Chapter 2

EMERGENT RISKS IN CRITICAL INFRASTRUCTURES

Scott Dynes

Abstract Firms cannot function successfully without managing a host of internal and external organizational and process interdependencies. Part of this involves business continuity planning, which directly affects how resilient a firm and its business sector are in the face of disruptions. This paper presents the results of field studies related to information risk management practices in the health care and retail sectors. The studies explore information risk management coordinating signals within and across firms in these sectors as well as the potential effects of cyber disruptions on the firms as stand-alone entities and as part of a critical infrastructure. The health care case study investigates the impact of the Zotob worm on the ability to deliver medical care and treatment. The retail study examines the resilience of certain elements of the food supply chain to cyber disruptions.

Keywords: Information security, emergent risk, health care, grocery retail

1. Introduction

No man is an island, entire of itself... John Donne (1572–1631)

Donne wrote these words while contemplating the responsibilities of individuals in a shared society (*Devotions Upon Emergent Occasions, Meditation XVII*). His words are just as applicable today when contemplating the role of individual actors in critical infrastructures. A critical infrastructure is a composite of various entities (firms) that produce products and/or services. Several market forces are in play so that the ensemble acts in an apparently reliable fashion to provide a critical need. One can think of the resulting good or service as being a quasi-emergent property of the ensemble of firms acting individually to maximize their (economic) utility. These emergent properties are the result of a complex set of interactions involving explicit and implicit coordinating communications as well as the transfer of information and physical goods.

Expanding on the theme of emergent risk requires looking beyond the risks of individual actors. The risk emerges at the level of the ensemble (infrastructure sector) due to a lack of understanding of the interdependencies and the consequences of various supply and information technology (IT) disruptions on the ability of the ensemble to produce the required good or service. Certain frameworks such as supply chain risk (e.g., [2, 7]) support the analysis of risk due to interdependencies. However, this paper focuses primarily on the risk to control mechanisms resulting from their use of the information infrastructure. The approach adopted is not to examine the resilience of the supply chain *per se*, but that of the communications used to coordinate the supply chain.

This paper examines the richness of coordinating signals relating to the resilience of the information infrastructure used to communicate information regarding business processes and the effect of the coordinating signals on business continuity. It investigates how information risk management (IRM) occurs among business participants to produce goods and services. The first hypothesis is that a correlation exists between an entity's dependence on IT and the level of IRM coordinating signals – entities more dependent on the information infrastructure take more steps to manage the risk due to cyber disruptions. The second hypothesis is that richer IRM coordinating signals result in more robust inter-entity business processes.

When examining critical infrastructure protection from an information security or risk perspective, it is also necessary to consider the emergent behavior of the ensemble. Much research has been devoted to IT risk management within individual firms. These firms are best viewed not as monoliths but as an integrated ensemble of agents whose activities are shaped by the economic forces driving the organization and its products. This view can explain why sophisticated organizations view information security as an exercise in IT risk management – appropriately reducing business risk means that the business will probably make more money.

To gain a deeper sense of the issue, it is instructive to view individual businesses and business sectors as a continuum of individual entities with differing levels of coordinating signals. At the highly coordinated end of the continuum is the individual corporation, which has separate departments for production, marketing, human resources, etc. Figure 1 shows a business as a set of individual entities (departments) with highly coordinated activities. Individual entities share information and/or physical goods with other entities in the business. These entities exchange a range of coordinating signals in order to optimize the production of goods and services. In some firms, the coordinating signals are explicitly mapped to enable them to better manage information risk. The emergent risk is reduced due to a decrease in the unknown response of the ensemble to specific disruptions.

