The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0957-4093.htm

Economic costs of firm-level information infrastructure failures

Estimates from field studies in manufacturing supply chains

Scott Dynes and M. Eric Johnson
Tuck School of Business at Dartmouth College, Center for Digital Strategies, Hanover, New Hampshire, USA, and
Eva Andrijcic and Barry Horowitz
School of Engineering, University of Virginia, Charlottesville, Virginia, USA

Abstract

Purpose – This paper presents a method for estimating the macro-economic cost of a firm-level information system disruption within a supply chain.

Design/methodology/approach – The authors combine field study estimates with a Leontief-based input-output model to estimate the macro-economic costs of a targeted internet outage that disrupts the supply chain.

Findings – The authors find that supply chain vulnerability or resiliency to cyber disruptions is not necessarily dependent on the types of technology employed, but rather how the technology is used to enable supply chain processes and the type of attack experienced. The authors find that some supply chains like oil and gas could be significantly impacted by certain cyber disruptions. However, similar to other causes of supply chain disruptions such as labor disputes or natural disasters, the authors find that firms can be very resilient to cyber disruptions.

Research limitations/implications – The validity of the approach is limited by the accuracy of parameters gathered through field studies and the resolution of government economic data.

Practical implications – Managers should examine how information technology is used to enable their supply chain processes and develop capabilities that provide resilience to failures. Lean supply chains that focus on minimizing inventory may be more vulnerable to major information system failures unless they take special steps to build resilience.

Originality/value – This paper provides a new approach to estimating economic vulnerability due to supply chain information failures.

Keywords Information security, Disruptions, Supply chain management, Economic estimates

Paper type Research paper

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

The authors are grateful for helpful comments from seminar participants at Cambridge University, Dartmouth College, and Harvard University. The authors would like to thank the many individuals and organizations that generously gave their time and support in enabling them to conduct these field studies; without their interest and efforts this work would not have been possible.

The International Journal of Logistics Management
Vol. 18 No. 3, 2007
pp. 420-442

0957-4093
DOI 10.1108/09574090710835147

1. Introduction

The increasing reliance of the US economy on the information infrastructure has raised questions regarding the security and robustness of the critical information infrastructure at all levels of the economy, ranging from small firms who are dependent on the internet for select business communication to large multinationals that are extensively networked with their customers and suppliers (Johnson, 2005). Until recently, managers and policy makers have had to rely mainly on speculation for guidance as empirical studies of the economic risks faced by individual firms and larger economic entities were unavailable (Cashell *et al.*, 2004). This lack of data concerning these issues was the original impetus for the research presented in this paper.

Supply chain processes represent critical business processes for large manufacturing organizations. As organizations increasingly rely on the internet to enable supply chain processes, each firm's information network has an impact on the extended enterprise of suppliers, collaborators, and channel partners (Davis and Spekman, 2004). Critical supply chain processes such as order fulfillment and manufacturing flow depend on vast transactional data on product sales and movement within the supply chain. Outsourcing and globalization have further increased the need for constant communication. Both strategic management processes, like supplier relationship management and manufacturing flow management (Lambert, 2006) and the tactical operating processes like operational order fulfillment influence the impact of an information disruption. Understanding the implications and vulnerability of information flows across the extended enterprise is a significant and under-researched topic (Johnson and Goetz, 2007). Like the interdependent risks faced by other business partnerships (Kunreuther, 2002, 2004), we hypothesize that information flow risks across trading partners exhibit many important risk management challenges.

In this paper, we examine the risks at a firm-level and macro-economic scale, looking at the possible productivity losses and resulting economic losses to particular regions of the US economy arising from specific information disruptions to supply chain processes. Rather than examine wide-spread outages, we analyze the impact of focused (firm level) cyber disruptions limited to the targeted firm. Moreover, our analysis focuses on information related to physical supply chain processes (product flow) and does not consider the impact of disruptions in other areas like invoicing or financial settlement. We present a method for estimating the macro-economic cost of a firm-level information disruption. Our approach employs field research to estimate parameters for an analytical economic model. As part of our field research, we explore the impact that an outage would have on the subject firm's ability to produce and ship product. Casting this as a change in the production of a standardized product enabled the utilization of an input-output model of the US economy to estimate the total impact such an outage would have on the economy. This total impact includes not only the direct economic consequences experienced by the affected sector, but also the indirect economic consequences brought about by disruption for suppliers, as well as the firm's customers. The economic impacts of these "ripple" effects can be greater than the direct economic impact experienced by the affected sector.

To illustrate our model, we examine three different supply chains. The firms we studied and describe here present different symptoms as a result of the

cyber events: we have focused on the impact of a disruption of their supply chain, manufacturing process, or distribution activity. We present results of supply chains whose primary manufacturing firm operates at different places on the product-process matrix (Hayes and Wheelwright, 1979). At one end of the spectrum, we examine oil refining which exhibits characteristics of continuous flow. We also study automotive component and electrical device manufacturing exhibiting high-volume/low-product mix and low-volume/high-product mix. Additionally, the firms presented span the range from build-to-stock to build-to-order enterprises.

To our knowledge, this is the first work that provides an empirically-based estimate of the macro-economic consequences of targeted disruptions to the critical information infrastructure. The knowledge resulting from this work should serve multiple important efforts:

- To reaffirm and continue to raise awareness that firms face and need to actively manage cyber-risk not just internally, but also in their extended enterprise.
- To allow interested parties to gauge and compare the risk due to cyber-events with other risks at a macro-economic scale.
- To make rational policy decisions regarding appropriate levels of information security for the critical information infrastructure.

We begin the paper by presenting our methodology, both for the field research and the economic modeling. Next we present results from our field research in the different firms. Then we integrate the results of the field work into a macro economic model to measure the financial impact of a disruption. We present our results and their limitations. We conclude by comparing cyber events to other disruptions and their implications for supply chain resiliency (Sheffi, 2005).

2. Methods

In this section of the paper, the methodology for the field research and the economics modeling are presented.

2.1 Field study

The field study consisted of a set of interviews with security and supply chain executives and managers at each participating firm. 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. At the start of each interview, we made it clear to the interviewees that the interview was anonymous; during the interview every effort was made to build a high degree of trust with the interviewee. Interviewees at "host" firms included top-level managers as well as lower-level individual contributors, of both information security and supply chain management. Interviews at supplier firms included managers of information security and of supply chain; at very small firms these might be the same individual. We interviewed CIOs, CSOs, VPs supply chain, buyers, production and warehouse managers, and other decision-makers about information failures and there impact. We have found that this triangulation approach works quite well; interactions with executives and managers with different responsibilities and decision support roles about the same issue allowed us to determine how well different firms and divisions communicate and are affected by events (see Dynes *et al.* (2005) for more information on the field studies).

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 and triangulated between the different data sources to arrive at a robust conclusion (Gurium and Holstein, 2002). Additionally, this approach exposed both strategic as well as tactical issues regarding information security and its role in maintaining the supply chain. The interviews along with all other collected data including slides, documents, etc. were used to develop research case studies on each supply chain (Yin, 1994). The insights obtained from these cases are presented in the following sections.

Questions asked during the interviews were centered on the identification and management of information security risks, and of particular interest for this work, business continuity risk firms faced as a result of using select technologies to manage their supply chains. These were open-ended questions eliciting the impact that an internet outage of certain durations would have on the ability of the firm to continue to produce and ship product. The interviewee would be queried about durations of one second, one minute, one hour, etc.; the conversation would quickly evolve to a discussion about the conditions, durations and impacts of consequential outages. The results of these conversations were documented, and serve as the basis for the determinations presented in this paper.

