22 Resilience to a Cyber-Attack on the Detroit Automobile Industry

A Computable General Equilibrium Approach

Adam Rose and Zhenhua Chen

Introduction

The world has become increasingly dependent on cyber activity due to a combination of globalization and technological advances. The gains in economic productivity have been immense. However, there is a growing realization of the increased vulnerability of businesses, markets, national economies, and global trade to cyber threats from terrorism, natural disasters, and technological accidents. These risks will continue to grow, as economic reliance on connected systems continues to advance, as user bases expand, and as more physical devices gain cyber components. As these vulnerabilities grow, so does the need to understand how to limit losses associated with them. This chapter develops and applies an economic framework for the analysis and measurement of ways for businesses to recover from cyber disruptions. We refer to the ability to recover as resilience. We illustrate these concepts in the context of the Detroit Metropolitan Statistical Area (MSA) economy and its resurgent automobile manufacturing sector on which much hope is placed to restore the city to its once great urban empire status.

There are several possible motives and impacts of cyber-attacks, including cyber-crime and malicious actions. Here we focus on instances of significant loss of functionality of a cyber-system itself or the system it helps operate. The latter translates into direct and indirect loss of output (sales revenue and profits) and loss of employment, and is often referred to as business interruption (BI). BI starts when the cyber-attack strikes but continues until the system and its host economy recover. Post-disaster business continuity (resilience) strategies that enable a system to rebound more efficiently and quickly hold the prospects of greatly reducing BI. This is all the more important, as it is generally recognized that it is impossible to fully mitigate many cyber threats up front (NRC, 2017).

There are numerous resilience tactics on both the cyber service provider side and customer side, many of which are relatively inexpensive. The latter include back-up data storage and equipment, substitutes for standard cyber components, conserving on cyber needs, and recapturing lost production once the cyber capability is restored. They are definitely much less expensive than the major supplier tactic of system redundancy (Rose, 2017).

The purpose of this research is to address the following questions: (1) What are the economic consequences of a cyber-attack on the automobile manufacturing sector measured in terms of GDP and (2) What are the impacts of the potentials of various cyber-resilience tactics to reduce losses. The overall objective of this research is to improve risk management for cyber-threats among both private and public sectors through a better understanding of the economic consequence of cyber-attacks and the benefits of various cyber resilience tactics in reducing these consequences. This objective is implemented in three stages: (1) estimation of direct effectiveness and costs of post-attack cyber resilience tactics, (2) adaptation of a state-of-the-art economic impact modeling approach to address cyber-attack consequences and resilience potential at both the microeconomic and macroeconomic levels, and (3) an empirical assessment of cyber-resilience to provide insights for decision-makers to enhance resilience to cyber-attacks.

We apply our methodology to a cyber-attack on the automobile manufacturing sector in the Detroit Metropolitan Area. We have chosen Detroit because it was once an urban empire. We have chosen the auto industry because it is still so prominent in Detroit and critical to the city's revival. It is also concentrated geographically, and is an iconic part of the U.S. economy, so hence an ideal industrial target for terrorists. We note that manufacturing of all types of motor vehicles is the endpoint of a supply chain consisting of several elements, including basic fabrication of a sequence of components and final product assembly. It is highly dependent on computerization of production and ordering, much of which, especially the latter, is dependent on internet and related services. Although, cyber services as a whole comprise only a small portion of the inputs to automobile manufacturing, their disruptions can bring it to a halt in the absence resilient responses. We simulate a base case disruption without resilience and then perform various comparative static analyses of the ability of each of six major resilience tactics to reduce BI losses.

The rest of this chapter is organized as follows. Section "Literature Review" reviews the relevant literature. Section "Resilience" provides a more detailed definition of economic resilience and a framework for the analysis. Section "Methodology" provides an evaluation of the effectiveness of major tactics and how they can be incorporated into a CGE model. In section "Detroit, an Urban Empire Built on the Automobile Industry", we present a discussion of the studied area – Detroit, the automobile industry and the role of cyber services in the auto industry. Section "The Role of Cyber Services in Motor Vehicle Manufacturing" provides a summary of the make-up of the USCGE Model used for the simulations. In addition, the results of a ten-day cyber-attack on automobile and parts manufacturers in the Detroit Metropolitan Area are also presented. Section "Simulations and Results" concludes with some recommendations for future research.

Literature Review

Various approaches have been applied to evaluate the economic consequence of cyber-attacks. For instance, Cashell et al. (2004) discussed the economic impact of cyber-attacks with a focus on the cost of attacks. Although their study provided a pioneering survey of the existing literature pertaining to the impact of cyber-attacks, the discussions were primarily about direct economic losses of cyber-attacks, whereas the indirect impacts were ignored. Hua and Bapna (2003) further investigated the impact of cyber-terrorism using a game theory simulation method. But again, the focus was on impact of cyber-attacks on cyber security investment rather than the impact of attack on the macro-economy. The only relevant study to the economic impact assessment of cyber-attacks on auto manufacturing was conducted by Dynes et al. (2007), in which an input-output model was applied to a hypothetical cyber-attack scenario. Their study found that, although the critical sectors in supply chains, such as auto manufacturing can be significantly impacted by certain cyber disruptions, information technology can help the system be resilient to these disruptions.

Although there have been many studies of the direct impacts of cyber threats on individual industries, nearly all of them relate to cybercrime, primarily theft of data or malicious activity. The only major studies on macroeconomic impacts relate to the stock market. Moreover, nearly all the studies of cyber resilience are limited to pre-threat mitigation (Onyeji et al., 2014), whereas there is a lack of attention on post-threat response.

