Information Security Investment Case Study: The Manufacturing Sector[1]

Summary: Cybersecurity in the Extended Enterprise

Over a period extending from December 2004 to August 2005 we interviewed 13 information security ("InfoSec") and supply chain executives at a Fortune 500 manufacturing firm ("Host") with plants and sales worldwide, members from its electrical and auto BUs, and 14 similar executives and directors at seven of its suppliers. The field study was designed to understand how firms assess and manage information security risk, and the risks the host firm faced as a result of using the IT infrastructure to integrate its supply chain. Below we break out the learnings by theme; here we note the key takeaways (current as of the time of the interviews):

- The host is adopting information security measures that are effective with coping with present threats such as worms/virii, web site hacking, and break-ins. As of the time of the interviews, the host was not considering the InfoSec implications of every new IT-enabled business initiative.

- The host has few critical IT integrations with business partners, leading us to conclude that the host's internal IT infrastructure is at low risk due to the compromise of an extended enterprise partner. We believe there is a good chance that this situation is different today, due to the outsourcing of many core logistics functions in the Auto BUs.

- None of the supply chains of the interviewed suppliers were at risk from internet disruptions. This includes very large to very small suppliers by size. The most noticeable effect from the supplier's point of view would be an impact on customer service due to the unavailability of email.

- With one exception, suppliers had an appropriate level of information security as judged by their cyber-hygiene record (i.e., no virii, break-ins, or website defacements in the past year). Cyberevents at the exception did not

[1] This report was written by Scott Dynes of the Center for Digital Strategies at the Tuck School of Business at Dartmouth College. This work was produced in part with support from the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College, and supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this [site and documents] are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security, the Science and Technology Directorate, the I3P, or Dartmouth College.

compromise their ability to deliver in terms of volume or quality, but were a source of internal cost.

- The host has considerable power to drive increased InfoSec capability in its supply chain by directly asking for capabilities, or merely suggesting by making an InfoSec practices and capabilities questionnaire part of the contract process.

- In comparison with firms interviewed as part of this and similar studies in other sectors, the host is above average in its organizational commitment to and achievement with regard to information security.

- While larger firms tend to have more structured means for managing information security, they are not necessarily "better" at information security as measured by the number of successful attacks.

- Of the InfoSec management paradigms seen during this field study, a "systemic" paradigm used at supplier D was the best at identifying and managing the risk to business continuity from an InfoSec event.

Study Background

Motivation for the Study

Developing and delivering products to market has become progressively more complex. In many industries, the forces driving outsourcing and inter-organizational collaborative product design and innovation also drive the development of complex, increasingly tight relationships with suppliers and customers. Product designers, marketers, and manufacturers are often no longer in the same organization, but form an extended enterprise dedicated to developing and delivering products to market. This extended enterprise can be spread over several organizations in different geographic regions with different cultures and business objectives. Effective collaboration within and across the organizations in this extended enterprise is the key to bringing the right products to market at the right time, both from a design perspective as well as from prosaic supply perspectives.

The internet is the enabling technology for this extended enterprise. Many large companies such as Walmart require suppliers to use the internet for routine purchasing and supply chain planning; others, including GM and HP, exchange detailed product design information over the web with their suppliers around the globe. As a result, many Global 1000 companies have made substantial investments in cybersecurity as part of enabling their extended enterprise. Safely behind hardened firewalls, information and connectivity within these large companies is relatively secure. However, for many smaller firms, many of them key suppliers and customers to large companies, cybersecurity continues to be a substantial concern: routine viruses and cyber failures typically have a disproportionate effect on smaller firms; data and intellectual property storage and protection may not be as sophisticated. As a result of this cybersecurity gap,

nearly every large firm faces risk within their supply chain and extended enterprise. These risks run the range of supply disruptions and delays to theft of shared intellectual property, compromised data integrity, or worse.

We are interested in exploring these risks by examining the dependence on the internet and the drivers of cybersecurity within the context of the extended enterprise. In this study, we hope to examine five broad topics:

- What supply chain risks are organizations exposed to through integration with their suppliers using the internet?
- What drives adoption of cybersecurity by organizations?
- What sorts of cyberattacks are organizations paying attention to?
- What is the limiting factor with respect to tighter integration in the extended enterprise?
- Is there a "cybersecurity gap" between large and small organizations?

