Chapter 4

INFORMATION RISK MANAGEMENT AND RESILIENCE

Scott Dynes

Abstract Are the levels of information risk management efforts within and between firms correlated with the resilience of the firms to information disruptions? This paper examines this question by considering the results of field studies of information risk management practices at organizations and in supply chains. The organizations investigated differ greatly in the degree of coupling from a general and information risk management standpoint, as well as the levels of internal awareness and activity regarding information risk management. The comparison of the levels of information risk management in the firms and their actual or inferred resilience indicates that a formal information risk management approach is not necessary for resilience in certain sectors.

Keywords: Information risk management, resilience, field studies

1. Introduction

Viewing information security in terms of managing information risk is a compelling idea [2, 4, 6, 8, 9] and with good reason. For the information security practitioner, it provides a wealth of tested risk management frameworks and processes. For a business executive, it relates what is unfamiliar (information security) to a very familiar process (managing business risks), enabling the development of a shared vision of the information-security-related business risk facing a firm.

Is information risk management (IRM) becoming a common information security practice following a lengthy gestation at the concept stage? This would represent a maturing of information security processes, moving away from the *ad hoc* approaches that were commonly used a few years ago [4]. Several processes that support information risk management, such as OCTAVE [1] and RiskMAP [10], have been developed. While these processes are conceptually similar, they differ significantly in terms of the resources required. To address

this issue, OCTAVE comes in three "sizes" ranging from a lightweight small business version to a large enterprise-strength implementation.

We describe RiskMAP to provide a flavor of the information risk management approach. The RiskMAP process works at four levels: (i) top-level business objectives, (ii) business processes that support these objectives, (iii) information flows that support each business process, and (iv) IT assets (hardware and networks) that enable information flows. A ranking takes place at the top level so that the importance of various business objectives are codified as ratios. Dependencies between the levels are exposed by clarifying the impact of the unavailability of a subordinate entity on the success of superordinate entities. For example, how would the unavailability of a database server affect the various information flows? Or, what impact would the loss of an entire business process have on a firm's ability to meet its top-level business objectives?

RiskMAP incorporates four impact categories: (i) no impact, (ii) minor disruption with work-around, (iii) major disruption with work-around, and (iv) cannot accomplish task. Each of these impact categories is codified numerically. The result is a set of matrices that together describe the relative importance of business processes, information flows, etc. on the core objectives of a business. By manipulating these matrices, it is possible to rank the most critical IT devices or to determine the level of exposure of the top-level business objectives.

More concretely, a field study of an oil refinery using RiskMAP identified four mission objectives: "Stay Safe," "Supply Customers Well," "Stay in Compliance" and "Stay Profitable." Each objective was assigned a numeric weight of its relative importance that reflected the shared belief of the CISO and the VP of Refining. The next step enumerated the thirteen business processes that were needed to accomplish these objectives, such as "Offload and Store Crude" and "Perform Fractional Distillation." Evaluating the dependencies between the top-level objectives and the supporting processes resulted in a 4×13 impact matrix. Similarly, the information flows that support business processes are determined. The same categories are used to express the impact of the loss of each information flow on each process and the impact of the loss of each device that enables the information flow.

When using RiskMAP, it is important to determine the correct level of abstraction – the refinery had hundreds of information flows and thousands of devices, which was clearly unworkable. The process was rendered both feasible and valuable by abstracting the information flow and devices into groupings such as "Distillation Control Information." The RiskMAP process resulted in a set of matrices as well as a shared understanding between business executives and IT executives of how IT risk maps to business risk. As a result of using RiskMAP, the VP of Refining started looking at information security investments in a fundamentally different way – not as a sunk cost, but as an investment in business resilience.