At the the other end of the continuum are business sectors or supply chain networks, where the entity of interest is the firm and the coordinating signals are few (Figure 2). Interactions between entities in the sector are based on market forces or possible collaborations; their efforts are actively optimized for

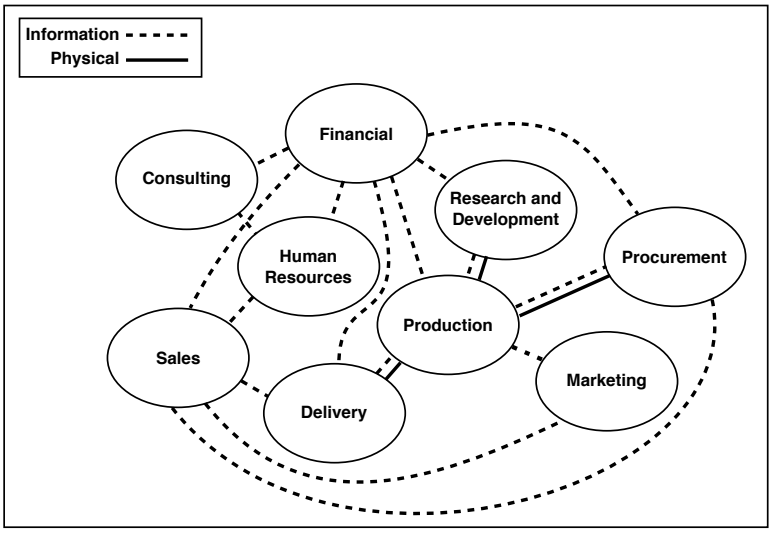

Figure 1. Business sector entities with highly coordinated activities.

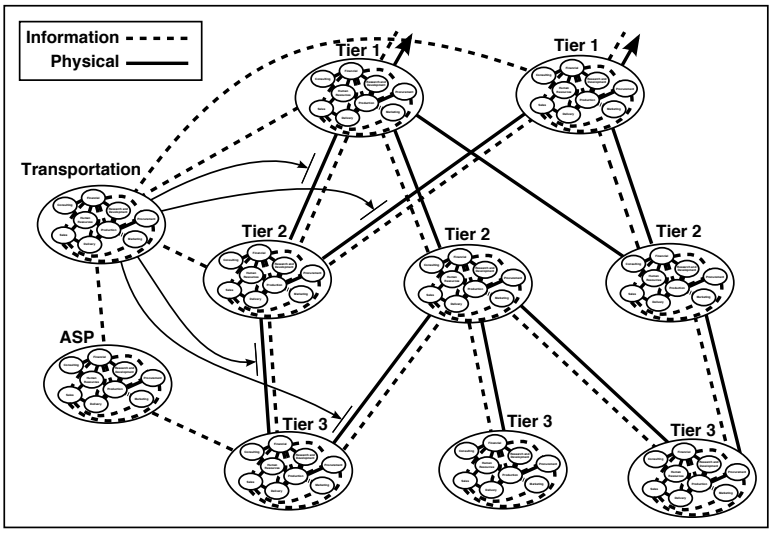

Figure 2. Business sector entities with loosely coordinated activities.

the good of the individual firms. In fact, interactions between entities may be limited to arms-length negotiations for goods and services, in which case IRM coordinating signals will be missing. Many firms are taking a more active approach in managing their referred risk (resulting from inadequate IRM practices at other firms) by requiring potential suppliers to fill out questionnaires about their information security practices [3]. Such assessments and follow-on

gap analyses are examples of high levels of IRM coordinating signals within business sectors.

In between the two extremes are firms that do not pay much attention to information risk and firms (e.g., in the financial sector) that pay a great deal of attention to IRM.

Managing IT risk within firms is a considerable challenge, even when firms tend to be well integrated and have rich coordination mechanisms and management structures that lend themselves to centralized control. In contrast, critical infrastructures such as the energy and retail sectors involve actors that are much less tightly integrated; control and coordination are achieved through market signals or government intervention as in the financial market. The paucity of control and coordination mechanisms at the sector level makes it more of a challenge for individual firms to manage risk outside their firms.