Our research approach is to quantify the perception of current cybersecurity-related risks and business opportunities on both sides of a business relationship through a set of interviews. We expect the results to illuminate:

- The level of risk to supply chains from cyberattacks as a result of tighter integration, and
- Mechanisms for mitigating that risk.

These results will be of use both at a practical level, as extended enterprises work to adopt a rational level of cybersecurity, and at the organizational and national levels by serving as an anchor for policy discussions about cybersecurity.

Methods

The host firm ("Host") for this study is a Fortune 500 manufacturing firm with plants and sales worldwide. As part of the study, interviews were conducted with information security and supply chain executives and directors at the host's headquarters and two of its business units (BUs), as well as seven of its direct suppliers (i.e., the supplier's product is core to the product of the host). Host interviews were conducted July 2004 through February 2005. Supplier interviews were conducted December 2004 through August 2005. 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 (e.g., a 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.

Thirteen individuals were interviewed at the host's headquarters and two BUs. 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, interviewees were explicitly told that their responses would be recorded anonymously; during the interview every effort was made to build a high degree of trust with the interviewee.

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 core set of role-dependent 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, seven suppliers agreed to participate in this study. 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 proximate to a few specified geographic locations (purely for ease of travel logistics). This was a "nice-to-have".

At the suppliers we spoke with information security and IT executives and directors, and, where applicable, the account managers of the host's account. For the seven suppliers, fourteen individuals were interviewed. Supplier interviews consisted of one researcher and one to three interviewees. Interviews with five suppliers were conducted in person; the remaining two were conducted by telephone.

In terms of exploring how firms made information security investment decisions, the interview questions for the suppliers 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. Table 1 gives some particulars about the host and the suppliers that were interviewed:

	Product	# of locations	Annual Revenues	Subsidiary?
Host	Conglomerate	many	billions	No
Supplier A	Metal	many	billions	Yes
Supplier B	Logistics Services	many	100 millions	Yes
Supplier C	Metal parts	many	100 millions	Yes
Supplier D	Metal finishing	few	10 millions	No
Supplier E	Metal parts	few	10 millions	No
Supplier F	Printing/Design	few	10 millions	Yes
Supplier G	Metal parts	one	millions	Yes

Table 1: Properties of Interviewed Firms.

Information Security Investment Decisions

While individual firms varied in the details of their approaches to information security, there was a general consensus that their InfoSec investment process was closely reflected by the framework shown in Figure 1, which posits that InfoSec directors first collect information on which they base decisions about their organizations' vulnerabilities and risks and then prioritize their mitigation efforts.

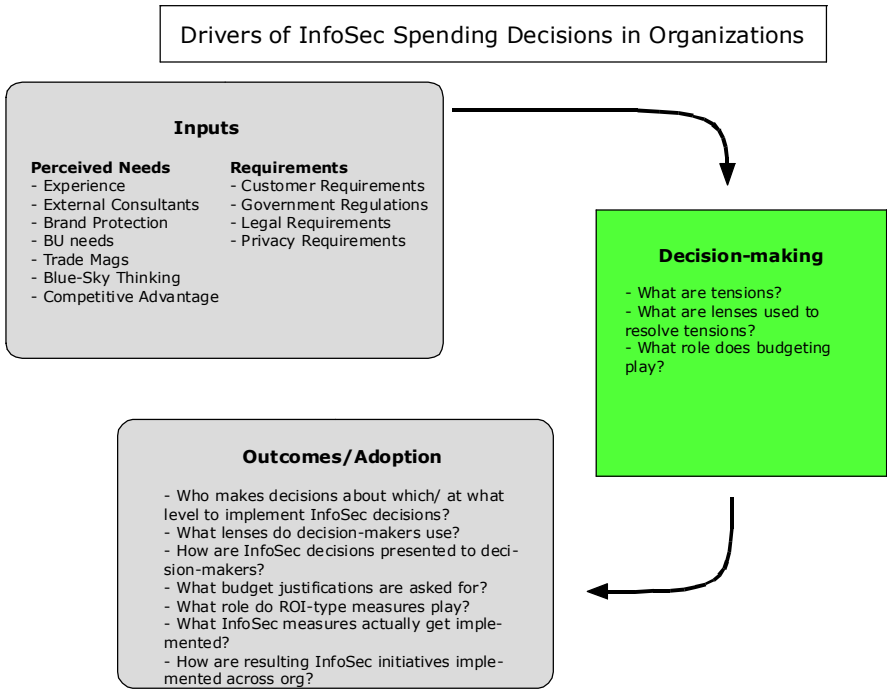

Figure 1. A possible framework showing how InfoSec managers approach thinking about information security managers decide on InfoSec investments. This framework was used as a basis for discussion about the accuracy of the framework and InfoSec investment decision activities.