It should be clear that the core activities of information risk management are to understand and clarify the sources of business risk, to determine the dependencies of business processes on IT, and to coordinate the organization's

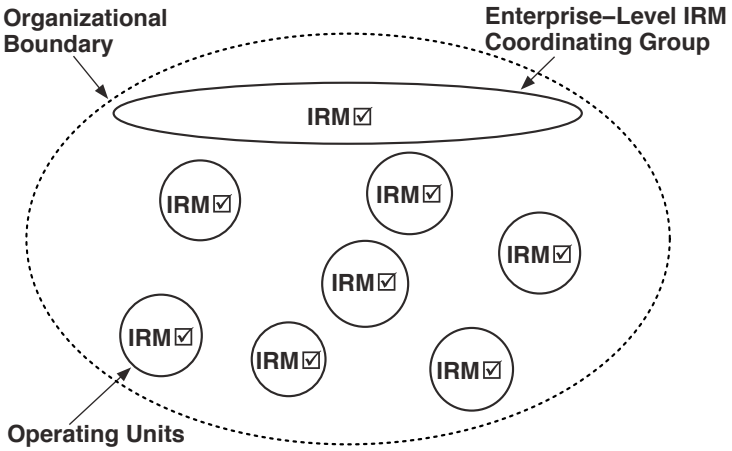

Figure 1. Information risk management process.

response. Clearly, the successful completion of these activities requires a detailed understanding of the firm. In small firms, it is likely that a general manager would have the required breadth and depth of knowledge about the firm. In the case of large firms, individual operating units would have to conduct the information risk management approach internally, and the results would be consolidated at higher organizational levels.

Figure 1 presents a canonical view of information risk management at a firm. Every operating unit conducts an internal information risk management effort; the results are consolidated at higher levels, including the enterprise level. An enterprise-level unit assists individual operating units and manages the information risk management process at the enterprise level, including the enactment of information security and business continuity efforts. Staff in the enterprise-level unit interact with business executives throughout the information risk management process.

This view can be applied to supply chains as well. In this case, the "operating units" are individual firms that are part of a supply chain network. Unlike the highly integrated nature of an individual firm with its rich set of coordinating mechanisms, supply chain entities generally have few coordinating mechanisms that are primarily related to negotiations for goods and services. Supply chains also lack centralized control. The absence of standardized interfirm information risk coordination signals and the lack of a central risk management coordinating unit suggest that supply chain networks would be more fragile to information disruptions than individual firms if, in fact, information risk management promotes resilience.

How do actual information risk management processes compare with the canonical model? What can be said about the efficacy of information risk management in promoting firm and sector resilience? This paper examines how closely information security efforts in firms correspond to the canonical

information risk management model, and the consequences of various supply disruptions and IT disruptions on the production of goods and services in individual firms and in supply networks. To study these questions, we use data collected from field studies of a health care organization, a pharmaceutical firm, and a grocery store chain and its suppliers.

2. Field Studies

The field studies consisted of interviews with security, supply chain executives and managers at the participating large firms; only the general manager was interviewed at small firms. The interviews were anonymous and designed to elicit the knowledge and beliefs of the interviewed individuals; audits or assessments beyond the interviews were not part of the study. Interviewees included top-level managers of information security, administration, clinical units and supply chains. Identical questions were asked of interviewees in the same organization to gauge the internal consistency of information provided in the interviews [7]. The interview questions centered on the identification and management of information security risks, and the resilience of the organization to information infrastructure disruptions.

3. Health Care Field Study

The health care field study focused on an organization comprising a medium-sized hospital and co-located clinics; the organization also operated other hospitals and regional clinics. Several elements of this field study have been presented elsewhere (see, e.g., [3, 5]). The principal hospital houses a data center that runs many applications and databases. Most of the regional clinics depend on the principal hospital for access to the applications and databases, and, in many cases, the Internet.