This paper attempts to elucidate IRM coordinating signals among actors in critical infrastructures and to relate them to emergent risks. First, it examines a health care institution that was affected by the Zotob worm; this institution acts like an infrastructure of loosely coupled clinical, business and service (e.g., IT) departments. Next, it analyzes the supply chain network of a retail grocery chain, examining the information and physical supply chains of the retail grocery and dairy suppliers. The paper studies the risk to the supply chain from cyber events and discusses the relationship between supply chain strategies and supply chain resilience.

2. Field Study Method

The field study involved a set of interviews with top-level information security managers, administrators of clinical units and supply chain managers at the participating firms. The interviews were designed to elicit the knowledge and beliefs of the individuals. Security audits were not conducted as part of the study. Interviews were conducted anonymously and every effort was made to build a high degree of trust with the interviewees. The same questions were asked of interviewees at each firm; this facilitated internal consistency checks and the triangulation of different data sources to arrive at robust conclusions [6]. The questions were also crafted to expose tactical and strategic issues regarding information security and its role in maintaining the functional ability of the firms.

Questions asked during the interviews focused on the identification and management of information security risk, in particular, the business continuity risk firms faced as a result of using IT to enable their services and supply chains. These open-ended questions elicited the impact that cyber events had on the ability of the interviewees' divisions to continue to operate. Another focus was determining the risk management culture within the division and the firm as a whole. The topics explored the perceived reliance on technology, the parties responsible for managing risk, and the development of contingency plans for cyber events. The results of these conversations were documented and serve as the basis for the conclusions presented in this paper.

The health care sector study interviewed eighteen individuals from two health care organizations (six clinical divisions, four administrative divisions and four information security (IS) divisions). The retail study interviewed twenty managers and directors from seven firms in the supply chain, ranging from suppliers of raw goods to a retail grocery chain.

3. Field Study Results

This section presents the results of the field studies in the health care and retail sectors. The goals of the field study interviews were to determine the flows of information and physical goods within firms and with their immediate suppliers/customers, and to determine the impact of a loss of communication or local IT capability on their ability to produce goods and services.

The primary questions asked in the field studies were:

- What coordinating information flows exist between entities that might promote effective risk management?
- Is there a correlation between these information flows and the level of resilience in the critical infrastructures? Note that the focus was on the resilience to cyber disruptions, i.e., the ability of the infrastructure to provide goods or services in the face of cyber disruptions.
- What characteristics of individual entities and their coordinating activities lead to this level of resilience? In particular, are there strategies that lead to more robust ensembles? Entities within firms presumably have internal incentives to address the risk they face from relying on the IT infrastructure; it is not clear to what extent coordinating signals between entities at the sector level are driven by concerns about IT risk. As such, the emergent behavior of the sector is likely not optimized for resilience in the face of cyber disruptions.

Several other factors affect the ability of these infrastructures to operate, including the availability of the telephone system and transportation (trucking companies). Therefore, it is important not to lose sight of the profound interdependencies that exist between critical infrastructures.

3.1 Health Care Field Study

The health care organization consists of a main campus housing a hospital and multiple clinics. The organization also operates several hospitals and clinics throughout the geographic region. The main campus provides most of the administrative functions and serves as the ISP for these hospitals and clinics.

The health care organization has physicians on staff as well as independent, affiliated physicians who have admitting privileges. Staff physicians have access to assets such as digital patient records, laboratory results and the scheduling system via the internal network. Affiliated physicians have access through Internet-mediated (web-based) interfaces to these applications. Patients may access a limited amount of information via a web-based interface.