Lastly, InfoSec directors work to implement these initiatives within the organization, which may or may not require interaction with other organizational entities. While we will organize this section around this framework, we must first remark on the range of organizational structures found during this study.

Firm Organizational Structures

Generally, larger firms had a more formal organizational structure than small companies. Most firms took a "gut-check" approach to evaluating risk and as a result tended to be reactive, focusing on known threats. Most firms also took a local view of what they needed to protect.

There is a clear pattern of larger companies having more structured approaches to InfoSec risk and remediation, as is clear from Table 2. The large companies that were interviewed all use a committee as a mechanism to coordinate InfoSec efforts at the corporate and BU level; the authority of this committee differs among organizations.

	Sec. group @ HQ; no BU reps	Sec. group @ HQ w/ reps from BUs	Sec. Group @ BUs; no HQ input	Single person reporting to gen. mgr.	Outsource to consultant
Host HQ		X			
Host Elect BU					
Host Auto BU		Plants fairly autonomous with respect to IT & InfoSec; InfoSec efforts at plants integrated by BU's Sec. Council member.			
Supplier A	X – according to A's corporate parent's Dir. IT		X- according to Dir. Risk mgmt @ supplier A		
Supplier B		X- w/in Supp. B	X – from B's parent's view		
Supplier C			X – from C's parent's view	X – from C's view	
Supplier D				X	
Supplier E				X	
Supplier F				X	
Supplier G					X

Table 2: Organizational Properties Relating to InfoSec Decisions.

The host has a security committee including the corporate director of information security as well as representatives from each of the firm's BUs. This committee meets regularly to address InfoSec issues raised by its members. The agenda includes issues that are corporate wide, will save money, or need broad support to gain buy-in from a particular

BU's CIO. The agenda is set by its members, who typically are gathering information on issues from their colleagues in the BU and at the plant level. One participant's filter for putting issues on the agenda is whether the issue is a real risk to the business. From an enactment standpoint, the committee acts as the main driver of company-wide initiatives that arise from best practices or from issues raised at meetings that have firm-wide impact. Examples include bringing in white-hat hackers, and dealing with InfoSec implications of legal/regulatory requirements such as Sarbanes-Oxley.

At the BU level there is a fair amount of autonomy from an IT and InfoSec perspective; there is a "high level of trust" around allowing BUs to enable their business. BU representatives use the firm-level security committee as a source of information and a sounding board. There are some issues on which the security committee acts to define firm-wide policies such as wireless access. From a spending standpoint, the committee is able to make smaller purchases (e.g., a firewall) on their own; for larger purchases they need to go before a group consisting of the corporate and BU CIOs.

This organizational structure is largely shared with Supplier B, where information is solicited from and shared between operating units on an ongoing basis. The InfoSec director described their approach to InfoSec investment as "bottom-up". He says that he can make obvious InfoSec investments himself, while larger decisions are referred to a committee consisting of C-level executives and an outside auditor. Supplier B is a wholly-owned BU of another company; at the time of the interview their parent was not active in prescribing InfoSec policies.

Supplier A, also a large company, takes a "top-down" approach to information security. Its corporate parent very clearly lays out a set of InfoSec policies to which its subsidiaries must adhere; individual BUs can adopt more stringent controls. The InfoSec director of the parent's U.S. operations said that BUs try to meet business needs within these guidelines rather than trying to create exceptions. He also made clear that information security is something that happens to employees; he assumes complete responsibility for information security within his organization.

Supplier C is also a wholly-owned subsidiary: the parent firm's IT organization deals mainly with large, corporate-wide issues such as Sarbanes-Oxley, anti-virus, and password policies, and most of the IS/IT/InfoSec operations are managed at the operating unit level. The InfoSec director for supplier C is the source of all information security efforts at his firm; he gets input from his peers at sister companies. He reports directly to the CEO.