Our study fills a major void in the literature by analyzing economic impacts of cyber-terrorism on a critical economic sector using auto manufacturing as an example and the implications for the economy as a whole. Moreover, the focus of our analysis is on post-disaster resilience, i.e., on loss reduction by various relatively inexpensive tactics such as back-up data storage, alternative technologies, and the relocation of economic activity.

Resilience

Researchers and decision-makers in the disaster field are evenly split on the definition of resilience. One group utilizes the concept to refer to any action taken to reduce disaster losses. This group, with a large representation by engineers, focuses primarily on mitigation with an eye to reducing the frequency and magnitude of disasters and strengthening property to prevent damage (see, e.g., Bruneau et al., 2003). This broad definition has also been adopted and applied across the board by major panels assessing resilience research and practice, such as the National Research Council, which defines resilience as: "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events" (NRC, 2012; p. 16).

The other group, with a large representation by social scientists, focuses primarily on actions implemented after the disaster strikes (Rose, 2007; Tierney, 2007; Cutter, 2016). This group takes the meaning of resilience more literally, referring to its Latin language root, whose definition is "to rebound". They also acknowledge that resilience is a process, whereby steps can be taken before the disaster to build resilience capacity, but resilient actions do not take place until afterward. Examples would include emergency drills, purchase of back-up electricity generators, and lining up alternative suppliers of critical inputs. In each case, the action serves no benefit before a disaster takes place but lowers the interruption of key business services when a disaster takes place. Here the focus is not on property damage, which has already taken place, but rather the reduction in the loss of the *flow of goods and services* emanating from property, or *capital stock*. The former is often measured in terms of gross domestic product (GDP) and employment, and is typically referred to as business interruption, or BI (Tierney, 1997). BI just begins at the point when the disaster strikes, but continues until the system has recovered or reached a "new normal" which is typically coming to be considered a "sustainable" level of activity (meaning a healthy economy). Measuring BI is thus much more complicated, because it involves matters of the duration and time-path of recovery, both of which are strongly affected by the behavioral responses of public and private decision-makers (Rose, 2015).

Defining Economic Resilience

There are many definitions of resilience, but Rose (2009) and others have found more commonalities than differences. We offer the following general definitions of resilience, which capture the essence of the concept, and then follow them up with definitions that capture the essence of economic considerations. Following Rose (2004, 2009), we distinguish two major categories of resilience:

In general, Static Resilience refers to the ability of the system to maintain a high level of functioning when shocked (Holling, 1973). *Static Economic Resilience* is the efficient use of remaining resources at a given point in time. It refers to the core economic concept of coping with resource scarcity, which is exacerbated under disaster conditions.

In general, Dynamic Resilience refers to the ability and speed of the system to recover (Pimm, 1984). *Dynamic Economic Resilience* is the efficient use of resources over time for investment in repair and reconstruction. Investment is a time-related phenomenon – the act of setting aside resources that could potentially be used for current consumption in order to re-establish productivity in the future. Static Economic Resilience does not completely restore damaged capacity and is therefore not likely to lead to complete recovery.

Note that economic resilience can take place at three levels of analysis:

- Microeconomic (operation of individual businesses, households, government agencies, e.g., conservation of or substitution for critical inputs, use of inventories or excess capacity, relocation, production rescheduling);
- Mesoeconomic (operation of industries and markets, e.g., the resource allocating mechanism of the price system);
- Macroeconomic (operation of the economy, e.g., supply-chain adjustments, importation of critical inputs, fiscal and monetary policy).

Another important delineation in economic resilience, and resilience in general, is the distinction between inherent and adaptive resilience (Tierney, 2007; Cutter, 2016). Inherent resilience refers to resilience capacity already built into the system, such as the ability to utilize more than one fuel in an electricity generating unit, the workings of the market system in offering price signals to identify scarcity and value, and established government policy levers. Adaptive resilience is exemplified by undertaking conservation that was not previously thought possible, changing technology, devising market mechanisms where they might not previously existed (e.g., reliability premiums for electricity or water delivery), or devising new government post-disaster assistance programs. It is important to realize that a good amount of resilience is already embodied in the economy at various levels (e.g., a firm's ability to substitute inputs, market signals for reallocating resources), and that policies should be designed to capitalize rather than obstruct or duplicate this capacity. At the same time, policy should also be geared to rewarding both types of resilience

An Operational Metric

The next step is to translate these definitions into something we can measure. For static resilience, this can be done in terms of the amount of BI prevented by the implementation of a given resilience tactic or set of tactics comprising a resilience strategy. For dynamic resilience, the metric would be the reduction in recovery time in addition to the reduction in BI, though obviously the former influences the latter. In both cases one needs to establish a reference point or baseline to perform the measurement. For static resilience, this would be the maximum potential BI loss in the absence of the resilience tactic, while for dynamic resilience it would be the duration and time-path of economic activity in the absence of resilience in relation to investment in repair and reconstruction.

Several studies have measured resilience using this and related metrics. Rose et al. (2009) found that potential BI losses were reduced by 72% by the rapid relocation of businesses following the September 11, 2001 terrorist attacks on the World Trade Center. Rose and Wei (2013) found that a reduction in potential BI from a nine-month closure of a major U.S. seaport could be as high as 66% from the implementation of several types of static resilience, most notably ship rerouting, use of inventories, and production rescheduling). Xie et al. (2018) estimated that BI losses could have been reduced by 30% and recovery time by one year by dynamic resilience through an increase in investment funds and acceleration of their timing in the aftermath of the Wenchuan earthquake in China.