2.2 Macro-economic model

In order to estimate the macro-economic consequences on the US economy due to internet outages to the three aforementioned sectors, the inoperability input-output model (IIM) was employed (Haimes *et al.*, 2005a, b; Santos and Haimes, 2004). The IIM is based on the economic theory of Wassily Leontief who won the Nobel Prize (1973) for the creation of the input-output model for the US economy, which describes economic interdependencies between various sectors of the US economy (Leontief, 1966). The general formulation of Leontief's input-output model can be described by the following equation:

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{c} \Leftrightarrow x_i = \left\{ \sum_j a_{ij} x_j + c_i \right\} \quad \forall \ i,$$

where x_i represents the total production output of industry i, a_{ij} represents the ratio of the input of industry i to industry j, with respect to the total production output of industry j (given n industries a_{ij} gives us the distribution of inputs contributed by different industries $i = 1,2,\ldots n$ to the total output of industry j), and c_i represents the final demand for industry i (i.e. it tells us what portion of industry i's total output is used for final consumption by end-user).

While the mathematical formulation of the IIM is very similar to the general Leontief model, its interpretation is different and "supply" and "demand" concepts of the Leontief model take on a new meaning. The input to the IIM is a vector of perturbations to sectors, which can include willful attacks, accidents, or natural disasters, and the output becomes a vector of inoperabilities (the percentage reduction in economic output from that sector caused by the disruptive perturbation to the systems used for production) of different sectors, resulting from the introduced perturbations (Santos and Haimes, 2004).

For this paper, the disruptions of interest are attacks on the information systems that support production and supply chain integration. Utilizing data on economic interdependencies from the US Department of Commerce – DoC (1998), the model is able to account for production and services interactions and dependencies of all of the significant industries in the USA, permitting one to determine the integrated economic impact of a specified reduction in productivity of any subset of industries, or a reduction in demand for any subset's products.

One of the metrics offered by the IIM is inoperability, which is defined as the inability of a system to perform its intended functions. In the IIM, inoperability can denote the level of the system's dysfunction, expressed as a percentage of the system's intended production level. Inoperability can be caused by internal failures or external perturbations, which negatively affect the delivery of a system's intended output. The formulation of the IIM is given by:

$$\mathbf{q} = \mathbf{A}^*\mathbf{q} + \mathbf{c}^* = (\mathbf{I} - \mathbf{A}^*)^{-1}\mathbf{c}^*.$$

In summary, the terms in this formulation are defined as follows:

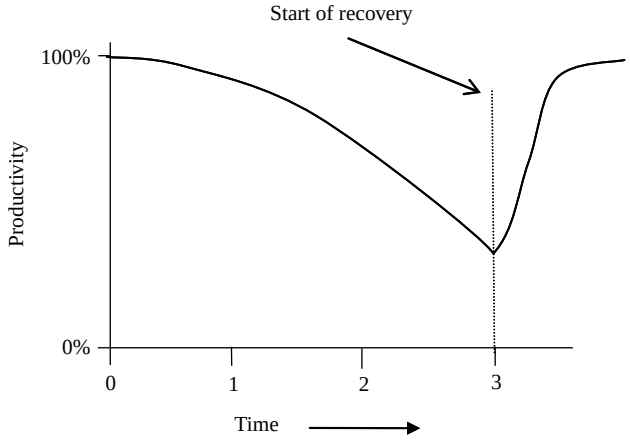
- $\mathbf{q}$ is the inoperability vector expressed in terms of normalized economic loss. The elements of $\mathbf{q}$ represent the ratio of unrealized production (i.e. "business-as-usual" production minus degraded production) with respect to the "business-as-usual" production level of the industry sectors.
- $\mathbf{A}^*$ is the interdependency matrix which indicates the degree of coupling of the industry sectors. The elements in a particular row of this matrix can tell how much additional inoperability is contributed by a column industry to the row industry.
- $\mathbf{c}^*$ is a perturbation vector expressed in terms of normalized degraded final demand (i.e. "business-as-usual" final demand minus actual final demand, divided by the "business-as-usual" production level).

A major benefit of the IIM is the fact that it is supported by a large, ongoing national data collection effort conducted by the US Bureau of Economic Analysis (BEA), resulting in a database which contains a series of input-output tables depicting the production and consumption of commodities (i.e. goods and services) of various sectors in the US economy (DoC, 1998). The BEA data record the physical exchange of commodities between various interconnected sectors of the economy, scaled by producers' prices into monetary units. The detailed national tables are composed of hundreds of industries, organized according to the Standard Industry Classification or more recently, the North American Industry Classification System codes. These tables are used to produce the Leontief technical coefficient matrix which depicts the economic interdependencies between nearly 500 US sectors. The IIM is also supported by a set of regional data (RIMS II) maintained by the BEA, Regional Economic Analysis Division (DoC, 1997). RIMS II releases regional data for various regions of the USA. Thus, with the availability of national and regional data, analyses can be conducted on the regional level, which provides a more focused and thus more accurate analysis of interdependencies for particular regions of interest in the USA. Note that the IIM is based on the assumption that the level of economic dependency between various sectors is the same as the level of physical dependency between those sectors.

For our application, the IIM considers a system consisting of 59 critical interconnected sectors and a regional analysis of impacts, with the output being their inoperability that can be triggered by one or more failures (see Santos and Haimes (2004) for more details). Inoperability represents a degradation in the system's functionality that is expressed as a continuous variable evaluated between 0 and 1, with 0 corresponding to a flawlessly operable system state and 1 corresponding to the system being completely inoperable. The inoperability caused to a particular sector can cause an inoperability ripple to the other sectors in the interconnected economic system. The IIM captures this ripple effect and provides a system for ranking the most vulnerable sectors. Combining the main output of the IIM, namely the inoperability of sectors caused by a particular perturbation, with the BEA data on economic interactions between the sectors, the IIM can compute the direct and indirect economic losses to all of the sectors of the US economy.

2.2.1 Integration of the company-specific data into the IIM. Firm-level disruptions were reflected into the macro-economic model through the development of productivity erosion curves. From the interview data and information about the supply chain processes, we estimated the impact on the production function during an internet outage. A notional example is shown in Figure 1, which shows an example of a curve of decreasing productivity after an internet interruption, followed by a recovery to 100 percent productivity.

One might consider whether it might be possible for the production to recover beyond 100 percent. Such could be the case if, for example, Amazon.com were to be down for an hour – the sales that occurred during that hour would not all be lost, but some percentage of them would occur shortly after Amazon.com reappeared and the order fulfillment department may use overtime to ship the increased demand. We focus on productivity as a percentage of normal activity, as opposed to some "potential maximum" output under unusual circumstances. In the example given, the productivity



Notes: In this example the failure commences at time = 0 and lasts until time = 3; productivity decreases until the outage ends and immediately starts to recover to 100 percent. Productivity recovery was limited to 100 percent in this work

Figure 1.
A notional diagram depicting how a firm's productivity might change following an internet failure

would increase above 100 percent. In the models derived here, productivity is held to a maximum of 100 percent to capture the potential disruption if some unusual effort to exceed normal productivity is not possible.

3. Field study results

Interviews were conducted in three manufacturing sectors: automobile component manufacturing, electrical component manufacturing, and oil refining. In the case of the automobile and electrical manufacturers, the host firm was a Fortune 500 manufacturing conglomerate with plants and sales worldwide. The participating oil refinery was a medium-size specialty refiner.

The interviews were conducted with security, information and supply chain executives and managers at both the headquarters level, and where applicable at an individual business unit (BU) level; interviews were also conducted at suppliers. The great majority of interviews were conducted in person with one or two researchers, and one to four interviewees. Interviews lasted from 30 minutes to 2 hours; the remainder was phone interviews.