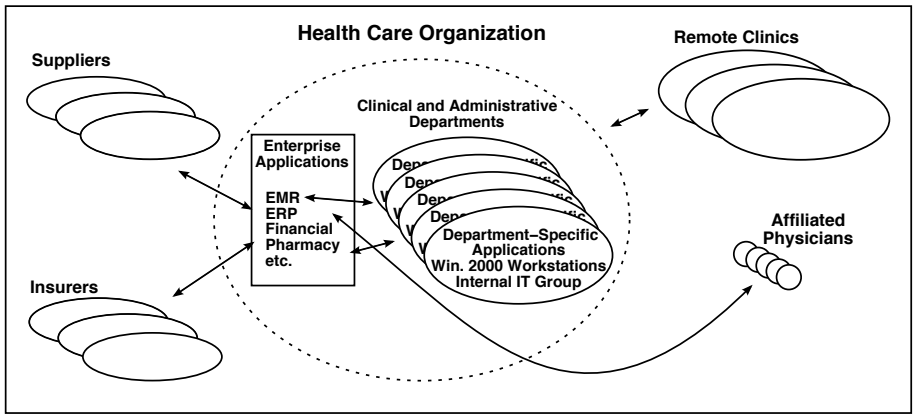

Figure 3. Information structure in the health care organization.

Every department is dependent to some extent on IT. In general, departments use software applications for scheduling, patient tracking and other core functions. The hospital's electronic medical record (EMR) system is a collection of databases and information from many applications presented as a unified whole via an end-user interface. The EMR system contains patient information such as medical charts, radiological images and laboratory test results. Access to the records is available via the Internet for individuals located outside the main campus.

Figure 3 presents an overview of the information structure of the health care organization. Administrative and clinical units use enterprise-level applications, mainly the EMR system along with department-specific applications. Affiliated physicians access the EMR system over the Internet. Affiliated clinics also access enterprise applications over the Internet. The organization has several thousand workstations that primarily run Windows 2000. These are used to access the EMR system, scheduling and other applications that run on Unix machines, and other network-based applications that are internal or external to the hospital.

Information Risk Management Coordinating Signals. The IS and clinical units are loosely connected; many clinical departments have their own small IS units for developing and running applications. A formal liaison program exists between the hospital-level IS department and each individual clinical unit. However, the level of interaction is fairly low; in particular, the hospital-level IS department does not appear to have a substantive understanding of the IT needs of clinical units.

The perceived low level of IRM coordinating signals was reinforced during conversations with the hospital CIO and administrative directors of the various departments. The CIO was the first point of contact for the field study. At the first interview (conducted three months after the Zotob worm event), he

mentioned that the impact of Zotob was felt almost entirely by the IS staff. He believed that few clinical or administrative personnel would recall the event and that its impact on the clinical and administrative departments were minimal. However, most of the clinical and administrative directors felt that the impact was significant. One clinical administrator declared, "All I can tell you is that it was living hell."

The IRM coordinating signals between the departments in the hospital appears to be very low. The response to IT reliability issues was primarily to develop a small departmental IS group rather than to coordinate with the hospital-level IS group. With respect to IRM planning, there is essentially no systemic risk management effort at the hospital level.

Resilience to the Zotob Event. Computing resources at the hospital were infected by the Zotob worm [9] in August 2005. Zotob targeted Windows 2000 machines, attempting to replicate itself by searching for other vulnerable machines on the network. The result was a flood of traffic on the hospital's intranet, resulting in denial-of-service attacks against the hospital's internal servers. The IS units were able to make the EMR system available about an hour into the event. However, most applications and the Internet were down for three days.

Zotob had a significant impact on business processes at the hospital, but there was little to no impact on the ability of the hospital to offer health care. The clinical and administrative units at the hospital were able to provide normal levels of service based on the volume of patients at the time. The principal exception was the radiology unit, which could take images but not deliver them via the intranet to physicians; consequently, the radiation oncology unit was also not operational. The interviewees universally agreed that the quality of care delivered was not affected by the event; however, they did feel that the event significantly increased the chances of providing substandard care.