The hospital uses IT to manage the processes that define the patient experience (e.g., scheduling and billing), the clinician experience (e.g., electronic medical records, documentation, prescriptions, radiological imaging and lab tests), administration (e.g., financial planning and supply management), and the hospital environment (e.g., HVAC). The systems that support these activities are a mix of home-grown systems and commercial, off-the-shelf systems located at the data center of the primary hospital; external applications are provided over the Internet.

The hospital has a central information services (IS) department that manages the data center and applications. This department liaises with other departments and units that are heavy users of IT services. Some larger departments have their own small IS units.

3.1 Information Security Practices

Clinical and administrative unit interviewees considered information security as the responsibility of the IS department. Only one interviewee (from

among interviewees from eleven units) believed information security to be a responsibility shared between his unit and IS. None of the clinical units had considered or developed contingency plans for information infrastructure disruptions. The unit responsible for supporting surgical patients and procedures, which had spent years developing applications to support its business operations, had never considered the consequences of its systems being infected by a virus. The radiology unit, which is very dependent on technology, had no contingency plans, only a list of phone numbers to call in the event of IT disruptions.

Only the materials acquisition unit had developed contingency plans. These included paper-based backup forms and staffing plans for the unit, and paper-based "favorites" lists that identified the supplies commonly ordered by various organizational units.

3.2 Canonical IRM Model and Resilience

The information security practices uncovered in the health care field study differ greatly from the canonical model. In particular, an information risk management process was utilized in only one of the eleven units interviewed. Moreover, an effective information risk management coordinating group did not exist at the enterprise level. Information risk management was not being practiced by the organization at the time of the field study (November 2005 through February 2006).

As it turned out, the field study permitted the direct investigation of the impact of an information infrastructure disruption on the operations of the health care organization. A few months before the field study (August 2005), the hospital was infected by the Zotob worm [11]. The infection flooded the hospital intranet with network traffic, essentially a denial-of-service attack against the internal servers. Normal access to internal applications and the Internet was affected for approximately three days. However, the IS department was able to make the electronic health record system (widely regarded as the most critical application) available just one hour into the event.

While the worm infection had a significant impact on normal business processes at the hospital, there was little to no impact on the ability of the hospital to provide health care to its patients. The administrative and clinical units were able to provide patient care, with the exception of the radiology unit, which could take images but not deliver them to physicians via the intranet; and the radiation oncology unit, which was not operational. The hospital was resilient to the information infrastructure disruption largely because of the corporate culture. Many interviewees held the view that they simply had to make things happen – not providing patient care was not an option.

4. Pharmaceutical Firm Study

The pharmaceutical field study focused on a mid-size pharmaceutical firm that operates production, and research and development sites in several coun-

tries. The field study involved a series of interviews conducted during the first half of 2008.

The pharmaceutical firm is organized into business units along functional and geographic lines; examples include marketing, research and development, enterprise information systems, and U.S. operations. Individual business units have integrative levels of management, and may have local business-unit-specific or function-specific IS organizations. Each business unit has an information officer. At the enterprise level, overarching most business units is a set of enterprise-level information management groups responsible for developing and managing the enterprise architecture, information asset governance policies (e.g., email retention), compliance efforts (e.g., HIPAA and Sarbanes-Oxley) and enterprise-level information risk management. An enterprise-level information infrastructure (EII) group maintains the firm's networks and data centers, and manages enterprise-wide applications such as the enterprise resource planning (ERP) system, which is used across the enterprise. Manufacturing and distribution operations are highly dependent on the ERP system as well as on plant-level applications, including process control systems.

4.1 Information Security Practices

Each business unit has internal information risk management efforts that interact with other business units as necessary. The enterprise-level information risk management group (EIRM) works to understand information risk at the edges of the firm and to manage information risks that exist at the enterprise level.