3.1 Automotive and electrical

The host for both the automotive and electrical sector studies was a Fortune 500 conglomerate. The electrical BU served a combination of both high- and low-volume customers (Figure 2). On the automotive side, the host was a tier one supplier to the automobile industry, meaning that its products went directly into the finished product, rather than a sub-assembly. As such, its customers were the automobile manufacturers (Ford, GM, etc.), which have rigorous requirements regarding electronic notification of dispatch of product shipments, access of design documents and other functions. Additionally, the auto and electrical BUs of the host organization were urging their entire supply chain to utilize either the host's web-based supply-chain applications or EDI (which can be thought of as e-mail formatted in standardized ways) to manage their business with the host. This was putting pressure on the host's suppliers to become reliant on the internet for this customer. In summary, the host was dependent on the information infrastructure to communicate with its customers, and was working to

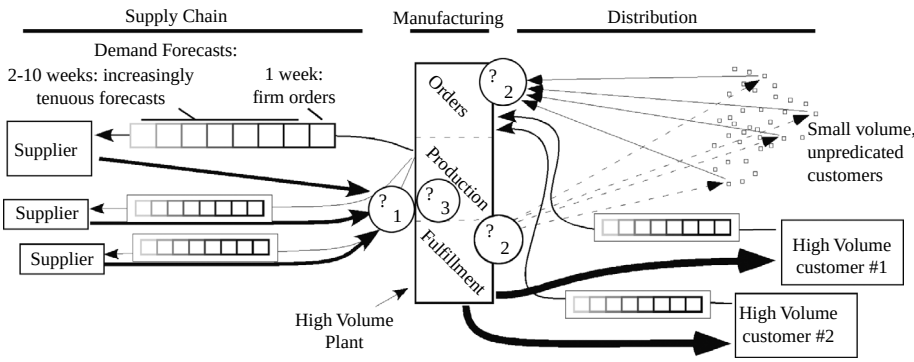


Figure 2.
Schematic of high-volume plant value chain, showing suppliers, the "plant" incorporating order processing, production and fulfillment, and distribution functions

Notes: Here, all suppliers are provided with forecasts of future demand; on the customer side high-volume customers who provide forecasting as well as smaller volume, occasional customers are represented. Three sources of interruption, denoted by the question marks ('?') are discussed in the text

move its supply chain management functions (communications with its suppliers) to be internet-based as well. Table I gives some particulars about the host and the suppliers. In all, 29 individuals were interviewed.

The host's suppliers were much more variable with respect to their dependency on the internet. Most communicated with their suppliers using phone and fax, and were much less susceptible to interruptions of their supply chain due to internet outages (for more discussion of the field stuffy findings, see Dynes *et al.* (2005) and Dynes (2006)). These tier-two suppliers were also less dependent on the internet for communication with their customers as well. As alluded to in Table II below, for these suppliers the major impact of an internet event would not be supply chain or production disruptions, but in customer service via e-mail.

	Product	Number 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 I.
Properties of interviewed firms for automotive and electrical

Internet down for	An afternoon	One day	Three days	A week
Electrical part manuf.	No impact	Low-volume plants: supply-side pain	High-volume plants OK	High-volume plants: shipping issues
Automobile part manuf.	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, would use phone, fax, expect no loss of business		
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 II.
Estimated impact on a firm's ability to produce and ship product resulting from internet outages of various durations

Table II is a high-level summary of the knowledge collected during the interviews that enabled the generation of specific estimates of the impact internet outages would have on the ability of firms to produce and deliver product (firm productivity). To show this process in detail, consider the electrical parts manufacturer. For the shortest duration outages (an afternoon is listed in Table II), we found no evidence that there would be any impact of the firm's ability to manufacture parts. If the outage lasted longer, there would start to be effects. This manufacturer produced electrical products that range from small, very high-volume items (many thousands produced a day) such as fuses and switches to large, very low-volume (a few a month) items such as power-station transformers. Because of the long lead time required for parts that make up these large items, they must be ordered days or weeks in advance. Thus, if the internet were unavailable the day that an order needed to be placed for one of these long lead-time parts, there would be some disruption in the supply chain for these low-volume items.

It is unlikely this would mean that the order would not be placed, and that the delivery date for the entire transformer would slip. In place of an internet-mediated order, the order could be placed by phone or fax: since these were low-volume items, phone or fax ordering is entirely feasible. Prolonged internet outages for low-volume items would likely result only in customer-service disruptions, as e-mail would be unavailable.

It is also the case that for many large items the largest suppliers of constituent parts were other plants of this manufacturer. To assure connectivity among these internal plants, the manufacturer had invested in an internal network that is separate from the internet. For these reasons, we estimated the impact of an internet outage on the production and delivery of low-volume items would be negligible.

There remains the case of the high-volume goods that this manufacturer also produces. Effectively supporting a manufacturing operation that produces many thousands of items a day involves frequent electronic communication of stock on hand and forecasting of demand. For example, a forecast to a supplier might reiterate the firm order for this week's supplies, a very good estimate for what will be needed the following two weeks, and a progressively ill-defined estimate of what will be needed up to ten weeks out. This forecasting and the history between the suppliers and the manufacturer result in what one interviewee termed a "supply chain learned behavior," If the internet were to fail, the suppliers would still deliver the needed supplies without any prompting from the manufacturer due to this "learned behavior." Based on our field work, we estimated that the first noticeable supply chain event would occur about three days into an outage, when the suppliers would start calling the manufacturer regarding future forecasting and shipment information.

The major impact of an internet outage on the high-volume plants would likely be an order fulfillment (see Croxton (2002) for a thorough discussion of the order fulfillment process) issue depending on the number and predictability of orders for the many thousands of devices being built. If there were a handful of large customers for the product, it would be likely that they also have forecasting and a "learned supply chain behavior" in place and shipments would be packed and shipped as expected. At the opposite end of the spectrum would be the case where there were hundreds of customers whose orders were delivered electronically and whose future orders were unknown. For such cases, our research led us to conclude that it is unlikely that the manufacturer could handle the potentially hundreds of faxes and/or phone calls for one or many products in various volumes, or to arrange shipment for product. Production and packaging would

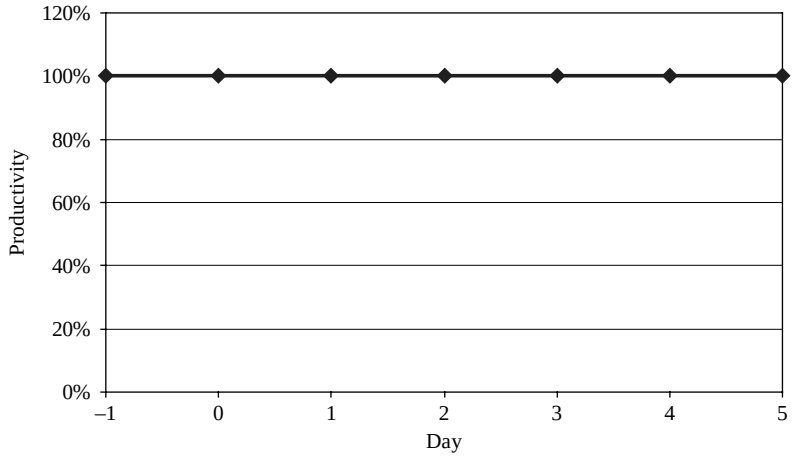
continue, but except for large customers these packages would accumulate on the shipping dock as the fulfillment system failed for smaller, *ad hoc* orders.

This is shown graphically in Figure 2, where we depict the value chain of a high-volume plant. As indicated in the text, the demand for stock from suppliers is forecast, as is the demand from high-volume customers. In the case of the electrical goods manufacturer, the supply chain would function, delivering components to the plants, which would continue to produce product. The high-volume customers, who have forecast their demand, would continue to receive shipments of product. The lower volume, unpredictable customers would face bottlenecks at the points indicated by $?_2$ because of the inability of the plant's order processing and fulfillment functions to cope with the volume of orders that would have been placed via the web, but are being phoned and faxed in due to the disruption of the internet.