Suppliers E and F are small companies and do not have large IT operations. At both companies, the InfoSec Director is the only IT person on staff, and reports directly to the general manager. Supplier G, the smallest supplier, completely outsources their InfoSec efforts to a consulting firm specializing in managing InfoSec for small and medium businesses.

Most of the suppliers are owned by a larger entity (A, B, C, F, G), or own other businesses (E). The level of InfoSec efforts at subsidiaries is often not primarily driven by a corporate parent; the predominant model in this group of firms seems to be the parent providing guidance and assistance for encompassing issues such as Sarbanes-Oxley while allowing a good deal of InfoSec autonomy for subsidiaries. This approach is also seen in the relationship the host has with its BUs, and is present in another business sector we are studying.

Supplier D does not easily fit in the organizational structure outlined above; in every other case the director of information security reports to a business entity that has some level of control over the budget that the InfoSec director can spend, as will be detailed below. At this supplier, the director of information security (also the director of IT), while reporting to the general manager, does not present InfoSec initiatives to the general manager for funding. Supplier D manages information security in a fundamentally different manner than every other interviewed firm; to their InfoSec director an InfoSec initiative and its costs are inseparable from the business process it supports. To him, the framework shown in Figure 1 (which presents information security as an activity separable from a business activity) was nonsensical; he had difficulty thinking about information security outside the context of a business process. Supplier D's approach is discussed in detail below.

Inputs

Interviewees talked about how they gather information about their firm's vulnerabilities and risks. The sources mentioned most often were: personal experience, talking with colleagues, industry magazines, external consultants, and vendors.

Infosec directors at larger firms tended to group inputs in terms of vulnerability, potential cost, and likelihood; these distinctions were not so apparent at small firms. The sources varied by the types of information being gathered. Threats to the firm typically came from conversations with colleagues within the firm, the probable costs to the firm of a successful exploit were a gut estimate, and estimates of the likelihood of a vulnerability being exploited were informed by past experience, industry publications, level of sophistication, and complexity of attack.

From this work, as well as from our studies of the oil refining and health care sectors, it is clear that information sharing among peers was viewed as an important source of information. One InfoSec director described the money he pays to belong to an InfoSec roundtable as the best investment he made in information security; another said he values the real-world experiences of his peers higher than any other source of information. While information-sharing opportunities among InfoSec directors are increasing in some sectors, there is still an opportunity for increased interaction and transparency between firms regarding InfoSec events.

Prioritization/Decision Making and Adoption

With the information in hand, how do InfoSec directors identify and prioritize InfoSec initiatives, and how are these initiatives adopted by their organizations? Broadly, there

were four different paradigms for prioritizing InfoSec initiatives among the eight interviewed firms; these paradigms were amended or trumped by additional factors.

The four paradigms:

The 'Sore Thumb' paradigm. The one example of this was seen at a small manufacturer that is rather independent of IT for its business operations. At this supplier, the director of information security received information about possible threats and best practices through industry publications and two InfoSec groups to which he belonged. The director prioritized his InfoSec efforts based on what was causing him the most pain within his organization. He had to go to the general manager of the firm to get funding for these InfoSec efforts; he was never denied funding by the general manager. This mainly reactive approach provides many opportunities for improvement.

The 'IT Risk' paradigm. Examples of this approach involve some level of implied risk management methodology to rank InfoSec initiatives, with the goal of reducing the risk to IT processes such as database and/or application servers and networks. The information for these efforts typically comes from the director of information security talking with IT managers and staffers within the organization, who relay InfoSec issues they've identified on the job or from the other sources previously described. In the examples seen, the director of information security will prioritize responses based on estimates of the likelihood and cost of a successful attack, and the cost to mitigate the vulnerability. There was a range in how explicit InfoSec directors were in this process; responses ranged from one director who was "conscious of saving money" while titrating risk and cost, to another who was very explicit about estimating the probability and costs associated with mitigating vulnerabilities. None of the directors explicitly talked about "risk management", although most talked about processes that identified consequences and costs, and served to manage risk. Here, if asked about what they were protecting, a director would talk about the network, servers, desktops – in short, devices. InfoSec initiatives here would relate to protecting hardware. This paradigm can be reactive and/or proactive.