This is not to say that providing medical care was easy. The Zotob worm had a great impact on operations – physicians did not know which patients they were to see and for what complaints; patients could not be scheduled; some medical procedures and services, especially those relying on radiology, were degraded (e.g., emergency room radiological images were viewed on the machines that took them). The hospital was able to function because of the dedication and flexibility of the staff. Many interviewees said that they simply had to make things happen – not providing medical care was not an option.

Is this resilience due to IRM coordinating signals between the various entities that make up the hospital? The evidence suggests not. Clearly, there was a lack of IRM coordinating signals among entities. The resilience was due to individual initiative and the ethic that medical care had to be provided.

3.2 Retail Grocery Field Study

The retail grocery environment is primarily a supply chain network, reaching from producers to retail grocery stores. The goal of the study was to determine

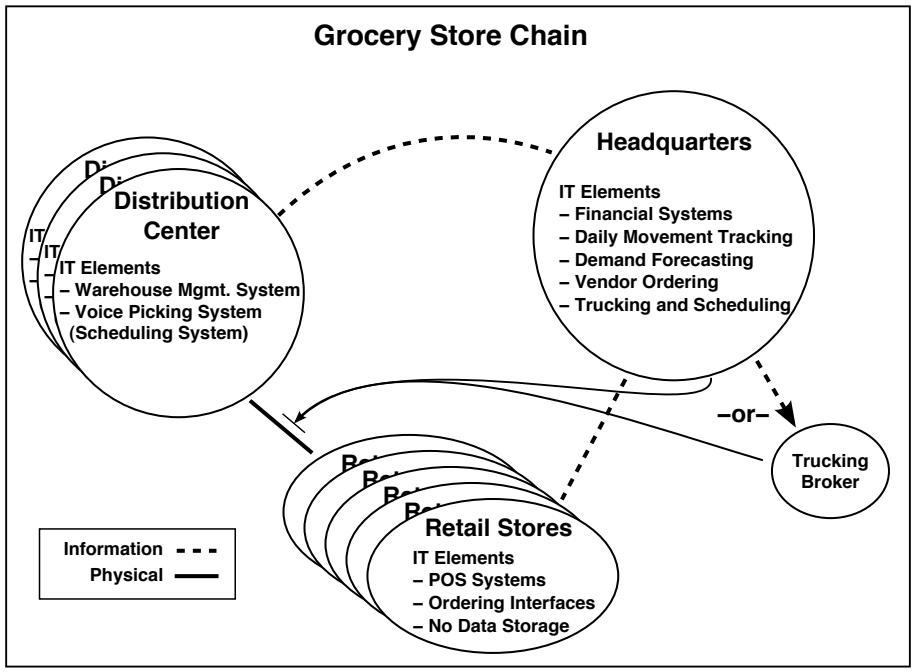

Figure 4. Schematic view of the retail grocery chain.

the resilience of the grocery supply chain to cyber disruptions. The method involved an analysis of the information and grocery supply chains, and the elucidation of IRM coordinating signals and reactions of entities to the signals. The retail grocery field study is different from the health care study in two key respects. First, the interactions of interest are between firms, not departments within the same firm. Second, the view of risk is evaluated proactively, not after a disruption as in the case of the health care field study. This section discusses the situation at the grocery retail chain as well as at a dairy supplier.

Retail Grocery Chain

The subject of the study is a U.S. regional grocery chain with more than 100 stores and in excess of 10,000 employees. The chain is wholly owned by a parent organization, which also owns and operates grocery chains in other regions of the country. The chain is fairly representative of others in the sector with respect to IT, stock replenishment and supply chain activities.

Figure 4 presents a schematic diagram of the retail grocery chain. It includes a headquarters, a distribution center and retail stores. The chain owns a fleet of trucks, but also contracts trucking firms. An important IT component is the scheduling system, a distributed system comprising servers located at the chain's headquarters and at distribution centers.