For these plants we believe the 80/20 rule is appropriate, where 80 percent of production at high-volume plants is destined for a few large customers – for example switches for retailers. We concluded that these large customers would not experience a disruption, and that some percentage of smaller customer orders would also be fulfilled. Based on our analysis, estimates of the impact on productivity are shown in Figure 3 for an outage of three days, and Figure 4 for an outage of ten days.

The quick recovery of "productivity" to 100 percent shown in Figure 4 is based on the fact that there is not a production disruption, but a fulfillment disruption, and that the resumption of electronic order and shipping fulfillment will quickly deal with the backlog. It is arguable that in this case the "productivity" might increase beyond 100 percent as the volume of shipments is highly likely to be much greater than typical immediately following resumption of internet service. As described in the Methods section, we limit the maximum to 100 percent.

A similar approach is used to estimate the impact an internet outage would have on the productivity of an auto parts manufacturer. The automobile parts manufacturer adopted a different approach to supply chain management than the electrical parts manufacturer.



Notes: For the reasons discussed in the text, we conclude that an outage of this duration would have no effect on production

Figure 3.
The impact of an internet outage of three day's duration on the production of an electrical goods manufacturer

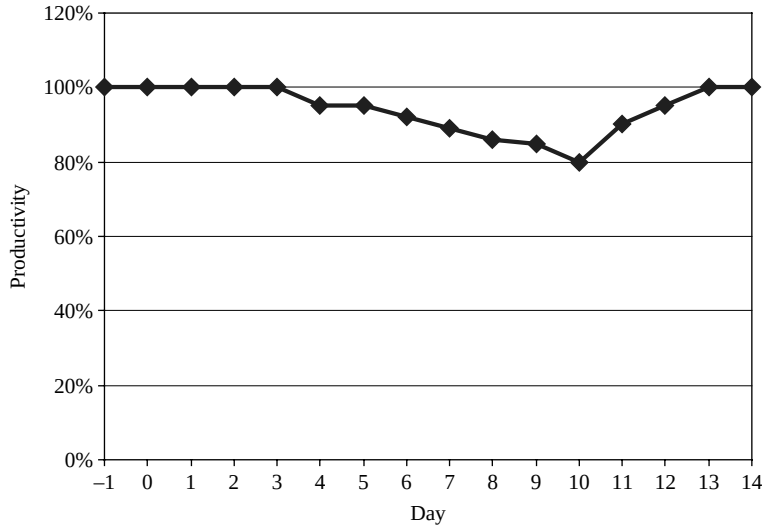


Figure 4.
The impact of an internet outage of ten day's duration on the production of an electrical goods manufacturer

Notes: As discussed in the text, we conclude that an outage of this duration would have a small effect on production

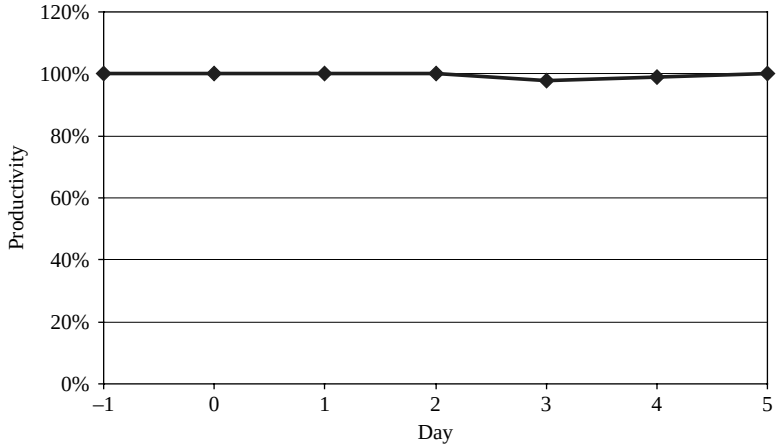
Where the electrical supply chain was expected to display certain inertia and continue to deliver parts to high-volume plants, the automobile manufacturer in some important instances adopted a more just-in-time approach to supply chain management. Many of the sub-assemblies that the manufacturer uses were produced by local suppliers. While the auto parts manufacturer shares forecasting information with these suppliers, the manufacturer ran its own fleet of trucks to pick up these sub-assemblies in order to keep costs down, and to maximize efficiency the manufacturer was very explicit about how items should be packed, and when they should be ready for pick-up. To be clear, these suppliers would not prepare items for pickup or delivery unless they were explicitly told to do so by the manufacturer using EDI transmissions. This communication was enabled by EDI via the internet.

An outcome of this strategy was the lack of a "learned supply-chain behavior": if they were unable to communicate with their suppliers, the supplies would not be delivered. From our analysis of the number of suppliers, the part counts and the frequency of ordering it is doubtful that these communications could be fully replicated via fax. As a result, there would be a restocking shortfall during an internet outage. The automobile parts manufacturer maintained a 3-5 day supply of stock; there would be attempts to restock parts. However, if stocks depleted there would be increasing disruptions to the manufacturer's ability to make and deliver product, as shown in Table II.

On the customer side, a few very large firms accounted for the great majority of the auto parts; the schedule of products and delivery was reliably known for these accounts for at least a week. Shipments for these customers would likely be limited by production rather than managing order communication. There were also many smaller customers for after-market parts; the particular volume for specific items was not known before the order, and these orders would likely be adversely impacted by an internet outage. This situation is also shown in Figure 2; in the case of the auto parts manufacturer,

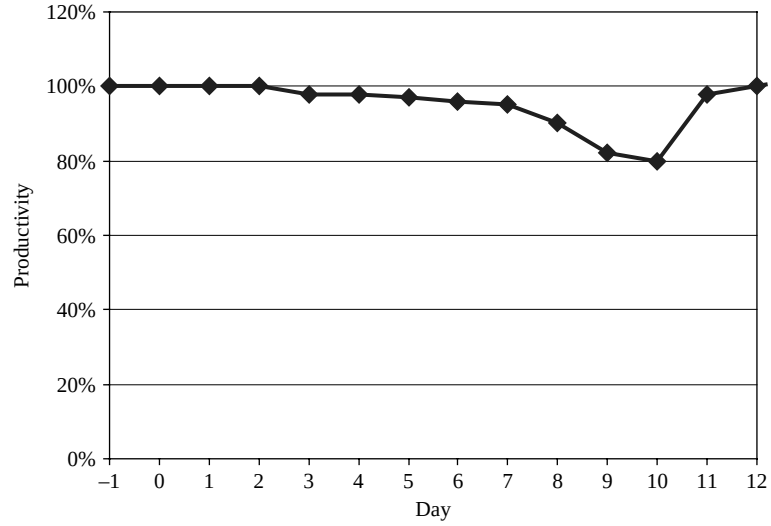
the bottleneck would not be in the order processing and fulfillment functions, but at the point labeled by ?$_1$: the ability of the supply chain to effectively respond to stock shortages due to the supply chain timing and packing optimizations utilized.