Other studies have found extensive potential of economic resilience. Kajitani and Tatano (2009) found extensive resilience possibilities among Japanese manufacturing firms in response to utility lifelines disruptions caused by disasters. Specialized studies have developed methodologies for examining potential of specific resilience strategies, such as use of inventories (Barker and Santos, 2010).

Methodology

A Computable General Equilibrium (CGE) analysis is introduced to evaluate the economic consequence of cyber-attack and cyber resilience. CGE is the state-of-the-art approach to macroeconomic simulation modeling. It is a multi-market model of the behavioral responses of individual producers and consumers to changes in prices, technology, taxes, and other external shocks, subject to the constraints on capital, labor, natural resources (Dixon and Rimmer, 2002). Essentially, CGE characterizes the economy as a set of interconnected supply chains. It represents a significant advance over its predecessor, input-output (I-O) analysis, by maintaining I-O model's strengths, such as fully accounting of all inputs, multi-sector details, focusing on interdependencies. It also overcomes the limitations of linearity, lack of behavioral content, and omission of markets and prices (Rose, 1995). CGE models have been used extensively to model various types of disasters (see, e.g., Dixon et al., 2011; Rose, 2015; Sue Wing et al., 2015), including considerations of resilience (see, e.g., Rose and Liao, 2005; Rose et al., 2017; Chen and Rose, 2018).

An enhanced version of the USCGE model is adopted for this assessment.[1] The model consists of 58 producing sectors, along with multiple institutions: nine household income groups, three government actors (two federal and one state and local), and external agents (i.e., foreign producers). The model has been applied to economic consequence analysis of various threat types, including human-related disasters, natural hazards, and technological system failure. The most recent applications of the USCGE model was the estimation of economic consequences of aviation system disruptions (Chen et al., 2017) and transportation system failure due to Hurricane Katrina (Chen and Rose, 2018).

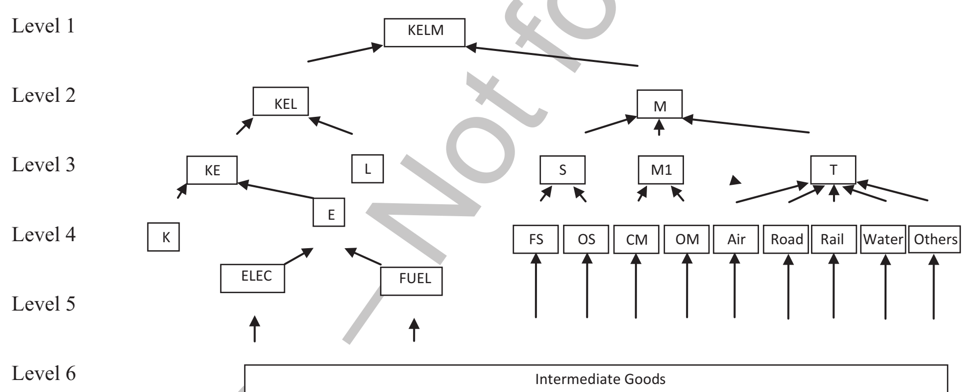
The production function of the model is that of a constant elasticity of substitution (CES) form as in Equation (1):

$$Q_i = \left[\alpha_{kl} K_i^{\frac{\alpha_{kl}-1}{\alpha_{kl}}} + \left(1-\alpha_{kl}\right) L_i^{\frac{\alpha_{kl}-1}{\alpha_{kl}}} \right]^{\frac{\alpha_{kl}}{\alpha_{kl}-1}} \qquad (1)$$

where Q_i denotes the output of sector *i*, *K* and *L* denote capital and labor input in sector *i*. α_{kl} and σ_{kl} represent the input share parameter and the constant elasticity of substitution, respectively. The production function is a hierarchical one, representing sequential decision-making relating to the choice of input combinations in each tier or "nest". Figure 22.1 illustrates the nesting structure of the model, which is a revision based on Rose et al. (2009), disaggregated to reflect substitution among various intermediate sectors.

To translate the various direct impacts caused by the transportation system failure to relevant CGE shock requires identifying appropriate exogenous variables in the USCGE model for each direct impact driver. In our methodology, ordinary direct impacts in terms of infrastructure damages are modeled as capital stock reductions. Labor shocks as a result of death and injuries are not included in this study because they were not extensive enough to affect the service ability of the transportation system itself.

The cyber-attack shock to the auto manufacturing sector was implemented by adjusting the factor productivity parameter at the KELM level for that sector by the amount calculated from the direct impact drivers. On the other hand, cyber resilience is implemented by changing the factor productivity parameter at the fourth level of the nesting structure of the Other Services sector (of which cyber services are a part).



L = Labor	T = Transport	FS = Finance	Air = Air Transport
K = Capital	S = Services	CM = Chemicals	Road = Road Transport
E = Energy	M = Materials	OM = Other Materials	Rail = Rail Transport
FUEL= Fossil Fuels		M1 = Materials Sub	Water = Water Transport
ELEC = Electricity		OS = Other Services	Others = Other Transport Services

Figure 22.1 USCGE Production Nesting Structure.