The use of IT is central to most of the business activities. At every store, point-of-sale data is used to track the movement of goods and create replenishment orders. Store managers of certain departments (e.g., produce) use wireless tablet devices to communicate their orders to headquarters. IT applications at each distribution center manage the inventory at the center. Wireless devices at the distribution centers assist workers in loading pallets; an algorithm optimizes pallet loads so that the heaviest items are placed at the bottom.

Practically all the IT systems are located at the chain's headquarters. There are no servers at store locations; the inventory systems used at the distribution centers are not located at the centers. When a customer swipes a credit or debit card to pay for a purchase at a store, the data is transmitted to the chain's headquarters. Applications that run the sales function contact a bank or clearing agent for approval, the approval is received by the application at the headquarters, which then sends the appropriate commands to the point-of-sale device at the store.

Communication with vendors is done primarily via electronic data interchange (EDI) or web-based applications. Examples include sending data about the daily movement of goods to vendors who manage their own inventories and to trucking firms that schedule deliveries to distribution centers and stores. Because of the dependence on IT, the grocery chain has invested in a backup data center that enables all data and applications to be quickly reconstituted after a disruption at the primary data center. The grocery chain also requires every store to have two ways of obtaining Internet connectivity to the applications running at its headquarters.

Information Risk Management Coordinating Signals. The grocery chain expends considerable effort to optimize its business processes. It has applications that optimize store replenishment orders based on the time of year and anticipated weather (e.g., hurricanes and snowstorms) and others that optimize the placement of products on shelves. There is a certain amount of pressure to automate business processes to "take the cost out of the business."

To support these efforts, the chain has a development group whose responsibility is to create and deploy applications that support business processes. The application development group works closely with the business side to define needs. Part of its task is to assess the levels of availability and redundancy of hardware, networks, disk storage, etc. to provide business continuity; these requirements are passed on to the infrastructure group.

The grocery chain clearly has a high level of IRM coordinating signals. Business managers interact with the application development group. The application development group works on a plan to manage the information risk, which is then made operational. Interviews with the head of the application development group indicated that he was very aware of the retail chain's dependence on the information infrastructure and that he was proactively taking steps to manage risk.

In contrast, there are few, if any, IRM coordinating signals between the grocery chain and its supply network. At the time the interviews were conducted, the grocery chain made no effort to determine IRM practices at its suppliers. Also, no examples of grocery chain and vendor contingency planning for cyber events emerged during the interviews.

Resilience to Cyber Events. Given these internal IRM coordinating signals, we examine the consequences of various cyber events.

- **Communications Events:** It is extremely important that stores can send their orders to the data canter. Each store has a leased line to the chain's headquarters along with a backup modem system that functions as a transparent failover. When a store does have a connectivity outage, a store manager writes the point-of-sale information on a CD or thumbdrive, takes it to a sister store, and uses the other store's resources to place its orders. In the event that the data center does not receive orders from a store, it uses the store's average order to replenish items at the store.

  Interviews with supply managers revealed that if the Internet were to go down, but the grocery chain's internal systems were up, and stores and distribution centers could access systems at the data center, orders to vendors that stocked the distribution centers could be replicated using telephone and fax communications. However, if the Internet outage were to be ongoing, the range of items ordered from vendors would be narrowed over time.

  According to the interviewees, an Internet outage that lasts a minute would pose no problem, nor would one that lasts an hour (no matter which hour). However, a daylong outage would impact purchase orders sent to vendors, the scheduling of deliveries at distribution centers, and orders from stores for perishable items. Orders for less perishable items and non perishable items would not be affected. Thus, the communications interruption would impact daily deliveries to stores; the impact to the business would not be serious.

  However, an outage that lasts two days would be problematic. Distribution centers would not be able to distribute goods or replenish their stocks; customers would certainly notice the difference. An outage lasting three days or longer would result in a chaotic situation, especially with regard to replenishing stocks at distribution centers and stores.

