either from increased revenue or reduced costs. The executives we interviewed felt that in their industry, there was little

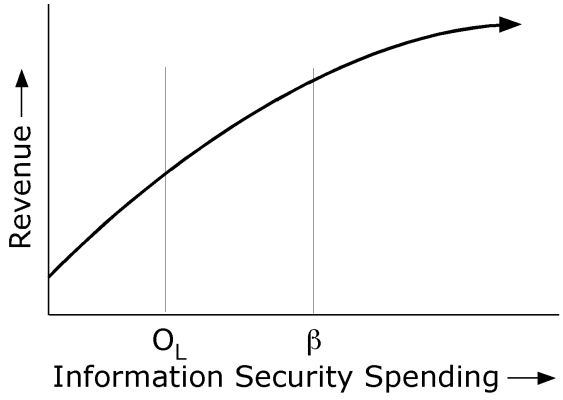

Figure 4. Increased information security yields greater revenues. This will be the case if increased information security confers a competitive advantage.

possibility to increase revenue through higher levels of security beyond a qualifying level (Q) required by some customers. Thus the firms felt that they faced either Figure 2 (no revenue impact) or Figure 3 (a qualifying level of security that enabled them to work with some customers). The Host said that some customers had required it to fill out questionnaires regarding its information security practices; the Host interpreted these questionnaires as describing a set of required practices. As part of becoming a vendor for a customer, Supplier B was subjected to a security audit to see whether its practices were acceptable. Both the Host and Supplier B indicated that they were able to qualify with their existing information security practices.

Assuming that if they did not qualify they would not have become vendors, a qualification requires that a firm must invest at a certain level in order to realize the new business associated with acquiring a new customer. This would be represented as a step function in revenue, as is shown in Figure 3. It is entirely possible that there would be a series of customers with qualifications requiring an incrementally increasing investment in security; in this case the step function in Figure 3 would start to resemble the curve in Figure 4. Here, increasing investments in security have a positive impact on revenue over the entire investment space. Only one of the executives we interviewed felt security investments in their industry led to increased revenue through such a competitive advantage.

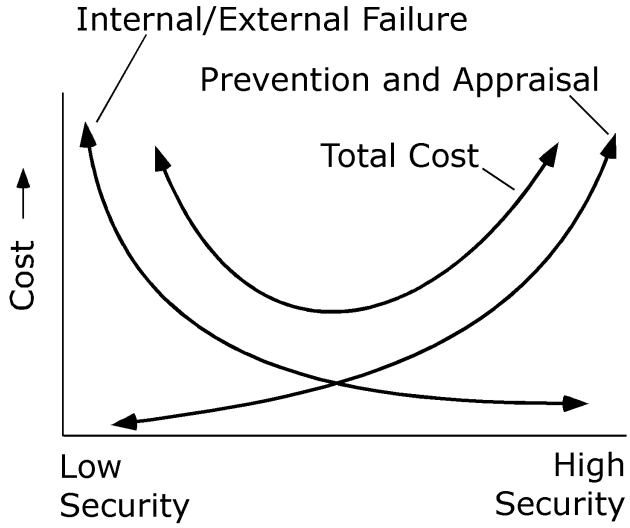

Figure 5. Information security investments in a framework from the quality literature.

Most of the executives we interviewed focused purely on the cost trade-off of security, disregarding the possibility of increased revenue. Coupling Gordon and Loeb's model with ideas from the quality literature (Jur2000), these costs can be broken into two major groups: Costs of avoiding security failures such as on-going security appraisals and investments in

Costs of Avoiding Security Failures	
Costs of Prevention Firewalls/Antivirus Training Patch management	Costs of Appraisal Audits Monitoring Intrusion detection
Costs of Security Failures	
Costs of Internal Failure Lost productivity IT services – restoration Time to market	Costs of External Failure Lost confidence/revenue Litigation Fines

Table 6. Categories of Security Costs with Examples.

preventive measures like installing a firewall. On the other hand, there are costs associated with security failures – either internal failures that are not observed by customers or external failures which are observed by those outside the firm (Table 6). Internal failures are security problems that are discovered internally, resulting in costs such as lost productivity (for example lost worker productivity and restoring information services). External failures, such as exposing confidential information can lead to many costs including litigation, fines, and brand damage. Figure 5 shows the resulting total cost; as in the work by Gordon and Loeb, there is an optimal level of investment.

One interviewee at the Host further argued that even when information security does not increase revenue there can still be a positive business value for increasing information security. This executive felt that even though increasing information security would likely not increase profits directly, the processes put in place would take costs out of the business. As an example she talked about single sign-on: while this was being done for reasons of information security, it would reduce her costs as well as increase the efficiency of her staff. Multiple participants at a recent CIO roundtable also made this point: some believed that the activity of adopting more rigorous information security will reveal opportunities for increasing efficiencies; others believed that the adoption of technologies for information security will result in better knowledge of business processes such as supply chain management, benefiting the business [Dyn04].