The enterprise information infrastructure (EII) group views IT risk primarily from a traditional business continuity and disaster recovery perspective. EII approaches IT risk management as a partnership with application owners and users, viewing itself as a supplier of infrastructure but dependent on various application group partners in business units to work with internal users to determine the proper level of disaster recovery and business continuity efforts for each application. EII is responsible for business continuity and disaster recovery for enterprise-wide applications such as email. EII exercises disaster recovery plans twice a year for important IT-backed business processes. EII relies on EIRM for an overall enterprise-level risk assessment and vulnerability management plan; however, EII operationalizes elements of this plan.

In the manufacturing organization, information risk management occurs at the plant and enterprise levels. Internally, the manufacturing IT group sets up and manages information security processes on the applications it owns, whether the applications are located at distant plants (e.g., process automation and control systems) or housed in the corporate data center (e.g., warehouse management systems and portions of the ERP system), where they collaborate with enterprise-level groups (EII and EIRM). EII and EIRM also provide the manufacturing IT group with advice and guidance related to information risk management efforts.

The starting point is to identify applications that are critical to the business processes related to making products, including process control systems and intellectual property management systems. The IT group works with application owners to determine the criticality of the applications and to develop business continuity plans. Business continuity plans for critical applications are exercised at least once a year; plant-level IT managers may exercise certain plans more frequently. Each plant runs a yearly "drawbridge" exercise in which the loss of the connection between the plant and the corporate data center is simulated to provide assurances that the plant can still manufacture product.

The EIRM group arose from the realization that, while every level of the organization should identify and manage information risk, local information risk management efforts were not integrated well at the corporate level. Also, while local initiatives might be effective at managing local risk, it was not clear that they would be effective at managing enterprise-level risk. The EIRM group determines enterprise risk by gathering information risks from across the enterprise and looking for common issues that raise the risks from a local concern to an enterprise-level concern. EIRM finds the common issues by bringing together IT managers who are tasked with canvassing their business units and identifying the risks to critical information processes and assets. Discussion groups are organized in which IT managers identify uncovered risks and share information risk management challenges and best practices. The results are used with other inputs (e.g., results from audits and assessments, other enterprise risk management efforts, external threat trends, and industry and regulatory trends) to generate a list of enterprise information risks. Once the list of risks and recommendations is developed, it is put before a governance board for approval. The approved document is provided to the CIO staff, who use the recommendations in deciding how to manage information risk.

4.2 Canonical IRM Model and Resilience

Based on the interviews, business units at most hierarchical levels in the enterprise are managing information risk. A strong enterprise-level group exists to identify and communicate information risk management issues to the various business units. In general, the firm's information security practices correspond very closely to the canonical model.

How might information disruptions affect the ability of the firm to manufacture and ship product? Unlike the hospital field study, no specific instances of information infrastructure disruptions were mentioned during the interviews. Consequently, resilience is inferred from the interview data.

First, we consider the raw materials used by the firm. The ERP system manages the supply chain operations. Consequently, it is important that the ERP system be functional and that the corporate headquarters and plants can communicate via the Internet. The firm has business continuity plans for its ERP. Also, some plants maintain redundant Internet connections to the corporate data center.

Individual manufacturing plants can function without the ERP system because they operate their process automation and control systems internally. In fact, the manufacturing plants would likely be able to make product for several days without access to the ERP system. The loss of the process automation and control systems internal to plants would have varying levels of impact depending on the type of plant (e.g., manufacturing or distribution). A process control system outage at a manufacturing plant could cause the product to be out of specifications, rendering the entire production batch worthless. As a result, the plant would be shut down until the process control system becomes functional. This is the reason why manufacturing process control networks are segregated from other networks.

Due to the nature of the pharmaceutical business, the firm is keenly aware that an interruption in the supply of certain products would potentially jeopardize human lives; as a result, the firm maintains a safety stock of certain products. The size of this safety stock depends on demand and production timelines. Products that require months to manufacture generally have substantial safety stocks.

It is impossible to accurately assess the resilience of the firm to information disruptions. However, the firm appears to be well-prepared for IT disruptions because the manufacturing side has a strong business continuity process in place, business units have continuity and disaster recovery plans that are exercised (including "drawbridge" exercises), and safety stocks are maintained.