Indirect impacts caused by a direct change of output are modeled through a combination of backward and forward linkage (supply-chain) effects with other intermediate sectors and the consumer response to the final demand price change, both stemming from a factor productivity parameter adjustment. The determination of the price of final demand is denoted as:

$$\text{PDMD}_{\text{fi},i} = \delta_{\text{fi},\,i} \cdot \text{PDMD0}_{\text{fi},i} \cdot \sum_{\text{inpt}} \left(sh_{i,\text{inpt}} \left(\frac{\text{PDMD}_{\text{inpt},i}}{\text{PDMD0}_{\text{inpt},i}} \right)^{1-\sigma_{i,\text{fi}}} \right)^{\frac{1}{1-\sigma_{i,\text{fi}}}} \tag{2}$$

where PDMD is the demand price; fi and inpt are composite factor inputs, with fi representing the upper level in a nest and inpt representing the lower level in a nest. For example, KELM (the capital, energy, labor, and materials nest) is fi to the inpt of KEL (capital, energy, and labor nest) and MAT (material nest); δ is the factor productivity, initially set to 1 across all nests and with respect to all sectors by default.

International trade is represented through an Armington substitution function between imports and domestic production (meaning that imports and good produced in the U.S. are imperfect substitutes). A constant elasticity of transformation function represents the substitution between exports and domestic sales. Input and import substitution elasticity values have been sourced and checked against the literature on these parameters. Household consumption is represented by a Linear Expenditure System of aggregate commodities. A Social Accounting Matrix of the U.S. national economy in Year 2012 from IMPLAN forms the empirical core of the model.

Nevertheless, the USCGE model is subject to the standard limitations of most CGE models. First, for the most part, it assumes the economy is in equilibrium, though we do incorporate disequilibrium in the supply of automobiles and parts, as well as in the labor market (unemployment equilibrium). Second, the model is static, so that it does not trace the time-path of impacts, including various economic cycles associated with employment and investment changes. Third, the model construction is based on a deterministic approach on the basis of a single base year of data (in contrast to the superior approach of econometric models, which use time series data and have goodness of fit measures).

Detroit, an Urban Empire Built on the Automobile Industry

In its heyday, Detroit was a prototypical 20th century American city. At the beginning of the last century, it was the site of ship and railroad car building and much small-scale manufacturing. However, rapid advances in automobile technology, the advent of mass production in the industry, its entrepreneurs, and comparative advantage (stemming from its manufacturing tradition and skilled workforce and location near major rail systems and waterways), soon turned it into the "Motor City", housing most of the major automobile manufacturers in the U.S. It is a classic example of the "Second Urban Revolution", which linked urbanization and industrialization into the "industrial city" (Short, 2012). By 1950, it became the fifth largest city in the U.S. Its past and present are closely tied to the automobile industry (Sugrue, 2007), and its future revitalization may be as well. Orum (2014) and others refer to Detroit as an urban empire, though not necessarily a global city like New York, Hong Kong, or Paris.

Detroit also prospered in the past because of the relatively high wages paid to autoworkers. This began with Henry Ford's realization that highly paid workers would purchase his automobiles and stimulate the local economy in general (Kennedy, 2011). This trend continued with unionization, though the racial segmentation of this institution was a foundation for tensions that have plagued the City for many years. The high wages were also a major reason for the automobile industry's decline in the City due to cost pressures that accelerated automation and caused automobile manufacturers to shift their operations to lower-wage areas. The industry's demise was further accelerated by the Arab Oil Embargo and subsequence oil/gasoline price hikes and by foreign competition. A brief resurgence of the industry in the 1990s (in part because of a downturn in gasoline prices) was cut short by the Great Recession, which resulted in bankruptcies of Chrysler and General Motors (Sugrue, 2007). Currently, the auto industry represents about 12% of Detroit's GDP.

Of course, Detroit's ills are not solely based on economics but also on historical planning decisions that backfired. One of the main examples is a transportation network that radiated outward from the city center, the Homer Hoyt paradigm of the preferred urban form. Unfortunately, this helped accelerate the movement to the suburbs by more wealthy white resident commuters. This short-circuited the inner city property value increases (Kennedy, 2011) and eventually led to the "hollowing out" of the city with the demise of the automobile industry in the latter quarter of the 20th century.

Some analysts have suggested that Detroit is in a difficult position and may have to continue to pin its hopes on the automobile industry. Orum (2014, p. 179) has noted that "some cities are simply less well-positioned to expand and connect to other cities in this new age because of the heavy burdens they possess owing to their success as industrial urban empires. He goes on to note that Detroit cannot readily pivot to management consulting and finance, as have other resurgent cities. At the same time, one might note that some, perhaps most notably Pittsburgh, have overcome their traditional dominant-industry heritage, though the move to a high technology center was facilitated by the presence of two leading universities, assets that Detroit lacks.

The situation is indeed ironic because several analysts, using the analogy of an eco-system, have pointed to Detroit as a classic example of a city lacking resilience to shocks because of its lack of economic sectoral diversity (Jacobs, 2011; Kennedy, 2011). Thus, future economic development needs to find ways to diversify its economy, though the automobile will remain at its core for the foreseeable future.

The automobile industry in Detroit and elsewhere faces continued strong competition and is very vulnerable to external shocks, such as a cyber-attack. Increased automation and just-in-time inventory practices make production less flexible to changes in inputs and their timing and hence less resilient. Specialization has decentralized automobile components and parts to neighboring areas, including Canada. It is not unusual for there to be six or more supply-chain links (production by separate factories) in the production of parts and in the assembly of components and complete automobiles. This makes production even more dependent on cyber technology, not just for manufacturing production lines but also for ordering and logistical routing of parts and components.

The Role of Cyber Services in Motor Vehicle Manufacturing

Motor-vehicle assembly in the U.S. is primarily driven by out-sourced processes. It is thus highly dependent on the integration of various sub-assemblies in over many locations in the following major categories: Development, Sub-Assembly, Assembly, and Inspection. The final product is integrated by remotely controlled robotic systems and skilled employees, together with Just-in-Time (JIT) inventory practices to acquire production inputs (Carlton, n.d.; Genta and Genta, 2014).