From these considerations we estimate the change in production due to an internet outage as shown in Figures 5 and 6. Figure 5 shows the change in production for an internet outage of three days. This plot shows no change until day three, at which there is a small decrease in production due to the inability to build some assemblies due to a



Notes: For the reasons discussed in the text, we conclude that an outage of this duration would have a small effect on production

Figure 5.
The impact of an internet outage of three day's duration on the production of an automobile parts manufacturer



Notes: For the reasons discussed in the text, we conclude that an outage of this duration would have a small effect on production

Figure 6.
The impact of an internet outage of ten day's duration on the production of an automobile parts manufacturer

shortage of some parts, understanding that the lack of a single part such as an O-ring can stop the production of a much bigger assembly. Figure 6 shows the change in productivity for an outage of ten day's duration. As before, there is no change until day three, and then there is a continuing decline in productivity. With five days of inventory, the productivity declines accelerate at that point. However, given that time to respond, we concluded that the manufacturer and suppliers will make accommodations to the internet outage, and that a steady-state production will not drop below 80 percent by the tenth day of the outage. Interestingly, the belief of this 80 percent was widely shared by managers in both electrical and automotive cases based on past disruption experiences like strikes. However, note the both the decline to 80 percent and the recovery differed based on the nature of the supply chains. In this automotive case, degradation is due to the challenges of coordinating multiple inbound components for the assembly using manual systems as well as the difficulty of handling after-market orders.

3.2 Oil and gas

The oil refinery that participated in the study was in the southern US that produced specialty petroleum products. We conducted multiple interviews over a span of months with nine key individuals including the CIO and other functional executives.

Unlike the electrical and automotive producers, the business operations at this refinery would be largely unaffected by an internet outage; supplies were typically ordered by phone with a lead time of weeks, and product orders while usually communicated via the internet could easily be handled via phone as well. As a result we estimate the change in production for this small refinery not as the result of an internet outage, but as the result of an attack on the refinery's Supervisory Control and Data Acquisition (SCADA) system (also known by other acronyms such as PCS and DCS). Oil refining involves performing a series of chemical reactions on the crude oil. At the refinery, there was storage for both the pre- and post-processed product; conceptually refining oil looks like storage-process-storage-process-storage until the refined product is stored for blending or delivery. The plant SCADA systems comprise the sensor, actuator, monitoring and logic systems required to run and monitor these processes. SCADA systems are present and play the same role in all large physical systems such as oil refineries, gas pipelines and electric generation and distribution systems.

Abstractly, there are two relatively separate SCADA networks in any refinery: a monitor and control network (MCN), and a safety network (SN). The MCN has device actuation (valves, pumps, etc.), sensing (temperature, pressure, etc.), data monitoring, control and archiving functionality; control is typically located at a central facility manned 24 hours a day. The refining process is continually monitored and adjusted to maintain optimal conditions for the current production run. The SN has sensors and actuators and logic that are designed to prevent conditions that would lead to physical harm, such as an explosion. The sensors, logic, and actuators are located at the protected device, and act automatically. Devices that form the SN (more properly, several separate sensor-logic-actuator networks) may not be used as part of the MCN.

The event considered is the compromise of part of the MCN, which will result in an action by the SN. This is presumed to result in the shutdown of the unit associated with the compromised part of the network, which would halt one step in the oil refining process. Because of the inter-process storage, there is some amount of time that the

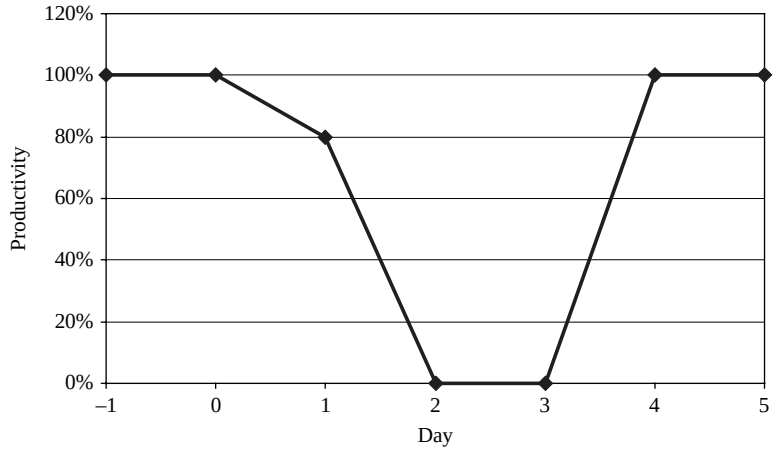
other processes would be able to run before they would need to shut down due to lack of pre-process product or storage capacity for the post-processed product. During this time the output of the refinery would be slowly decaying. Once the refinery was shut down, there would be no production of finished product. In the language of Figure 2, this scenario would result in the bottleneck being at point $?_3$ in the "Production" box of the manufacturer; neither $?_1$ or $?_2$ would be bottlenecks.

After the compromise is detected and corrected, the refinery would be restarted. While refineries would take several days to restart from a "cold" shutdown, the most likely course in this event would be a warm shutdown, where the functioning units are kept warm. In this instance, the refinery would resume 100 percent production in roughly eight hours. These considerations result in the production vs time plots shown in Figures 7 and 8.

We note that in reality the refinery maintained a large enough reserve of product to handle (without any additional production) normal demand for a period of time exceeding that required to recover from most any event, including the physical destruction of major refinery structures such as cracking towers. The result is that the ten-day event would impact the refinery's ability to "boil oil" and refine product, but not their ability to deliver product to the customer. Of course, because the refiner's capacity constraints they must eventually make up the lost production, which would erode their ability to accept new future demand or increase their costs. On the other hand, any production interruption for many large gasoline refiner would represent an immediate decrease in their revenue due to limited finished goods inventory. To summarize, the productivity curves shown would be representative of a SCADA attack on a tight capacity or low-reserve refinery.

4. Macro-economic model results

The macro-economic model was parameterized using the productivity data displayed in the figures above. For the analysis presented in this paper, the IIM was used to



Notes: As described in the text, the refinery will run at a reduced rate for roughly a day, and then move to a warm shutdown state from which they can quickly restart

Figure 7.
The impact of a SCADA safety system event of three day's duration on the production of an oil refiner

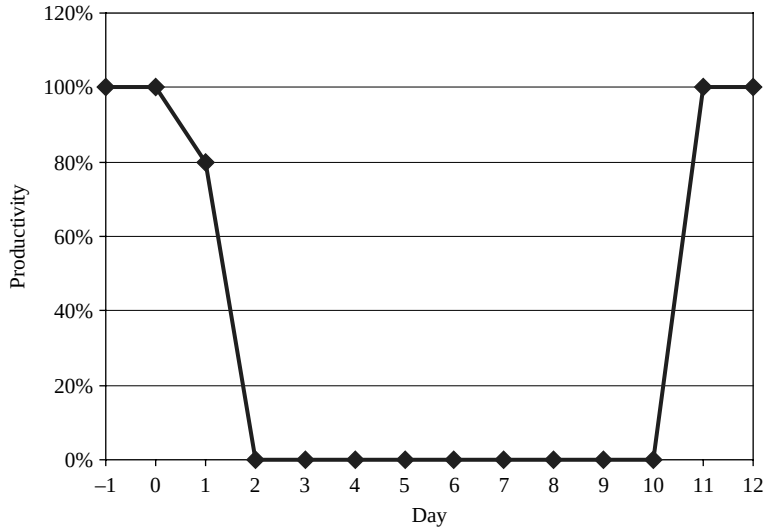


Figure 8.
The impact of a SCADA safety system event of ten day's duration on the production of an oil refiner

Notes: As described in the text, the refinery will run at a reduced rate for roughly a day, and then move to a warm shutdown state from which they can quickly restart

calculate the economic impact to particular regional US economies due to perturbations to supply chains of three different sectors. Three separate, regional analyses were conducted, of two Petroleum Administration for Defense Districts (PADD) regions, namely PADD II – Midwest region, and PADD III – Gulf Coast region. The impact of a supply chain perturbation to the automobile and electrical device manufacturing companies was evaluated in the Midwest region and the impact of a supply chain perturbation to the oil refining company was evaluated in the Gulf Coast region. The following assumptions were made so as to provide appropriate inputs to the model:

- Given that the supply chains of the companies were interrupted and possibly resulted in an inability to produce and/or ship products to customers, a supply constraint was introduced to the model. In other words, the supplying capability of the company was constrained by the introduced perturbation. This is the perturbation shown in Figures 3-8.
- In order to calculate the perturbation to the output of a particular sector, it was necessary to convert the supply chain perturbations affecting a particular company to a sector-based perturbation. This was done by finding the relative size of each company's output to the sector output in a particular region. In order to calculate the relative size of each company's output to the size of the sector output in the particular region, we modeled the automotive manufacturer to represent 5 percent of the total national output of the motor vehicle, body, trailer, and parts manufacturing sector, electrical device manufacturer produced 5 percent of the total national output of the electrical equipment and appliance manufacturing sector, and the oil refinery produced 10 percent of the total national output of the oil and gas sector. These quantities were disguised to protect the identity of the participating firms, but are representative of those

firms and the desired level of disruption impact. Knowing the size of the regional output for the three sectors, it followed that the automotive manufacturer represented approximately 7.5 percent of the regional output, the electrical manufacturer represented approximately 11.5 percent of regional output, and the oil and gas company represented about 16.1 percent of the regional output.