  If EDI transmissions to vendors were to be interrupted, operations would be manual (telephone and fax) for the first few days. If the interruption were to continue, triage would occur and fewer items would be ordered and shipped. The first priority is to ensure that products are on store shelves. Managers believe they could transmit orders to vendors via telephone or fax. However, the resources required for this would be so substantial that little else would be done in the way of business. In any case, it is not

clear if vendors would be able to accept and process the blizzard of phone calls and faxes.

- **Hardware Events:** The grocery chain has two data centers, one located at its headquarters and the other, a backup center, located a few hours drive away. Each data center has a complete data set, but not a complete set of applications. Consequently, if the data center at headquarters were to have a major hardware failure, stores would be required to re-transmit their orders to the backup site.

Dairy Supplier

One goal of the study is to follow the supply chain of a staple food from a producer to the retail chain. The dairy supply chain is a good example. Diary products include milk, cream-based products (butter and cheese), dry milk products as well as casein, which is used in processed foods, adhesives and certain plastics. We primarily focus on liquid dairy products. The supply chain consists of dairy farms, dairy processors that process raw milk from dairy farms, and grocery stores that receive shipments of milk from dairy processors.

Coordinating Signals and Resilience. The grocery chain is the only entity in the dairy supply chain that exhibits IRM coordinating signals. In fact, our conclusion is that the grocery chain has a high level of internal IRM coordinating signals and acts on these signals. However, despite the lack of coordination signals, the evidence suggests that the diary supply chain would be resilient to cyber events, primarily because of its low level of reliance on technology. The dairy processor would suffer from a process control system outage, but many of the core functions can be performed manually.

4. Discussion

What do the field studies say about the first hypotheses in the introduction? This hypothesis states that entities that are more dependent on the information infrastructure take more steps to manage the risk they face from cyber disruptions. The hospital and the retail grocery chain are very dependent on technology; cyber disruptions could severely impact their ability to function. This was seen at the hospital during the Zotob worm event. It is also clear that the grocery chain has much greater levels of IRM coordinating signals. This is evident in the efforts expended by the application development group to understand business needs and translate them to IT-based applications (and likely also review the applications that support business processes).

In contrast, the hospital IS organization made few, if any, attempts to understand the risk. Clearly, the hospital's IS group did take steps to ensure that certain applications would continue to run despite IT failures. This "local" view of their responsibility was evident from interviews with the CIO: the fact that applications were not accessible due to the Zotob infection was not as important to the CIO as the fact that they were running. The great majority

of hospital departments believe information security to be the responsibility of the IS department. While it is not clear if the IS department feels that information security is its responsibility, it is evident that no IRM coordinating signals originate from the IS department. In fact, the only IRM coordinating signals observed at the hospital came from the materials acquisition department. This department developed a paper-based alternative to the usual web-based restocking application, which it distributed to other departments.

The other firms in the field studies are much less dependent on technology. One can argue that the dairy farm's dependence on electricity for refrigeration, automatic milking machines, etc. is a technical dependency. Diary farms are certainly very focused on managing this risk by maintaining redundant generators and storing fuel on site. Nevertheless, the conclusion is that the first hypothesis is false – no correlation exists between an entity's dependence on the information infrastructure and its IRM efforts.

Regarding the second hypothesis – Do increased IRM coordinating signals lead to more robust inter-entity business processes? – the results presented here and elsewhere [1, 4] indicate that the answer is not clear. The retail grocery chain did elect to take some action based on the observed information risk. However, there are several examples where increased coordinating signals have no impact on a firm's IRM efforts. A recent oil refinery study [5] specifically focused on developing IRM coordinating signals. This study utilized the RiskMAP process [8] to expose the refinery's business and IS leaders to the impact IT risk might have on their business. Despite the mapping of IT risk to business risk, the refinery chose not to invest in additional resources to reduce its risk (mainly because it did not perceive a significant threat). The conclusion is that, while IRM coordinating signals are required to increase the resilience of inter-entity business processes to cyber disruptions, they are not sufficient. The sticking point is that CISOs from major firms indicate that decisions regarding the acceptable level of risk are made on the basis of instinct. Therefore, increased IRM coordinating signals would lead to more robust inter-entity business processes only to the extent that a partner entity that makes a security investment sees a threat to its business.