The 'Business Risk' paradigm. The key distinction between the 'IT Risk' and this paradigm is that the former looks at risk to IT processes, while this paradigm explicitly looks at how InfoSec risks could impact business processes. Here, if asked about what they were protecting, an InfoSec director would talk about the ERP system, the customer order system, etc. – in short, business processes. InfoSec initiatives here would relate to protecting business continuity. This approach can be reactive and/or proactive.

The 'Systemic' paradigm. The only implementer of this approach was supplier D; this paradigm is sufficiently different so that it cannot be placed on the continuum that encompasses the above strategies. As mentioned earlier, the InfoSec director of supplier D had trouble comprehending the framework that is shown in Figure 1. While he understood and participated in gathering information using the same methods as his peers at other firms, he did not buy into the concept of prioritizing and funding InfoSec

initiatives. To his mind, this spoke of an IT organization that was deciding what needed to be done to enhance information security, and then trying to get buy-in at the firm level, a process which he thought irrational. To him, InfoSec efforts are not an activity separate from business strategy, rather the two are inseparable. As such, as the director of IT for his firm, he thinks of information security at every step of developing an IT process to enable a business strategy. To him 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" InfoSec initiatives that are not developed as part of some business process. This approach leads to his never having to ask for funding for InfoSec initiatives: the budgets he presents for IT efforts do not have InfoSec costs as a separate item, but as part of the overall project. There is another distinction. At every other firm interviewed, the interface between InfoSec and business is a person-to-person or committee-to-committee interface. At supplier D, the interface is internal to this one individual: he only talks business strategy to those above him, and talks technical strategy (along with how this impacts the business strategy) to those in his IT organization. This paradigm is proactive.

The first three approaches could all be present in an organization; clearly the 'Sore Thumb' approach becomes a tactical response to InfoSec events such as a virus infection. The presence of the 'IT Risk' and 'Business Risk' strategies in firms is more subtle; among the interviewed firms there were examples that were predominantly, but not exclusively one or the other. Outside of this study, interviews with businesses from other sectors do show there are pure examples of each; another of our field studies indicates that moving a firm from 'IT Risk' to 'Business Risk' is possible through an exercise of mapping IT risk to business risk.

Reactive vs. Proactive

One focal issue for this study was whether firms are largely reactive or proactive about information security. With the exception of the 'Sore Thumb' approach, the first three paradigms can be reactive or proactive. Here, reactive means that InfoSec initiatives can come as the result of uncovering already exploited vulnerabilities (e.g. a virus infection due to unpatched software) or by reacting to a request for an additional InfoSec capability, proactive in the sense of anticipating and managing future vulnerabilities now.

As noted before, the 'Sore Thumb' approach is largely reactive – substantive InfoSec efforts occur only after the organization is feeling pain. The 'Systemic' paradigm is proactive – InfoSec efforts are based on a reasoned approach to identifying and managing the risks associated with utilizing IT to support a business process during the design.

The interviewed firms spanned the reactive-proactive spectrum. The interviewed firms felt that internally they had a reactive InfoSec posture; one went so far as to say that they felt been "historically very fortunate" with InfoSec events. While most thought themselves reactive, their activities indicate that there are different standards. Some of the larger firms were taking proactive steps with regards to developing policies for their wireless networks. The firms that were the most proactive were not necessarily the biggest or the most dependent on IT; the firms that were the most reactive were not necessarily the smallest, but did tend to be the least IT dependent.

Adoption
As discussed above, in most firms (with the exception of supplier D) the InfoSec director must interact with business managers (typically the CIO or general manager) to obtain funding for InfoSec initiatives. Interviews show that commonly-accepted best practices, such as anti-virus suites, are not controversial and are always approved; essentially the InfoSec director has the ability to just invest in certain "baseline" technologies. For InfoSec efforts beyond this baseline, they would have to make a business case before a higher group of decision-makers (business managers).

The formality of this request depends on company size: supplier A's director would have to develop a business plan including a quantitative financial model of the return on investment. Most other suppliers adopt a less formal approach, discussing the potential costs to the business of the vulnerabilities being addressed, and the costs of reducing the vulnerabilities or mitigating the outcomes. These arguments are a more qualitative approach to return on investment (ROI), reflecting the "gut-level" assessment of risk due to the lack of certainty around costs and probabilities. None of the firms had an explicit risk-analysis methodology they used to rank possible investments, as is the case with certain financial firms.