5. Grocery Field Study

The grocery field study focused on a retail food supply chain stretching from producers of raw ingredients to grocery stores. The results of interviews with individuals from eight firms that play different roles in the food supply chain are presented. The firms include a regional grocery chain with individual grocery stores, providers of fresh produce, canned goods, and a liquid dairy processor with two dairy farms.

5.1 Grocery Store Chain

The grocery chain is a U.S. regional chain with more than one hundred stores and employing tens of thousands of associates. This firm is fairly representative of other grocery store chains from the point of view of data processing, replenishment and supply chain activities.

IT is central to the business activities of the grocery chain. Point-of-sale (PoS) data are used to track the movement of goods at stores; the movement data is used by the grocery chain's distribution centers and direct-to-store vendors to restock most items. Credit card and debit card data are exchanged with banks to complete transactions. IT applications manage the inventories at distribution centers; Internet applications help schedule vendor deliveries to the distribution centers and replenishment deliveries to stores.

Most IT systems are located at the data center at the grocery chain's headquarters. No servers are maintained at store locations; PoS and credit card devices connect directly to the grocery chain's data center. Similarly, the inventory systems used by the distribution centers are also located at the data center. Communications with the grocery chain's vendors are done primarily via electronic data interchange (EDI) transactions or web-based applications. Examples include sending data about the movement of goods to vendors who manage their own inventories at the host's distribution centers, and trucking firms who make appointments to deliver goods to distribution centers. The grocery chain has invested in a backup data center and each store has redundant connectivity to applications running at the grocery chain's data center.

Information security is handled primarily by an internal business application development group. This group works with business managers to understand the business needs for applications, including the level of redundancy and business continuity plans. The grocery chain's infrastructure group develops the needed infrastructure.

Everything stops when stores cannot communicate with the grocery chain's data center (or its backup). To manage this risk, each store has a leased line to the data center along with a backup modem system as a transparent failover. If both fail, contingency plans include taking PoS data to a sister store and placing orders from that location. When a store cannot send data, managers at headquarters use the store's average order as its replenishment order. Redundant Internet connections exist between the distribution centers and the main data center; the distribution center we visited had multiple electric power supply sources.

Few, if any, information risk management coordinating signals are exchanged between the grocery chain and its supply network. At the time of the interviews, the chain made no effort to assess information risk management practices at its suppliers. Moreover, no examples of contingency planning between the grocery chain and vendors emerged during the interviews.

The resilience of the grocery chain to IT disruptions was discussed at length. The head of the applications development group spoke of the firm as providing an "essential service." Workers at the grocery chain's headquarters and distribution centers exhibit a high level of dedication to ensuring that food is always on store shelves. If the Internet went down but the grocery chain's internal systems were operational and the stores and distribution centers could access systems at the chain's data center, supply managers believed that they could replicate orders for vendors (who supply goods to the distribution centers) using phone and fax. Ongoing Internet troubles would result in the range of items ordered from vendors to be narrowed over time. The impact of communications outages between the grocery chain headquarters and stores, distribution centers and vendors varies with duration. A one-day outage would affect deliveries to stores, but not have a serious business impact. A two-day outage would impact the replenishment of stores and the restocking of distribution centers. However, when discussing communications outages, grocery managers said they "would

wrestle the problem to the ground." One manager said that his distribution center had not missed a store replenishment order in more than 40 years.

From an information risk management perspective, there is no evidence that the grocery chain has information risk management efforts at its edges. However, there is a central group that coordinates an effective organization-level information risk management effort. Thus, the grocery chain has a poor fit with the canonical model.