The motor manufacturing industry is moving towards an industrial internet of things, as the industry implements interactive remotely programmed and controlled autonomous robots that are becoming more autonomous and flexible. To monitor vehicle manufacturing operations and progress in its assembly, each of the components is labeled with either a Vehicle Identification Number (VIN), small radio frequency transponders, or sensors attached to the parts. The production process is organized in a vertical automation pyramid where parts are labeled so that operators can identify stages of vehicle production (Rüßmann et al., 2015). Some manufacturers are using embedded computing in their vertical automation pyramids to be able to feed more information in the process control system. Specifically, the incorporation of data analytics contributes to the optimization of production based on the analysis of the data collected from the identification codes embedded in the parts that go through the production line. Data analytics are becoming standard practice to support real-time decision-making (Rüßmann et al., 2015). To deliver data and to analyze it, digital interconnection between data sources and data software is required.

The supply chain of Motor Vehicle Parts is characterized as being clustered. Also, the motor industry has moved towards the minimization of costs through the implementation of JIT purchasing to reduce flow and response times between suppliers and customers and hence the need for inventories. This logistic approach requires a frequent exchange of orders and receipts between buyers and suppliers. Thus, the industry has implemented a system known as electronic data interchange (EDI), a tool to facilitate exchange between plants at a rapid pace (EDI Basics, 2017).

The structure of the auto-motor supply chain requires the use of internet communication protocols. Among the most popular between Auto-makers is the Odette File Transfer Protocol (OFTP), which offers secure exchange of documents using encryption and the exchange of digital certificates. EDI also facilitates the delivery of large CAD files through the internet. Bar codes, Kanban, and identification labels contribute greatly to managing shipments of materials for the production of auto-motors. The final assembly process requires the collection of various parts of the vehicle that are delivered using the EDI (EDI Basics, 2017).

Motor-vehicle manufacturers are also using cloud-based software for some enterprise and analytic applications, which involves more data sharing across entities in the supply-chain, which has sped up their interaction. Consequently, production process data are becoming increasingly cloud-based. Even systems that monitor and control these processes may become so (Rüßmann et al., 2015).

There are two kinds of suppliers that involve cyber-connections in production assembly lines: suppliers of material and suppliers of systems. The first uses sensors, labels, EDI, and cyber connections to supply material and to exchange information related to purchase orders. The second sources software and system updates. Because the motor-vehicle industry has become very customized, the supply of physical products involves the participation of different certified suppliers identified as Original Equipment Manufacturers (OEMs) that satisfy needs by progressively moving independently (Genta and Genta, 2014). Motor vehicle manufacturing also requires greater connectivity, interaction, and systems in factories. For this reason, manufacturing-system suppliers play a major role in the industry by offering IT products that update or permit the functionality of the robots, sensors, embedded devices, controls, and performance monitors. In

Table 22.1 Sectoral and Regional Share of Auto Manufacturing and Cyber Sectors (2012)

	Gross Output (Millions of Dollars)			*Share of National Gross Output*		
Sector	*National*	*Michigan*	*Detroit MSA*	*National*	*Michigan*	*Detroit MSA*
Automobile manufacturing	510,780	56,568[a]	38,023[a]	0.0178	0.0025	0.0013
Telecommunication	370,794	16,182[a]	8,689[a]	0.0261	0.0006	0.0003
Total sectors	28,663,246	947,299	466,327	1.0000	0.0345	0.0170

Source: National and Regional Data – U.S. Bureau of Economic Analysis and IMPLAN.

[a] The number is adjusted for both variations in price and quantity based on 2016 gross output data obtained from IMPLAN. The price adjustment is based on the BEA deflator, whereas the quantity adjustment is based on the employment ratio between 2016 and 2012 provided by the U.S. Bureau of Labor Statistics.

addition, online portals for downloading software and partner relationships offer flexible equipment configurations for production.

Finally, because automobile components are produced at various sites, this necessitates quality control. Quality audits, using cyber capabilities, are performed by parts suppliers and assembly plants to exchange data about the parts, to test them, and/or to simulate their use. Quality control processes during the final manufacturing stage include: inspection, balance, force variation, and X-ray, all of which utilize cyber services (Duchamp et al., 2016).

One should note that understanding of role of cyber services in auto manufacturing is important, as it provides a foundation for the development of an analytical framework to evaluate the economic consequence of resilience to a cyber-attack on Detroit's automobile industry. Specifically, the focus of our assessment is on the Automobile Manufacturing sector in the Detroit-Warren-Dearborn Metropolitan Statistical Area in Michigan. Table 22.1 provides the sectoral and regional levels and shares (proportions) of both auto manufacturing and cyber sectors in Michigan and the Detroit Metro Area, in relation to the national economy. The industrial share of national GDP in the Detroit MSA is used to scale the direct impact drivers for the simulations in a national CGE model.

The Potential of Resilience against Cyber-Attacks in Auto Manufacturing

Six major resilience tactics to recover from a cyber-disruption caused by a terrorist attack in the Automobile Manufacturing Industry in the Detroit MSA are presented in Table 22.2. The tactics are specific to a disruption of Telecommunication Services narrowly defined (as opposed to curtailment of Data services, Internet Publishing, or Broadcasting). Specifically, we are focusing on a disruption of both external and internal internet access by firms engaged in the production of motor vehicles. The six resilience tactics are only half of the dozen tactics identified by Rose (2009), but we confine our attention to those that are likely to have the greatest effect on muting business interruption losses in this case and those that can be quantified.