The reception of business managers to the InfoSec initiatives presented varied. At some firms, business managers saw little value in InfoSec initiatives beyond the baseline; at other firms, they were more receptive. Those organizations where the reception was better tended to be those that had more reactive approaches to InfoSec (so the requests were likely part of fixing an existing issue or implementing an existing best practice) or were more dependent on IT.

ROI
One issue that is currently being discussed is the role ROI should play in InfoSec investment decisions. Several articles (e.g. [Gor2002], [Gor2006]) have made the case that information security investment decisions can and should be based on ROI considerations. In a quantitative form this would require that there exists substantive knowledge of the probabilities of successful attacks, and the costs of the resulting damage. Others, including directors of information security at Fortune 500 companies and their correspondents, argue that these probabilities are currently unknown, and as a result quantitative ROI is not possible. One indicator that such probabilities and costs are reliably known is when inclusive cyberinsurance becomes widely available.

The analogy to insurance is clear: an investment in information security is an investment to reduce the risk of a bad occurrence. This is one reason why we think ROI arguments are not an effective route to making a case for investment in information security. A better approach to a business case may be to look at InfoSec investments as an investment in business continuity. This approach is resonating with business managers at a firm that is part of another field study, and has been a theme that is emerging in information security workshops and conferences.

None of the interviewed companies utilized quantitative ROI models except in cases where the numbers and arguments were clearly obvious. Most utilized a more quantitative approach in looking at the probabilities of successful attacks and their resulting costs, not as part of an ROI calculation, but as part of their InfoSec investment decision process.

Additional factors

While InfoSec directors could easily invest in baseline InfoSec efforts, and had a more difficult time getting additional InfoSec efforts funded, there were other factors that drove firms to invest in information security. Chief among these were customer requests, business requirements, and government regulations.

In general, firms said they are very responsive to requests from customers. The host and a few suppliers received requests from potential and current customers to either complete a questionnaire about their InfoSec practices, or for specific InfoSec processes, such as the use of particular protocols. The customers that were requesting this information ranged from airplane manufacturers to oil refiners to heavy trucking companies.

Firms said they treat such InfoSec questionnaires as qualification documents, meaning that they will make sure they can answer in the affirmative the information security-related questions. With one exception, the firms that received these questionnaires felt that their current InfoSec practices were sufficient to meet the requirements set forth in these questionnaires; the exception felt that the questionnaire resulted in a beneficial increase in the firm's information security. While none of the interviewed firms believed they lost business as a result of their InfoSec practices, a conversation with a director of information security at an oil refiner reveals that companies do base supplier decisions on the responses to these questionnaires.

The responsiveness of firms of all sizes to customers' requests for general InfoSec practices, and for specific InfoSec processes indicates that firms have a considerable amount of leverage over the InfoSec practices of their suppliers. While firms are apparently able to exert some level of control over the risks faced from using IT to manage their extended enterprise, very few of the interviewed firms have any InfoSec requirements of their suppliers.

Another important driver of additional levels of information security, among the top three drivers for the firms interviewed, are government regulations. One interviewee from the host firm noted that regulations drive adoption more than perceived needs, and drive priorities as well. As has been noted previously [Dyn04], while regulations may be an effective driver for additional InfoSec practices, none of the firms felt that the additional practices were particularly effective. One InfoSec director summed it up by saying that regulations changed the focus from "important things" to "not-so-important things". As an example, rather than focusing on business continuity, he had to focus on the security of the computer center door.

Perception of Information Security Benefit in the Marketplace
There was no consensus about whether information security was a cost, qualifier, or competitive advantage. One supplier thought that it was a cost that was becoming a qualification; another supplier thought that information security was a competitive advantage in the sense that customers felt more comfortable doing business with them as a result of their focus on information security.

Outcomes
The metric used to ascertain the efficacy of InfoSec efforts was the number of cyberevents suffered by the firm in the 12 months previous to the interview. Cyberevents included virus/worm infections, web site defacement, and break-ins. Of the firms interviewed, only the host (web site defacement) and supplier E (virus/worm) had suffered cyberevents, as shown in Table 3.[2] This suggests that the majority of firms have adopted sufficient levels of information security to mitigate these threats facing internal systems. In other words, most of the interviewed companies, at the time of the interview, had in place information security methods that were effective at preventing the best-known threats.