5.2 Fresh Produce Vendor

The fresh produce vendor has a multi-region presence covering retail groceries and institutional food settings (e.g., hotels and fast food restaurants). The vendor owns and operates packing plants that clean, mix and bag harvested produce; in addition, it operates several distribution and cross-docking facilities. The vendor has long-term exclusive contracts with fresh produce growers. Most of its orders (including the grocery chain's orders) are received via EDI and are processed by the vendor's order management system. The produce to fill an order is shipped (one day after the order is placed) from a production facility to a cross-docking facility and, from there, to the grocer's distribution center.

Fax or email is used if the vendor is unable to send or receive EDI transmissions. If the Internet is down, the vendor would likely ship an estimated order. The vendor also may have to revert to manually scheduling trucks to ship orders, which would be very challenging and would require additional resources. The resulting slowdown would give rise to delays at the shipping dock. Also, deliveries would be refused because trucks would miss their appointments.

The fresh produce vendor does not have firm-wide information risk management and business continuity planning efforts. It does not fit the canonical model at all.

5.3 Canned Goods Vendor

The canned goods vendor owns production and distribution facilities. Orders from stores are sent via EDI and phone; the firm also has a vendor-managed inventory sales channel. At the time of the interview all supplies were ordered by fax or phone; however, the vendor did plan to move supplier ordering to web-based EDI. EDI orders from customers are entered into the vendor's enterprise resource planning system. For store-based orders, this includes the items and their volumes; for the vendor-managed inventory channel, this includes the inventory and movement of goods at the customer's distribution center. An order is then computed based on the safety stock and other factors. In the case of the vendor-managed inventory, safety stocks range from a little less than a week to two weeks. Once the order (direct or calculated) is in hand, the ERP system places an order for shipping with a third-party trucking vendor, who arranges shipping, makes an appointment at the grocery chain's distribution center and then notifies the canned goods vendor that shipping has been ar-

ranged. The canned goods vendor then sends an EDI to its warehouse with the order and shipping arrangements; the order is picked up, loaded and shipped. The order-to-ship cycle is two days.

Customers are expected to fax in their orders if EDI communications were to fail. The vendor could handle the increased volume of faxes for about a week; additional staff would be hired if there is any indication that the EDI outage would last longer. The vendor would communicate with its warehouses via email and send documents via FedEx. Also, it has a comprehensive contingency plan is in place with a transport vendor to communicate shipping needs via fax. The vendor would not be able to service vendor-managed inventory customers for outages lasting more than one week.

The vendor has gone through an enterprise-wide contingency planning effort; this arose from an initiative spearheaded by the vendor's global crisis committee. Portions of the resulting business continuity plan are exercised periodically. These plans were used during a three-day power outage at the order management office, during which time the vendor did not miss a single shipment.

5.4 Dairy Sector

The dairy sector study attempts to examine information risk in the supply chain network of liquid dairy products. The supply chain network includes suppliers to dairy farms, the dairy farms themselves, dairy processors and grocery stores.

Dairy farms revolve around the cows that produce about a hundred pounds of milk in two milkings per day. The production drops considerably when cows miss even a single milking. As a result, dairy farmers take steps to assure a reliable supply of electricity for running the milking machines and for refrigerating the raw milk until it is picked up by the milk processor. Electricity is also needed to run water pumps, lighting and fans.

One small farm that was studied maintains (and periodically tests) two backup generators with six weeks supply of fuel. A larger farm maintains multiple backup generators, each of which uses a different fuel (e.g., gasoline and propane). Dairy farms also require feed mix ingredients, water, drugs and cleaning agents. Safety stocks of feed components at the small farm ranged from one week to a month; the larger farm stored enough feed for one year. Some supplies (e.g., certain feed components and sawdust for bedding) are delivered to the farm automatically; the remaining supplies are ordered by phone.

The amount of information risk at the dairy farms is small, but not zero. Technology is used to track the milk output of cows (for optimizing milk production) and to develop feed rations from various grains, hay, alfalfa, etc. The software programs run on local computers; Internet connectivity does not play a role in core dairy processes. Neither dairy farm had information risk management efforts.