General definitions of the tactics are as follows, with specific examples applicable to telecommunications disruptions presented in the second column of Table 22.2:

- *Conservation* is maintaining production with fewer inputs
- *Input substitution* is shifting input combinations to achieve the same function or level of productivity

Table 22.2 Cyber Resilience Tactics for Manufacturing: Assumptions, Parameter Values and CGE Loss Adjustment Methods

Resilience Tactic	*Assumptions and Parameters*	*CGE Loss Adjustment Method*
Conservation	Likely to be very low, since majority of uses are essential in factories = 2%	Reduce disruption in Auto Sector through upward adjustment in Telecommunications input productivity parameter
Input Substitution	Rose and Miller (2017): low to moderate: 20% or 35% reduction of disruption	Ideal is L or M substitution for K or Adjust Telecom input productivity parameter upward
Relocation	Determine excess auto sector capacity elsewhere by make/model = 5%	Apply direct percentage to gross output or GDP reductions
Inventories	Determine (non-cloud) data back-up in the Auto sector = 5%	Adjust Telecom input productivity parameter upward
Production Isolation	Use Telephone Importance Factor = 5%	Adjust Telecom input productivity parameter upward
Production Recapture	Adjust Recapture Factors for implementation obstacles = 49%	Apply direct percentage to gross output or GDP reductions

Source: Authors' summary.

- *Relocation* refers to changing the site of business activity
- *Inventories* include both emergency stockpiles and ordinary working supplies of production inputs
- *Resource isolation* refers to the portion of business operation that can continue without a critical input
- *Production recapture* refers to working overtime or extra shifts to recoup lost production.

Note that the parameter values vary by tactic and disruption characteristic as follows:

Conservation – In this case, conservation can be attained at little additional cost, or even cost-savings by simply reducing telecommunications to essential use, in cases where the telecommunications disruption is not total. However, non-essential uses are limited on assembly lines and their support functions in the factory so we assume conservation potential to be only 2%, i.e., the auto industry is only able to do without 2% of the cyber input without a loss in productivity.

Input Substitution – According to the various input substitution options presented in Rose and Miller (2017), 20% to 35% of the direct service disruptions can be prevented, over the seven-day period. Moreover, the costs are estimated to be rather low. Another type of input substitution could come from using text rather than voice or other internet connectivity. The potential here decreases over time, as the high potential at first is due to the initial spike in use of telecom to communicate the outage (both internally and external to the factory) and to determine cause of the disruption. Cost is likely to be low, because of existing contracting with alternative communication providers and excess capacity in their services.

Relocation – The potential effectiveness of this tactic is stifled a bit by the fact that the specialized nature of automobile manufacturing means that production can be transferred only to branch plants that produce the same make and model as the plants being disrupted. There are only four automobile plants in the Detroit Metro Area and they are specialized to certain makes of cars. Moreover, a plant dedicated to one or several models cannot be transformed in a short period to produce other models. Also, there is little duplication of models produced in Detroit throughout the country. The only real Relocation option is for Jeep Cherokees produced in Belvidere, Illinois. Given the capacity at the Detroit factory and the capacity at the Illinois factory, we estimate the relocation potential to reduce the direct disruption for this one make by 5%. The cost is difficult to determine but likely to be low.

Data Inventories – This tactic is limited to the extent that local copies of data exist, but the advent of data clouds has significantly reduced this option. Note, however, that clouds themselves are not relevant here because internet access is necessary to retrieve the data from them. Hence, we estimate this as only 5%. The cost is very low – storage fees.

Production Isolation – This is likely to be rather low in a high-tech industry such as Automobile Manufacturing. We estimate it to be 5%. The cost is zero, since this is a case of naturally occurring inherent resilience.

Production Recapture – Recapture factors have been standard in the literature for 20 years (see, e.g., FEMA, 1997; Rose and Lim, 2002). However, two adjustments were considered in this case. First, is the extent of excess production capacity that can be worked overtime or extra shifts. However, even if this is small, given the short duration of the disruption in this case, the lost production that needs to be recaptured is not likely to strain the excess capacity. Still, standard recapture factors really represent recapture potential, and thus we adjust the factor values downward by 50% to a recapture factor of 49% for Auto Manufacturing to represent the consideration of obstacles to efficient implementation. The cost is over-time pay.[2]

The methodologies for incorporating resilience are presented in the last column of Table 22.2. The majority of the adjustments are simply to reduce the direct disruption by the percentage Conservation, Relocation, Inventories, or Production Isolation. Alternatively, Conservation can be modeled as an adjustment of the productivity parameter for Telecommunications in the Auto sector. Ideally, Input Substitution would be modeled within the substitution possibilities of the constant elasticity of substitution production functions in the CGE model, if there is sufficient disaggregation of cyber sectors. However, our model is not sufficiently disaggregated, so we use the alternative of reducing the direct disruption by the percentages presented in the Table. Production Recapture on the other hand is simply a scalar factor applied to the loss of gross output or value added caused by the cyber-attacks.

Simulations and Results

The CGE simulations for a ten-day disruption of the Auto Manufacturing sector due to a cyber-attack on its distributed control system (DCS) are based on the following assumptions:

1 The DCS cyber-attack would cause a 50% reduction of automobile production in the Detroit MSA for ten days. This is based on the direct effect on output of the Automobile Manufacturing sector from the refinement of previous work by others.[3] Because we are "downscaling" impacts from a national CGE model to the Detroit Region, the direct impact we simulate is a 0.065% reduction in Automobile Manufacturing, based on 50% of 0.0013, the proportion of automobile manufacturing in the Detroit MSA as a proportion of total U.S. gross output (see the last column of Table 22.1).