Given the lack of IRM coordinating signals between firms in the field studies, is there emergent risk in these critical infrastructures? Despite the limited nature of the field studies, a recurring theme seen during the interviews was "the will to succeed." The main focus of all the hospital staff throughout the Zotob event was the continuity of patient care. The attitude of the clinical department managers was, "we can't stop, we just have to do what it takes to keep on going." The result was that even though some departments experienced major disruptions, patient care was delivered at normal levels. This is not to say that the worm event did not affect the delivered care. Interviewees indicated that while the care delivered was not compromised, the risk of substandard care was increased. The administrator of the perioperative unit was clear about this, saying "if we have to go backwards and do it (record notes, document procedures, phone for lab results) by hand, it sets us up for failure."

His concerns centered around the execution of operative procedures (worrying about waiting two to three times as long for lab results and wondering if nurses were going to pay attention to the computer screen to make sure an order for blood went through) and the documentation of what happened during the procedures (because of the staff's lack of experience using paper forms).

The will to succeed was also evident in the retail grocery field study. Despite the efforts at redundancy, distribution centers suffer from IT failures, which can have a significant impact on their ability to receive goods and build shipments for individual stores. Nevertheless, the interviews revealed that the distribution centers had not missed a shipment to a store in more than 40 years. The interviewees felt that, because they provide an essential service, they are duty bound to ensure that store shelves are well stocked. A fresh produce vendor also has the same will to succeed.

5. Conclusions

The field studies suggest that the degree of dependence on the information infrastructure within a firm and the steps taken by thse firm to manage information risk are not necessarily coordinated. Also, it is not clear if increased IRM coordinating signals lead to more robust inter-entity business processes. IRM coordinating signals are a requirement for increasing the resilience of inter-entity business processes to cyber disruptions, but they are not sufficient. Therefore, while there may be emergent information risk from poorly understood failure modes, the impact of the risk on the ability of infrastructures to operate would likely be less than expected.

Acknowledgements

This work was partially supported by the Institute for Information Infrastructure Protection (I3P) at Dartmouth College, Hanover, New Hampshire, under Award 2003-TK-TX-0003 from the U.S. Department of Homeland Security.

References

[1] Center for Digital Strategies, Security through Information Risk Management: A Workshop for Information Security Executives, Tuck School of Business, Dartmouth College, Hanover, New Hampshire (mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CISO2007.html) 2007.

[2] M. Christopher and H. Peck, Building the resilient supply chain, *International Journal of Logistics Management*, vol. 15(2), pp. 1–14, 2004.

[3] S. Dynes, Information Security Investment Case Study: The Manufacturing Sector, Technical Report, Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, New Hampshire (mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecManufacturing.pdf), 2006.

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

[5] S. Dynes, E. Goetz and M. Freeman, Cyber security: Are economic incentives adequate? in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 15–27, 2007.

[6] J. Gubrium and J. Holstein, *Handbook of Interview Research: Context and Method*, Sage Publications, Thousand Oaks, California, 2001.

[7] A. Norrman and R. Lindroth, Categorization of supply chain risk management, in *Supply Chain Risk*, C. Brindley (Ed.), Ashgate, Aldershot, United Kingdom, pp. 14–27, 2004.

[8] C. Watters, Analyzing corporate risks with RiskMAP, presented at the *Second Annual I3P Process Control Systems Security Workshop*, 2006.

[9] Wikipedia, Zotob (computer worm) (en.wikipedia.org/wiki/Zotob), 2005.