- Daily perturbations (interruptions) to the three sectors were computed by converting the daily loss of sales to the company into sales reductions to the entire sector, by using the numbers obtained in (2). For example, a 5 percent loss of sales to a company which represents 7.5 percent of total regional output resulted in a perturbation of 0.00375 (5 percent $\times$ 7.5 percent $= 0.05 \times 0.075 = 0.00375$) to that sector. The perturbation was then introduced as a supply constraint to the model. The model assumes there are no substitutions available, that is, it assumes sales will drop. So, if there is an internet outage which prevents supply and delivery of goods, the model assumes that those goods will not be delivered.
- The IIM produces annual results, so the losses were adjusted accordingly to obtain a daily losses.
- Two regional IIM models, one for PADD II region (Midwest) and one for PADD III region (Gulf Coast) were used instead of a national IIM to provide a more focused and more accurate analysis of the relatively small perturbations. These regions were chosen to reflect the activity of the firms in question.

Mapping between the results obtained from the field studies and the inputs into the IIM occurred by utilizing the productivity functions developed in the field studies. The primary input into the IIM, the perturbation to a particular sector, was obtained by looking at the percentage loss of sales on a particular day for a particular company and the size of the company with the respect to the total regional sector output, as described in point three above. Six different analyses were performed – for each company a three- and ten-day event were evaluated.

Daily perturbations were individually entered into a customized regional IIM model (i.e. for a three-day perturbation three different calculations were made, one for each day), and the model produced a yearly loss to the US economy. The total loss due to a three -day event was computed by adding the daily losses for the three days. Based on the interdependency matrix in the IIM, this total loss was then separated into direct losses (losses to the attacked sector) and indirect losses (losses to the sectors that are interconnected with the attacked sector), and a ratio between indirect and direct losses was computed to indicate the significance of the indirect losses, which are most often overlooked in the economic analyses of cyber events. For example, an indirect-to-direct ratio of 0.66 would indicate that for every dollar that is directly lost to the perturbed sector 66 cents are indirectly lost by other sectors. Similarly, computations for other sectors followed the same procedure.

4.1 Electrical

The macro-economic model estimates for the electrical manufacturer are shown in Figure 9, which shows the losses for several days of a ten-day internet outage. We see that a three-day internet outage would result in no loss to the economy of the Midwest, while the ten-day internet outage would result in a loss of $22.6 million. These amounts include the direct economic losses to the manufacturing sector that was perturbed, as well

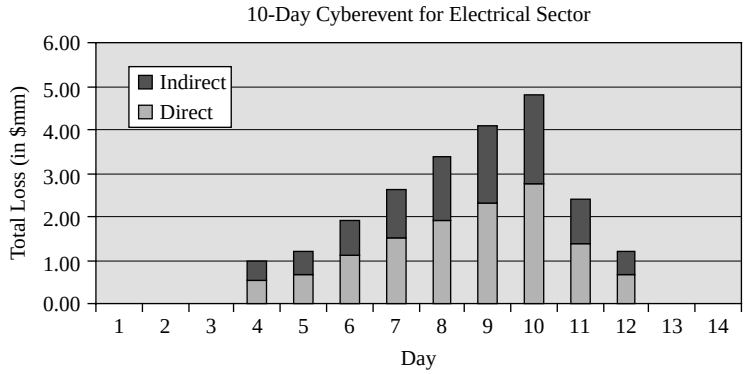


Figure 9.
The impact of a SCADA safety system event of ten day's duration on the production of an oil refiner

Notes: The manufacturer was assumed to represent 5 percent of the total sector capacity nationwide; direct losses are the economic losses to the perturbed sector, indirect losses include those due to reduced demand from suppliers and reduced sales by customers. The integrated loss is $22.6 million

as the total indirect losses due to reduced demand for the supplies needed by the manufacturer and the inability of the manufacturer's customers to produce their products.

4.2 Automotive

Figure 10 shows the results for the automobile parts manufacturer. The total economic losses for the three-day outage are $2.96 million, the losses for the ten-day outage are $65.16 million. The higher figure for the three-day event is due to the development of parts shortages sooner for the auto parts manufacturer; the larger amounts are also due to the relative sizes of the auto and electrical parts sectors. To provide contrast, note that a one-day loss (zero productivity) of the entire national automotive sector would result in a $1,476.8 million disruption.

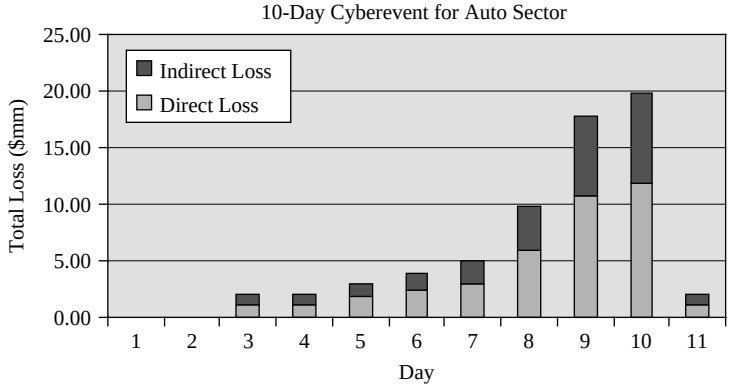


Figure 10.
Estimates of the daily macro-economic cost to the Midwest regional economy of an internet outage of ten day's duration to an automobile parts manufacturer

Notes: The manufacturer was assumed to represent 5 percent of the total sector capacity nationwide; direct losses are the economic losses to the perturbed sector, indirect losses include those due to reduced demand from suppliers and reduced sales by customers. The integrated loss is $65.16 million

4.3 Oil and gas

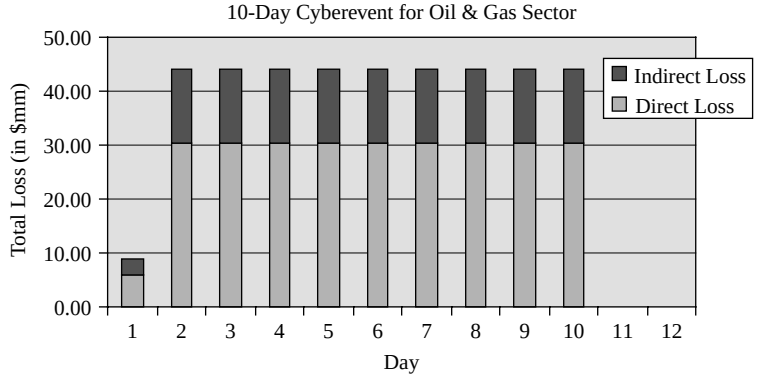
For this SCADA event, the three-day event would result in a total economic loss of $96.79 million, while the ten-day event would result in a loss of $405 million. Figure 11 shows daily losses for the ten-day event. In contrast, a one-day loss (zero productivity) of the entire national oil and gas sector would result in $594.2 million disruption.