2 Auto manufacturing production is conducted in a stable manner throughout the year (i.e., there are no seasonal or weekly production cycles).
3 Given that our analysis focuses on a short disruption period, firms have limited flexibility to adjust factor inputs (e.g., substituting labor for capital or vice versa, or substituting other inputs for cyber inputs). Hence, the elasticities of substitution of factor inputs for all sectors are set at a very small value (0.01).
4 Production technology and economic structure of the U.S. economy is analogous to the economic structure of the Detroit MSA. Hence, the results simulated through a national CGE model would reasonably accurately reveal the indirect economic impact of a cyber-attack on the Automobile Manufacturing sector in the Detroit Metro Area.

The CGE simulations were implemented in nine groups with a differentiation in direct impact drivers. Specifically, the comparison of the different simulation results helps us to understand the economic consequence results in both the base case scenario without resilience and the effects of each of the various types of resilience tactics alone and in combination. As illustrated in Table 22.3, the base case results (in the absence of resilience) indicates the economic consequence of the auto manufacturing system disruption due to a cyber-attack would be substantial if it involved all automobile manufacturers in Detroit MSA. Assuming the cyber-attack causes a 50% reduction of production capacity as a result of a disruption to Automobile Manufacturing, the shock translates into a 0.0663% adjustment of the productivity parameter for this sector (MODR). The result for the Detroit Metro Auto industry is likely to cause a direct $210.21 million GDP loss during a ten-day disruption period.

The impact estimates of various resilience tactics are summarized in Row 2–6. It is clear that the effects of individual resilience tactics in reducing GDP losses vary substantially. For instance, conservation and production isolation were found to have a relatively smaller effects on eliminating the GDP losses, whereas the effects of production recapture and inventory were found to be relatively stronger. The effect of input substitution was found to be the largest among all the resilience tactics. A lower-bound substitution, which reduces the level of disruption by 20% in the base case, is likely to reduce the GDP losses by $41.39 ($210.21–$168.82) million, whereas an upper-bound substitution, which reduces the base case disruption by 35%, can potentially reduce GDP losses by $72.65 ($210.21–$137.56) million.

The simultaneous effects case, which incorporates all resilience tactics into the base case scenario, indicates that the resilience tactics implemented after a cyber-attack on the Automobile Manufacturing sector are substantial. The lower-bound estimate of GDP loss in a ten-day disruption (which contains a lower-bound input substitution effect and other types of resilience at their normal levels) is $130.15 million, or a muting of GDP losses by 38%. On the other hand, the upper-bound estimate of GDP loss in a ten-day disruption (which contains an upper-bound input substitution effect and normal levels of other types of resilience) is $104.38 million, or a muting of losses of GDP by 50.34%.

A validation of the CGE modeling simulation focuses on the Base Case of the cyber-attacks. The total gross output (sales) value of Automobile Manufacturing in the Detroit MSA is around $37.5 billion. The gross output loss during a ten-day disruption is thus equivalent to $1,027 million ($37.5 billion/365×10×1,000). The direct GDP loss due to a complete ten-day disruption would be around $244 million, based on the fact that the GDP vs gross output ratio is only 0.2374 because so many intermediate goods are included in an automobile. A 50% reduction in

Table 22.3 CGE Simulation Results of a Cyber-Attack on Auto Manufacturing in the Detroit Metro Area

ID	*Scenario*	*Shock/Resilience*	*Shock (%)*	*Model Sector*	*Productivity Parameter Shock (Proportions)*	*GDP Losses (Millions of 2012 Dollars)*	
						One-year National Impact	*Ten-day Regional Impact*
BS	Base Case	50% reduction of disruption	0.5	MODR	–0.0663	–7,673	–210.21
CO	Conservation	2% improvement of the telecom productivity	0.02	COMC	0.0006	–7,669	–210.10
IS1	Input Substitution	20% reduction of the disruption in the base case	0.4	MODR	–0.0531	–6,162	–168.82
IS2	Input Substitution	35% reduction of the disruption in the base case	0.325	MODR	–0.0431	–5,021	–137.56
IV	Inventory	5% reduction of the disruption in the base case	0.475	MODR	–0.0630	–7,296	–199.89
PI	Production Isolation	5% improvement of the telecom productivity	0.05	COMC	0.0015	–7,663	–209.94
RE	Recapture	Adjusting Recapture Factors to 49%	0.5	MODR	–0.0663	–6,318	–173.10
S1	Simultaneous 1	BS+CO+IS1+IV+PI+RE	0.375 0.07	MODR COMC	–0.0497 0.0020	–4,750	–130.15
S2	Simultaneous 2	BS+CO+IS2+IV+PI+RE	0.3 0.07	MODR COMC	–0.0398 0.0020	–3,810	–104.38

Source: Authors' calculation.

production capacity is thus likely to cause a $122 million GDP loss over ten days. Our general equilibrium analysis GDP impact results for the Base Case are $210 million, and thus the ratio of total to direct GDP losses is 1.72. This is a very reasonable "multiplier" for a region the size of the Detroit MSA, especially for a "short-run" analysis, where we have decreased various elasticities of substitution to very low levels.

Conclusions

This chapter develops a framework for analyzing consequences of and resilience to a cyber-attack. The framework adapts the state-of-the-art tool of economic consequence analysis – computable general equilibrium modeling – for this purpose. The chapter presents an analysis of resilience to cyber disruptions and incorporates six major resilience tactics into the CGE model. The model is then applied to a ten-day cyber-attack on the automobile industry in the Detroit Metropolitan Area.