The dairy processor interviewed in the study collects raw milk from several local dairy farms. Upon arriving at the processing plant, the raw milk is tested

for bacteria and other impurities. If the raw milk is accepted, it is pasteurized, processed and packaged as various types of milk (e.g., low fat milk) and shipped to stores. Orders from customers are communicated to the processor via an order-processing application hosted at the headquarters of the dairy processor's parent firm. Workers at the dairy processor pick and load the orders onto a truck, which is then dispatched. Orders from stores for liquid dairy products are handled via telephone.

There was no indication of internal information risk management activities or of conversations with headquarters and suppliers of packaging materials on the subject of information risk. The laboratory equipment and control systems for processing raw milk are run on set of computers that have no need for Internet access; a UPS system is available for backup power for twelve hours. In the event of an emergency, a local firm is contracted to deliver a diesel generator within two hours for powering all the plant machinery and refrigeration systems. The dairy processor relies on the Internet to receive shipping orders for stores. The processor maintains three T-1 lines for network communications: one for general networking, one specifically to communicate with the order-processing application, and a spare. If Internet connectivity is interrupted, requests from the order-processing application would be received by fax. If the order-processing system is down, the dairy processor would send the previous day's order. The evidence suggests that operations would degrade gracefully if the laboratory computers and process control system go down – low fat milk might not be produced, but it appears likely that pasteurized whole milk would be available.

Dairy section managers at four grocery stores belonging to different chains were also interviewed. The four stores have at least two common vendors of liquid dairy products and orders to the vendors are communicated via telephone. The dairy sections have milk products on display and additional stock in reserve. Replenishment orders are computed manually based on the daily movement and remaining stock, or with the assistance of a software application running at the store. Stock and replenishment orders are sized to have just enough product on hand until the next delivery to maintain product freshness and reduce waste. Safety stock ranged from a few cases (with four one-gallon containers per case) to enough product to cover sales for two or three days. The managers said that it was unusual to run out of stock; however, if it did happen, a special delivery order would be placed with the vendor or stock would be obtained from a sister store. The interviews indicated that vendors have never run out of milk.

5.5 Canonical IRM Model and Resilience

The grocery supply network is an ensemble of loosely connected entities. Some of the entities have effective information risk management efforts; however, no network-level body is in place to coordinate or integrate information risk management efforts. Thus, information security efforts in the grocery supply network have a poor fit with the canonical model.

Table 1. Level of information risk management efforts.

Field Study	**IRM at Edge**	**Central Coordination**
Health Care	Individual	Low
Pharmaceutical	Systemic	High
Grocery Chain	None	High
Dairy Sector	Individual	None

That said, the sector does seem resilient to short-term IT and communication disruptions. This is because safety stocks are kept in stores and at the main distribution centers, stores and vendors quickly adopt work-arounds or continue to make product and deliveries based on past data, and the entities generally have a "wrestle the problem to the ground" culture.

Prolonged IT disruptions in the grocery sector result in a graceful degradation of functionality. Sugar-free chocolate ice cream cones with sprinkles may not be on the shelves after a weeklong outage, but milk and other staples would be available as usual. It is important to note that the demand may be much higher than normal during outages, possibly due to the perception that the supply chain network has failed. Public awareness campaigns and rationing may be needed in such situations. Also, as noted in several studies, transportation is often the principal challenge during outages.

6. Discussion

Information security efforts at the field study entities ranged from disparate efforts to systematic efforts with strong levels of integration. Table 1 shows the level of information risk management efforts in individual entities and the level of central communication and coordination. An "individual" entry in the table means that individual entities might manage information risk; "systemic" means that information risk management efforts are expected by the firm.

Not one firm interviewed in the field study was of the view that it would cease to function shortly after the onset of an information infrastructure disruption; this includes a disruption to the integrated food supply chain.