Are market forces present? It appears that internally, firms are more responsive to information security issues than is required to minimize tangible costs. This is likely due to the consideration of intangible costs in deciding on an appropriate level of information security. As a participant in a recent Cisco/Tuck CIO Summit said, “Failure in security, that gets noticed. If you're successful, it's expected.” [Dyn04]. This mindset will drive organizations to adopt a much stricter level of information security than that needed to minimize tangible costs. From an external point of view, it appears that there is a growing trend to require that business partners have a base level of information security.

Government Investment

Our results say nothing about the effectiveness of government investment as a means of promoting increased information security.

Liability
None of the interviewed firms felt that a lack of information security on their part would result in their being liable for damages, with the possible exception of liability resulting from Sarbanes-Oxley. None of the interviewed firms specifically held a cyberinsurance policy.

Risk to Supply Chain Continuity
The robustness of supply chains and extended enterprises is an important constituent in what would constitute a level of information infrastructure security consistent with the public good. If crucial infrastructure supply chains and extended enterprises can be incented to adopt levels of information security so they are robust against information security lapses, they would also be robust from the perspective of the greater public good with respect to information security. What do our initial results say about the risks faced by firms that utilize the information infrastructure to manage their supply chain?

One interesting result was the variability in the use of the internet by the different firms. The Host, a Fortune 500 company, utilizes the internet extensively for both its supply chain and for interacting with some large customer. Supplier A, which is also a very large company, does not use the internet at all in the management of its supply chain. Suppliers B and C utilize the internet for more than half of their supply chain ordering.

At a superficial level, executives at the interviewed organizations were very confident that they would be able to manage their supplier and customer relations in the event of an internet outage, particularly at the larger companies. All were certain that their firm would do whatever was necessary to enable their producing and shipping product. All spoke about using phone, fax and FedEx as their fall-backs if they were unable to communicate via the internet. All thought that the most pain would be experienced in the invoicing and payments process as these processes would not be a priority, and picking up all the pieces later would be tedious and error-prone.

Is it possible to substitute the three Fs (fone, fax, FedEx) for the internet?

At the smaller suppliers (C and D) it seems very possible that they would be able to use the phone and fax for their supply chain communications; Supplier D is a very small firm without a web presence, and their small volume and lack of technical sophistication makes it seem reasonable that they would be able to effectively communicate with phone and fax.

It seems likely that Supplier C, the printing and graphic design firm, would also be able to function using the three Fs. They recently experienced an outage of broadband internet connectivity for a period of weeks; while this was a major IT event, it was not a major corporate event. The actual supplies that they order are printing stock, film, inks and adhesives; orders for standard supplies are communicated by phone or email; in either case a paper copy is sent via mail. Custom supplies are obtained by talking with the vendor via phone to work out the details, and then making the order as above. Customers and Supplier C exchange designs via email or FTP; email is used to communicate with a

remote design location. Supplier C said that they would revert to dial-up access to their machines or to FedEx if the internet were unavailable. As noted above, the largest impact to Supplier C would be the way they maintain their relationships with their customers.

Supplier A is interesting in that today it manages its supply chain using only fax and phone, while it does communicate with its customers, including the Host, using EDI and web-based applications (90% of its communications with the Host are via EDI or web-based applications). It would seem that an internet failure would not impact its supply chain at all, but would impact its ability to communicate with its customers. A member of Supplier A's risk management group said that they have thought about this, and while they made sure that they have enough phone lines to adequately deal with the expected volume of calls should internet communication be disrupted, they did not do the same for fax machines or fax servers. Thus, Supplier A has identified this risk to its ability to maintain business operations in the face of an internet outage, and has taken steps to mitigate that risk.

The Host is the most dependent on the internet for management of its supply chain, and is planning to become even more dependent: executives at both of the Host's business units aim to interface with all their suppliers using either web applications or EDI. As noted above, the Host is often a major supplier to itself; this is one reason that the Host has invested in an intranet that is separate form the internet. Another reason is the reliance on centralized applications: a supply chain manager stated that he would not know how to enter data into the Host's internal systems if their intranet was unavailable.

Would the Host be able to rely on the three F's to maintain business as usual should the internet fail, as they hopefully assert? Probably not. During one interview, a supply chain executive calculated that the number of faxes that would have to be sent to replicate the information carried via the internet would be roughly 30,000 a week from each plant; the supplier has well over a dozen plants, and due to the centralized nature of their enterprise applications, these faxes would all be sent from fax servers at one location. The issue of whether the supplier could deal with all the faxes coming from multiple customers was also raised: those suppliers with few customers are more likely to be able to manage a reversion to three F communication than suppliers with many customers.

The lack of ability to run the business as usual does not mean the business will not run. Supply chain managers at both of the Host's BUs talked about how the Host forecasts supply requirements with high-volume suppliers. As noted above, one supply chain manager was quite confident that the "learned behavior" of the supply chain would result in deliveries happening as scheduled without the need for communication.

There are certain costs associated with doing business using the three F's; these were not explored in a systematic manner. The interviews suggests that none of the interviewed firms has thought of this either; at most, interviewees talked about the overtime that would be needed to enter faxed invoices into the firm's computers for processing, and the increased error rate associated with this activity.