5. Evaluation

Here, we present the first industrial process-based estimates of the macro-economic costs of two types of cyber events to the US economy. These estimates are based on field studies elucidating the impact that the cyber events would have had on the productivity of the firm, and the macro-economic model, which provides a means for determining how a change in the production or demand in one sector will ripple through the economy, resulting in the indirect cost being some multiple of the direct losses suffered by the affected firm.

It is important to note the indirect-to-direct losses multiplier, which indicates how much in terms of dollars the US economy loses indirectly for every $1 lost directly. Often, in evaluation of costs due to cyber events, indirect losses are completely ignored; however, very often those costs are almost as high, and sometimes higher, than the direct costs, and they should be of great concern to the interconnected sectors. The major benefit of IIM analysis is that it provides one with indirect-to-direct multipliers so that even if the accurate estimates of direct costs were not known, as is usually the case, one could make assumptions about the size of the direct losses, and could then easily compute the resulting indirect losses by simply multiplying the assumed direct losses with the indirect-to-direct multiplier.

While the IIM benefits from BEA data collections and a community of users and developers that continue to pursue improvements such as regional sub-model developments that correspond to national data and protect privacy, critics note that the IIM is a static, linear model that does not account for market-place substitutions.



Notes: The refiner was assumed to represent 10 percent of the total sector capacity nationwide; direct losses are the economic losses to the firm, indirect losses include those due to reduced demand from suppliers and reduced sales by customers. The integrated loss is $405 million

Figure 11.
Estimates of the daily losses to the Gulf regional economy of a SCADA safety system event of ten day's duration to an oil refiner

Of course, many of the criticisms can be addressed. For example, the linear model is reasonable since changes due to short-term internet outages are small compared to the overall economy and can thus be dealt with as a small perturbation in a linear fashion. The fact that IIM does not deal with market-place substitutions generally limits its use to cases in which:

- no important substitution capabilities exist; and
- impacts of substitution are derived as a direct analytical result.

Often, suppliers of specialty components are sole sourced or cannot be substituted within the short time windows represented by the disruptions considered in this paper. Moreover, our goal is simply to understand the relative magnitude of cyber disruptions. Thus, in the context our analysis, the IIM assumptions do not appear to be overly restrictive.

5.1 Supply chain processes and technology

Although the auto parts and the electrical parts firms are both discrete manufacturing firms, the impact of short internet outages differs greatly between the two. In the case of the electrical firm, there was little or no expected supply chain disruption for several days because of the manner in which their supply chain relationships have evolved. The expectation is that the suppliers would continue to behave as they have in the past, and deliver the ordered or forecasted number of supplies to the various plants, enabling them to continue producing product. Using a just-in-time approach, the auto manufacturer takes a much more control-oriented stance; here the expected behavior is to not ship until told to do so. That, along with the levels of on-hand stock leads to their running into production difficulties in a few days. To contrast, the oil refiner maintains enough finished goods inventory to cover many production disruptions, however when capacities are tight, lost production eventually impacts petroleum markets.

Note that there is not necessarily a correlation between utilization of technology and the resiliency of a given firm to cyber disruptions. The electrical manufacturer is vigorously involved in moving their entire supply chain to a web-based order and quality management system; their aim is to become 100 percent dependent on the information infrastructure to manage their supply chain. The auto parts manufacturer is also attempting to move the management of their supply chain to be entirely internet-based (web and EDI). The point is that it is not just a firm's dependence on the information infrastructure, but also how they use it that determines how vulnerable a firm's supply chain operation is to internet-based communication disruptions. The electrical firm uses technology to enable a fairly autonomous flow of supplies while the auto firm uses technology to implement a just-in-time supply control structure. An interesting question is whether the clear benefits from the highly controlled, lean approach outweigh the increased resiliency inherent in the less optimized, more autonomous approach, or whether there are approaches that combine the best characteristics of both.

A side note is how executives viewed the future of supply chain management. When asked what they would like to see most from a more tightly integrated supply chain (implicitly enabled by the information infrastructure) their response, almost without exception, was a greater view into the future demands of their customers. These executives would like access to their customer's present and future sales predictions so they could better plan their business. This desire went beyond the ten weeks of forecasts

that the electrical and auto manufacturers currently send to their large suppliers. The suppliers wanted to be more integrated in their customer's sales activities. There is little doubt that this would result in fewer supply chain surprises – the unexpected demand for product from the supply chain to cover an unplanned order. The implication of these surprises is inventory. Suppliers throughout the supply chain, carry safety stock to mitigate uncertainties in demand and supply, which drives associated holding costs. Better demand and supply information could reduce these uncertainties and the required safety stocks. Of course, reducing inventory would make supply chains more vulnerable to information failures.

Our findings show that many lower tier suppliers are not yet dependent on the internet to manage their supply chains. As can be seen from Table II, except for the largest businesses (annual revenue in the billions), an extended internet outage would not hamper the ability of any supplier to produce and deliver product to their customers. Even large suppliers such as Suppliers B and C were not critically reliant on the information infrastructure. From these results it would be reasonable to conclude that, as of the time of these field studies, beyond the first tier, the manufacturing sector supply chain is quite resilient to internet disruptions as a result of the lack of dependency on the internet for managing orders with their customers and suppliers.

6. Conclusions

In this paper, we examined supply chain processes and their reliance to cyber disruptions. Using a modeling approach, we found that supply chains that utilize significant automation and process control, like oil and gas, could be significantly affected by targeted cyber disruptions that penetrate internal control systems. However, we found that many manufacturing supply chains are less automated or have processes that can continue to operate using manual intervention without internet communications, making them surprisingly resilient to internet outages.

These results are consistent with many real-world supply chain disruptions. For example, in a highly studied incident (Evans and Wolf, 2005), Toyota was able to replace production lost when a supplier of brake valves experienced a devastating fire. Even though the valve was unique and sole-sourced, Toyota and its supplier base was able to jury-rig production lines in 62 locations enabling the final assemble plant to resume limited production within four days. The entire supply chain was back to full production within two weeks.

Likewise, many predicted dire consequences from the ten-day west coast dockworkers strike in 2002. The October disruption was particularly worrisome for the world's largest toy makers, Mattel and Hasbro, who were at the height of the holiday shipping season from production sources in Asia (Gentile, 2002; Isidore, 2002). Yet, both firms were able to find many ways to work around the problem including air freight and diverting product destine for other markets resulting in very little real economic impact (Gianoukos *et al.*, 2002; Mattel, 2002). In fact, that holiday season showed good growth and resulted in strong stock performance.

A study of the disruption to airline operations by a snowstorm also shows that the costs due to a three-day snowstorm event centered around Boston, MA are small compared to the annual costs of cancellations and diversions (Shavell, 2000). This study, which examines the larger, systemic disruptions due to the reduction in

performance at a single airport states that airlines are very good at adapting to emergent disruptions to minimize the impact on future operations and revenue.

In a study on the impact of a cyber failure in health care, we have also found resiliency (Dynes, 2007). The organization studied consists of several hospitals and clinics, including a teaching hospital incorporating many specialty services and a trauma center. That organization was affected by the August '05 Zotob worm. The worm event lasted three days and resulted in a complete disconnection from the internet along with internal network failures. The hospital was highly reliant on information infrastructure and many units experienced major operational disruptions as a result of the worm. However, despite cyber failure, the hospital found work-arounds and experienced little impact in terms of productivity or patient care quality.