	Virus/Worm	Break-in	Web Site Defacement	# of InfoSec methods used (out of 16)
Host	N (Y in 2003)	N	Y	10
Supplier A	N	N	N	?
Supplier B	N (Y in 2003)	N	N	12
Supplier C	N	N	N	10-11
Supplier D	N	N	N	8-9
Supplier E	Y	N	N	7
Supplier F	N	N	N	6
Supplier G	N	N	n.a.	8

Table 3. Reported cyberevents during the 12 months prior to interview.

What Table 3 does not show is how the methods came to be. Were these methods put in place in reaction to some earlier event at the firm, or knowledge of similar events at other firms, or some other mechanism?

[2] We note that there is the possibility that a firm may be unaware of cyberevents that may have occurred at other firms in its extended enterprise.

Risks to Extended Enterprises From Reliance on the Information Infrastructure

In this study, two types of risks were explored in detail: risks to the host's internal IT systems and information as a result of tight integration with supply chain partner's information infrastructure, and risks to the host'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), 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 InfoSec director 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 then 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	Y	Y
Supplier D	N	N	N	Y
Supplier E	N	N	N	Y
Supplier F	N	N	N	Y
Supplier G	Y	N	N	Y

Table 4: Types of connections firms utilize with their business partners

As shown in Table 4, of the suppliers, A and B used EDI and email to communicate with their business partners (customers and supply chain), but did not utilize VPN or web-based applications. Supplier F used only email; and G used email with a single supplier having access to information stored in a database using a web-based interface.

The interviews uncovered no existing examples of tight integration between the host's and suppliers' core IT systems. Although there were a few examples of suppliers that had VPN access to specific applications and servers of the host, there appears to be little risk to the host's IT systems as a result of using the IT infrastructure to integrate the extended enterprise.

This will change; one of the host's initiatives discussed during an interview was the outsourcing of core logistics functions to a third-party logistics provider (3PLP). This outsourcing will require much tighter IT integration between the host's material

requirements planning systems and the 3PLP's internal systems. This level of integration has the potential to subject the host's internal systems and information to the weaknesses of the 3PLP's InfoSec processes.

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 5, which shows the division of the types of communications used to order their supplies at the time of the interview.

	Web App	EDI	email	Phone/Fax
Host BU #1	(20% -> 100%)	(40%)	0%	12%
Host BU #2	0%	0%	0%	~23%
Supplier A	0%	0%	0%	100%
Supplier B	0%	60%	0%	40%
Supplier C	0%	0-30%	0%	70-100%
Supplier D	0%	0%	>50%	<50%
Supplier E	0%	0%	0%	100%
Supplier F	0%	0%	80%	20%
Supplier G	0%	?	?	?

Table 5: Percentage of Interviewed Firm's Supply Chain Order Communication by Connection Type

Among the interviewed entities the host's business units (BUs) were the largest user of the internet for supply chain management; the use of web applications and EDI accounted for over 75% 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, used only phone and fax to order their supplies. Supplier B relied on EDI for 60% of its supply chain communications, with the

remainder being phone or fax. Supplier F used email to order 80% of their supplies; they followed up both their email and fax orders with hard copies sent by mail.

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[3], 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 a lack of access to the internet is mainly time-dependent: the longer the outage, the greater the effect. Table 6 combines the reported impact that outages of various durations would have on the supply chains of the interviewed firms.

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	ASN disruptions	Customer service disruptions; no production disruption		
Supplier D	No impact	Fax ASNs, phone/fax suppliers, no production disruption		
Supplier E	No impact	No impact	No impact	No impact
Supplier F	No impact	No impact	No impact	No impact
Supplier G	No impact	No impact	No impact	No impact

Table 6. Reported impact of an internet outage of various durations on the supply chains and customers of interviewed entities.

[3] At the host, the largest suppliers to some plants are other host plants.

There were several viewpoints expressed during interviews at the host on 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 was 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) was noticed, and was a factor in renewing a supplier's contract. Some executives at the host firm 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.

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 two- to three-day internet outage without difficulty; this interviewee expected that around that point the suppliers would start notifying 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 was 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 this interviewee was using, the custom product requires components with lead times of days: to meet the delivery schedule, it would have to be ordered today.