Logistics Suppliers
Above, we discussed the ability of the interviewed firms to use phone and fax in the case of an internet outage. What about the third 'F', FedEx, and other providers of transportation and logistics services? Providers of these services are becoming increasingly important in supply chains: one of the interviewed firms was on the verge of contracting with a third-party logistics provider (3PLP) to handle the shipping, warehousing, and delivery of a very substantial portion of its supplies. Essentially, this firm has outsourced its supply chain management to the 3PLP: the inventory of supplies at a plant will be completely managed by the 3PLP. This will require a tight integration between the firm's materials requirements planning systems and the 3PLP's systems.

Will 3PLPs and other providers such as FedEx perform in the face of a widespread internet outage? The central role that such firms play in the ability of other firms to operate makes an examination of the robustness of these providers particularly important.

The Big Picture
This study examined how firms identify and manage information security risks internally and within their supply chains. Our initial results, which we caution readers are from a sample size of 5 and are likely industry specific, lead us to believe:

- Firms are adopting levels of information security that are appropriate for their internal operations.
- Market forces, in the form of customer requirements or qualifications, are the primary driver for additional information security measures.
- The interviewed firms were reactive in their approach to information security.
- Firms need to pay more attention to the risks they are exposed to as a result of using the information infrastructure to manage their extended enterprise.

As of the date of this report, firms seem to have reacted sufficiently to existing internal threats. We think that at this point information security conversations would benefit most from turning from threats to internal systems to threats to external relationships by examining the risks in the ways they conduct business within their extended enterprise. The important question for them to ask in regards to risks is, "Who owns the risk?" [2]

In the absence of solid knowledge about the threats and probabilities of occurrence needed to make reasoned estimates of risk, firms should think about managing the outcomes of information security events through redundancies.

Future work
We are currently planning a more extensive study that would include multiple supply

[2] The provenance of this pointed yet practical formulation of the issue lies with Dan Geer

chains in the same business sector, so that we can gauge the variability within an industry. We also plan to study more than one business sector, as we believe that organization's information security practices will vary widely by industry. For example, in our experience we have found that the financial industry is vastly more sophisticated in managing security risk, both because of their business (money and trust), and because they are highly regulated. We hope to compare their practices to other critical infrastructure industries such as oil and gas.

This work was supported in part by a grant from the World Bank. Points of view in this document are those of the authors and do not necessarily represent the official position of the World Bank.

This work was supported in part under Award number 2000-DT-CX-K001 from the Office for Domestic Preparedness, Department of Homeland Security. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security.

The authors gratefully acknowledge the generosity of the firms interviewed; this research was possible only through their interest and willingness to devote their time to this effort. The authors thank Adam Golodner, Michael Freeman, Bob Bruce, Bill Brown, Dan Geer, and Denise Anthony for valuable conversations and insights, and Genevieve Chan for her invaluable assistance with this manuscript.

References

[AOL04] AOL/NCSA Online Safety Study
http://www.staysafeonline.info/news/safety_study_v04.pdf

[Bla2001] Blakley, B. (2001) "An imprecise but necessary calculation," *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4. A publication of @stake.

[Dav2004] Davis, E.W. and R.E. Spekman, Extended Enterprise. FT Prentice Hall, NY, NY (2004).

[Dyn2004] Dynes, S. B. C. "Security and Privacy: At Odds With Speed and Collaboration?"
http://mba.tuck.dartmouth.edu/digital/Programs/CorporateRoundtables/SecurityAndPrivacy/Overview.pdf

[Fre2004] Freeman, Michael, S. Dynes and E. Goetz, "*The Known Unknows of Cyber Security and Cyber Terrorism"* Dartmouth Institue for Security Technology Studies working paper. http://www.ists.dartmouth.edu/library/119.pdf

[Gee2001] Geer, D. E. Jr. (2001) "Making choices to show ROI," *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4. A publication of @stake.

[Gor2002] Gordon, L. A. and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, (November 2002), pp. 438-457.

[Gun2004] Gunther, R. (2004) "At Risk," *Wharton Magazine*, Spring 2003.

[Joh2004] Johnson, M. E. "The safety of secrets in extended enterprises," Financial Times, 18 August 2004, A7.

[Jur2000] Juran, J.M. and F. M. Gryna (2000), Quality Planning and Analysis, Forth Edition, McGraw-Hill, NY, NY.

[Kun2002] Kunreuther, H. (2002) "Interdependent Security: The Case of Identical Agents," *National Bureau of Economic Research*, Insurance Project Workshop, Cambridge, Feb 1.

[Kun2004] Kunreuther, H. (2004) "Risk Analysis and Risk Management in an Uncertain World," Forthcoming in *Risk Analysis*, Wharton School Working Paper.

[Soo2001] Soo Hoo, K. J., Sudbury, A. W., and Jaquith, A. R. (2001) "Tangible ROI through secure software engineering," *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4, 2001. A publication of @stake.