Of course, a widespread internet outage affecting many firms would be much more disruptive. And as more firms become increasingly dependent on the internet for order placement and processing, the disruptions will grow. For example, the general manager at Supplier G, which at the time of the interview did not have a web site and relied on the internet only for mail, was working to enable EDI transmissions in the near future. This does not necessarily mean that small firms will become vulnerable with respect to internet disruptions; their small scale and current reliance on phone and fax for running their business makes it highly likely they would be able resume those activities with little or no disruption in their ability to produce and ship product. This is borne out by Supplier D, who in conversation with the automobile parts manufacturer decided not to implement EDI to transact business due to the limited volume of business between the two firms. Nevertheless, many such firms are being migrated to simple web-portals that are subject to disruption – not at the supplier itself, but in their customer's ability to post orders. Supply chains are steadily becoming more reliant on the internet and the potential for production disruption from cyber events will grow.

References

Cashell, B., Jackson, W.D., Jickling, M. and Webel, B. (2004), "The economic impact of cyber-attacks", Congressional Research Service Documents, CRS RL32331, Washington, DC.

Croxton, K.L. (2002), "The order fulfillment process", *International Journal of Logistics Management*, Vol. 14 No. 1, pp. 19-32.

Davis, E.W. and Spekman, R.E. (2004), *Extended Enterprise*, FT Prentice-Hall, New York, NY.

DoC (1997), *Regional Multipliers: A User Handbook for the Regional Input-Output Modeling System (RIMS II)*, US Department of Commerce, Bureau of Economic Analysis, US Government Printing Office, Washington, DC.

DoC (1998), *Benchmark Input-Output Accounts of the United States, 1992*, US Department of Commerce, Bureau of Economic Analysis, US Government Printing Office, Washington, DC.

Dynes, S. (2006), "Information security investment case study: the manufacturing sector", CDS Report, Tuck School of Business, Dartmouth College, Hanover, NH, available at: http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecManufacturing.pdf

Dynes, S. (2007), "Information security and health care – a field study of a hospital after a worm event", CDS Report, Tuck School of Business, Dartmouth College, Hanover, NH, available at: http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecHealthCare.pdf

Dynes, S., Brechbühl, H. and Johnson, M.E. (2005), "Information security in the extended enterprise: some initial results from a field study of an industrial firm", paper presented at

Workshop on the Economics of Information Security, Harvard University, Cambridge, MA, June.

Evans, P. and Wolf, B. (2005), "Collaboration rules", *Harvard Business Review*, Vol. 83 Nos 7/8, pp. 96-104.

Gentile, G. (2002), "Container backlog may leave Santa at the dock", *Seattle Post-Intelligencer*, Associated Press, New York, NY.

Gianoukos, D., Fox, M. and Abdel-Misih, R. (2002), "Toy review 2002", *JP Morgan*, December 12.

Gurium, J.F. and Holstein, J.A. (2002), *Handbook of Interview Research*, Sage, London.

Haimes, Y.Y., Horowitz, B.M., Lambert, J.H., Santos, J.R., Crowther, K.G. and Lian, C. (2005), "Inoperability input-output model (IIM) for interdependent infrastructure sectors I: theory and methodology", *Journal of Infrastructure Systems*, Vol. 11 No. 2, pp. 67-79.

Hayes, R.H. and Wheelwright, S.C. (1979), "Link manufacturing process and product life cycles", *Harvard Business Review*, Vol. 57 No. 1, pp. 133-40.

Isidore, C.V. (2002), "West coast ports reopen", *CNN/Money*, October 9.

Johnson, M.E. (2005), "A broader context for information security", *Financial Times*, September 16, p. 4.

Johnson, M.E. and Goetz, E. (2007), "Embedding information security risk management into the extended enterprise", *IEEE Security and Privacy*, Vol. 5 No. 3, pp. 16-24.

Kunreuther, H. (2002), "Interdependent security: the case of identical agents", paper presented at National Bureau of Economic Research, Insurance Project Workshop, Cambridge, MA, February 1.

Kunreuther, H. (2004), "Risk analysis and risk management in an uncertain world", Wharton School Working Paper, Forthcoming in *Risk Analysis*.

Lambert, D.M. (2006), *Supply Chain Management, Processes, Partnerships, Performance*, 2nd ed., Supply Chain Management Institute, Sarasota, FL.

Leontief, W.W. (1966), *Input-output Economics*, Oxford University Press, New York, NY.

Mattel (2002) Annual Report, Mattel, El Segundo, CA.

Santos, J.R. and Haimes, Y.Y. (2004), "Modeling the demand reduction input-output inoperability due to terrorism of interconnected infrastructures", *Risk Analysis*, Vol. 24 No. 6, pp. 1437-51.

Shavell, Z. (2000), *The Effects of Schedule Disruptions on the Economics of Airline Operations*, MITRE Corporation, Bedford, MA, available at: www.mitrecaasd.org/library/documents/shavell.pdf

Sheffi, Y. (2005), *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, MIT Press, Cambridge, MA.

Yin, R.K. (1994), *Case Study Research: Design and Methods*, 2nd ed., Sage, Thousand Oaks, CA.

Further reading

Dynes, S., Andrijcic, E. and Johnson, M.E. (2006), "Costs to the US economy of information infrastructure failures: estimates from field studies and economic data", Paper presented at Workshop on the Economics of Information Security, Cambridge University, Cambridge, MA, June.

Goldsby, T.L. and Garcia-Dastugue, S.J. (2003), "The manufacturing flow management process", *International Journal of Logistics Management*, Vol. 14 No. 2, pp. 33-52.

Haimes, Y.Y. and Jiang, P. (2001), "Leontief-based model of risk in complex interconnected infrastructures", *ASCE Journal of Infrastructure Systems*, Vol. 7 No. 1, pp. 1-12.

Haimes, Y.Y., Horowitz, B.M., Lambert, J.H., Santos, J.R., Crowther, K.G. and Lian, C. (2005), "Inoperability input-output model (IIM) for interdependent infrastructure sectors II: case study", *Journal of Infrastructure Systems*, Vol. 11 No. 2, pp. 80-92.

Lian, C. and Haimes, Y.Y. (2006), "Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input-output model", *Systems Engineering*, Vol. 9 No. 3, pp. 241-58.

About the authors

Scott Dynes is a Senior Research Fellow at Tuck's Glassmeyer/McNamee Center for Digital Strategies. His current research interests include conducting field study exploring how firms identify and manage the risks they face as a result of their use of information technologies, both internally as well as in their extended enterprise; he is also interested in policy issues to promote resiliency in critical infrastructures. He has presented his research at numerous conferences and has published articles have appeared in journals as diverse as *Hearing Research* and the *Journal of Visual Languages and Computing*. He holds a PhD in Physics from MIT.

M. Eric Johnson is Director of Tuck's Glassmeyer/McNamee Center for Digital Strategies and Professor of operations management at the Tuck School of Business, Dartmouth College. His teaching and research focuses on the impact of information technology on supply chain management. He is currently studying how information security and trust effect supply chain relationships. His research articles have appeared in such academic journals as *Management Science, Operations Research, IEEE Security and Privacy, Communications of the ACM, Production and Operations Management, Manufacturing and Service Operations Management*, and *Transportation Science*. He holds PhD in Engineering from Stanford University. M. Eric Johnson is the corresponding author and can be contacted at: m.eric.johnson@dartmouth.edu

Eva Andrijcic holds a Master of Science degree in Systems Engineering from University of Virginia. Her research focusing on the creation of a macro-economic framework for evaluation of cyber security risks related to protection of intellectual property was published in *Risk Analysis: An International Journal*.

Barry Horowitz is currently a Professor in the Systems and Information Engineering Department at the University of Virginia. He also is the Research Site Director of UVa's Wireless Internet Center for Advanced Technology, an Industry/University Collaborative Research Center Sponsored by the National Science Foundation.