As for the suppliers interviewed, 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.

For supplier B, while EDI was a very significant part of its 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 F, 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, supplier F revealed that even when they use email for ordering, the email is essentially a follow-up of a phone call; the email is also then 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. One concern for supplier F was customer relations: they like to maintain a close relationship with their customers using email. An internet outage would greatly affect this.

Risk to Supply Chain Continuity

The robustness of supply chains and extended enterprises is an important component 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 F 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 (phone, fax, FedEx) for the internet? At the smaller suppliers (F and G) it seems very possible that they would be able to use the phone and fax for their supply chain communications; supplier G 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 F, the printing and graphic design firm, would also be able to function using the three Fs. They had 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 F exchange designs via email or FTP; email is used to communicate with a remote design location. Supplier F 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 F would be the way they maintain their relationships with their customers.

Supplier A is interesting in that at the time of interview it managed its supply chain using only fax and phone, while it did communicate with its customers, including the host, using EDI and web-based applications (90% of its communications with the host were 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 had 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 had identified this risk to its ability to maintain business operations in the face of an internet outage, and proceeded to take 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 director stated that he would not know how to enter data into the host's internal systems if their intranet were unavailable.

Would the host be able to rely on the three Fs 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 per 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.

However, the lack of ability to run the business as usual does not mean the business will not run. Supply chain directors 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 Fs; these were not explored in a systematic manner. The interviews suggests that none of the interviewed firms had 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.

Conclusions

At a big picture level, one way to interpret these results is that most firms are adopting an appropriate level of information security: the great majority of firms had not experienced a break-in, virus event, or web site defacement in the year prior to the interview. From this standpoint, it would seem that the baseline set of best practices and whatever additional InfoSec processes that were being implemented were adequate for the threat environment that the interviewed firms were facing.

From a business perspective this leads to wondering what the justification is for investing in any additional levels of information security. This was visible in this study, as well as in other field studies we are conducting in other sectors. One such field study is at a niche oil refiner, where we are focusing on information security in the supervisory control and data acquisition (SCADA) systems that are used to run the refinery. In speaking with the vice president of refining about the incentives he perceives to invest in better SCADA information security, his view was, "How will it help me make better oil?"

Often organizations are receptive to increasing information security only after an event – as is the case at a health care organization that is the subject of another field study. This organization was struck very hard by a worm; afterwards they "got religion" and started making plans to increase their baseline level of security. Regarding the transference of such experiences, our vice president of refining said that he would not be motivated to

increase his SCADA security unless a similarly-sized refinery was attacked – he would not, for example, be concerned if an Exxon refinery's SCADA system were attacked.

This study shows that firms are becoming more dependent on the information infrastructure to enable their business processes, but are slow to adopt a commensurate InfoSec risk management approach. We are concerned that firms are not paying enough attention to assuring the availability of the data and applications associated with business processes: essentially, with business continuity. This series of interviews shows that there are approaches to information security that directly address these issues.

Implementing these approaches calls for a much greater level of collaboration between business and InfoSec directors regarding the identification of the core business processes and the information flows and devices that enable those processes. InfoSec and business directors working together to map IT risk to business risk will result in a shared understanding of the risks that face the firm, leading to a reasoned InfoSec investment process. As a result of such a joint IT-business risk mapping exercise, the vice president of refining did come to understand how investment in SCADA security would help him to make better oil through increased resiliency of his firm. By using the leverage he has with his supply chain and asking his suppliers if they are using a similar process, he can also greatly increase the resiliency of his extended enterprise as well.

The host, as well as the other suppliers that participated in this study, have a similar power to influence the resiliency of their supply chains. Although using the information infrastructure to manager the extended enterprise involves risk, there are powerful mechanisms for managing that risk.

References

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

[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.

[Gor2006] Gordon, L. A. and M. P. Loeb, "Budgeting process for information security expenditures," *Communications of the ACM*, **49**, 1, January 2006, p. 121.

[Dyn04] Dynes, Scott, "Information Security and Privacy: At Odds with Speed and Collaboration?" *Thought Leadership Summit on Digital Strategies Publication,* 2004. http://mba.tuck.dartmouth.edu/digital/Programs/CorporateRoundtables/SecurityAndPrivacy/Overview2.pdf (all one line, no spaces).