Based on the lack of an effective information risk management effort and organizational complexity, the hospital appears to be the least likely to continue to function in the event of a disruption; however, it demonstrated that it could indeed function during a major IT disruption. The pharmaceutical firm has a robust information risk management effort in place; the level of planning and the exercising of contingency plans indicate that IT disruptions would likely not affect the firm's ability to manufacture or distribute products. The grocery chain has also actively investigated its IT-based business risk. The challenge is

to devise processes that would allow the stocking of stores; this seems entirely possible given the resilience of the hospital.

The entities in the food supply chain are not well integrated in that they do not exchange a lot of internal process data, only data relating to orders and payments. From a resilience standpoint, it is important to share the orders for replenishing stock and raw materials. All the suppliers indicated that, absent an actual order, they would be able to estimate an order and ship it. As a result, the grocery supply network would likely continue to function in a "ballistic" mode.

The results suggest that three different types of resilience are in play for a firm or sector during information infrastructure disruptions: technical resilience, operational resilience and organizational resilience. Technical resilience results from efforts to reduce the likelihood that IT processes will fail; examples include redundant servers or Internet connectivity. Technical resilience is the result of implicit or explicit information risk management processes applied before a disruption. Examples of technical resilience in the field studies include redundant generators at the dairy farms, redundant Internet connections from the grocery chain's distribution centers and stores to headquarters, and backup data centers at the pharmaceutical firm and grocery chain.

Contingency plans are examples of operational resilience: a planned workaround exists if the standard way of accomplishing a task is not possible due to a system outage. This is also a result of information risk management. Examples include the canned goods vendor requiring workers to work at a backup site to test the effectiveness of procedures and to build "muscle memory" that lessens business disruptions during transitions.

Organizational resilience may or may not be due to prior planning; it arises from the corporate culture and the work ethic and innovation of individual workers. Organizational resilience is what remains when things are not working as planned – it is why the hospital was able to function effectively during the IT disruption.

7. Conclusions

The field studies suggest that different types of risk might be best managed by focusing on three types of resilience: technical resilience, operational resilience and organizational resilience. For example, IT disruptions (e.g., application failures and network outages) would be best handled by technical and operational resilience if an analysis showed a net benefit. In such cases, the number of likely interruptions should be low, which renders feasible both the analysis and the potential technology investments.

On the other hand, if the number of likely disruptions is high, the enumeration of the disruptions and the analysis of the potential consequences would be very resource intensive. In such a situation, a compelling business case cannot be made for reducing the risk further or for mitigating the consequences. Consequently, the best approach is to develop organizational resilience.

Acknowledgements

This work was partially supported by the Institute for Information Infrastructure Protection (I3P) at Dartmouth College, Hanover, New Hampshire, under Award 2006-CS-001-000001 from the U.S. Department of Homeland Security and Award 60NANB1D0127 from the National Institute of Standards and Technology.

References

[1] C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley/Pearson, Boston, Massachusetts, 2003.

[2] L. Bodin, L. Gordon and M. Loeb, Information security and risk management, *Communications of the ACM*, vol. 51(4), pp. 64–68, 2008.

[3] S. Dynes, Information Security and Health Care: A Field Study of a Hospital after a Worm Event, Technical Report, Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, New Hampshire, 2006.

[4] 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, 2006.

[5] S. Dynes, Emergent risks in critical infrastructures, in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 3–16, 2008.

[6] D. Geer, Risk management is where the money is, *The Risks Digest*, vol. 20(6) (catless.ncl.ac.uk/risks/20.06.html), 1998.

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

[8] M. Johnson and E. Goetz, Embedding information security into the organization, *IEEE Security and Privacy*, vol. 5(3), pp. 16–24, 2007.

[9] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, Maryland, 2002.

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

[11] Wikipedia, Zotob (computer worm) (en.wikipedia.org/wiki/Zotob), 2009.