It should be noted that although the economic consequences of a cyber-attack can be significant, various resilience tactics can reduce the potential losses by more than 50%. The results should be juxtaposed to the cost and benefits of mitigation to find a balanced combination of strategies. It is likely that resilience is currently under-utilized, because of lack of awareness of extensive resilience alternatives. Moreover, the resilience tactics analyzed are relatively inexpensive compared to mitigation. For example, conservation more than pays for itself, relocation to existing branch plants has minimal costs, and recapturing lost production simply requires the payment of overtime wages. Also, unlike mitigation, which involves costs before any disaster occurs, most resilience tactics need not be implemented, nor money expended, until after the cyber-attack starts.

Our study has several implications for risk management and decision-makings. First, economic modeling can provide both public and private sectors a better understanding of the economic impacts of cyber-attacks. Modeling can also be used to develop strategies for incorporating various resilience tactics into the existing cyber risk management system. Second, given that the effectiveness of various cyber resilience tactics may differ given the presence of a cyber-attack, risk management agencies need to educate the relevant stakeholders and communities to be prepared for cyber-attacks and prioritize and implement appropriate resilience tactics after the event.

We estimate that the economic consequences of a cyber-attack of a realistic ten-day disruption would be significant. We also estimate that the combination of six resilience tactics can reduce the potential losses by more than 50%. One should also note that our analysis is preliminary due to the data limitations. Nevertheless, future research could be extended in at least the following two directions. The first is to improve the accuracy of the estimates of resilience effectiveness for most of the tactics examined. This can be done by adapting data from historical experiences or developing better simulation techniques. The second would be to test the robustness of our analysis, which could be done by examining further refined cyber-attack scenarios.

Acknowledgments

This study was supported by a research grant from The Risk Institute of the Fisher College of Business, The Ohio State University, and the Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California. The authors wish to thank Oscar

Neyra for his research assistance, and Dan Wei and Oscar Neyra for compiling important data for this chapter.

Notes

1 The model was originally developed by Oladosu and Rose for environmental policy analysis (Rose and Oladosu, 2002) and for consequence analysis of natural disasters and terrorism events (Rose et al., 2009).
2 The estimates above are consistent with those of a recent study of cyber disruptions on the San Francisco Bay Area economy caused by a catastrophic earthquake (see Sue Wing et al., 2018).
3 Dynes et al. (2007) estimate a cyber-attack would reduce production by 20%, but their estimate applies to the broader Automobile and Parts sector, which is less dependent on automobile manufacturing itself, and also includes some elements of resilience.

References

Barker, K., & Santos, J. R. (2010). Measuring the efficacy of inventory with a dynamic input–output model. *International Journal of Production Economics*, *126*(1), 130–143.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., & Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, *19*(4), 733–752.

Carlton, Rick (n.d.). "Car manufacturing process." itstillruns.com. Retrieved from: https://itstillruns.com/math-help-build-car-4965668.html

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

Chen, Z., & Rose, A. (2018). Economic resilience to transportation failure: A computable general equilibrium analysis. *Transportation*, *45*(4), 1009–1027.

Chen, Z., Rose, A., Prager, F., & Chatterjee, S. (2017). Economic consequences of aviation system disruptions: A reduced-form computable general equilibrium analysis. *Transportation Research Part A: Policy and Practice*, *95*, 207–226.

Cutter, S. L. (2016). The landscape of disaster resilience indicators in the USA. *Natural Hazards*, *80*(2), 741–758.

Dixon, P. B., Giesecke, J. A., Rimmer, M. T., & Rose, A. (2011). The economic costs to the US of closing its borders: A computable general equilibrium analysis. *Defence and Peace Economics*, *22*(1), 85–97.

Dixon, P., & Rimmer, M. T. (2002). *Dynamic General and Equilibrium Modelling for Forecasting and Policy: A Practical Guide and Documentation of MONASH* (Vol. 256). Elsevier.

Duchamp, H., Bayram, I., & Korhani, R. (2016). Cyber-security, a new challenge for the aviation and automotive industries. Seminar in information systems: Applied cybersecurity strategy for managers. Retrieved from: http://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf

Dynes, S., Johnson, M. E., Andrijcic, E., & Horowitz, B. (2007). Economic costs of firm-level information infrastructure failures: Estimates from field studies in manufacturing supply chains. *The International Journal of Logistics Management*, *18*(3), 420–442.

EDI Basics. (2017). EDI basics eBook. Retrieved from: https://www.edibasics.com/edi-by-industry/the-automotive-industry/

Federal Emergency Management Agency (FEMA). (1997). *Earthquake Loss Estimation Methodology* (*HAZUS*). Washington, DC: National Institute of Building Sciences.

AU: Please provide publisher location for this reference.

Genta, G., & Genta, G. (2014). *The Motor Car: Past, Present and Future*. Mechanical Engineering Series. Springer.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, *4*(1), 1–23.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, *22*(2), 175–186.

Jacobs, J. (2011). *The Nature of Economies.* Toronto: Random House.

Kajitani, Y., & Tatano, H. (2009). Estimation of lifeline resilience factors based on surveys of Japanese industries. *Earthquake Spectra*, *25*(4), 755–776.

Kennedy, C. (2011). *The Evolution of Great World Cities – Urban Wealth and Economic Growth*. Toronto: University of Toronto Press.

National Research Council (NRC). (2012). *National Earthquake Resilience: Research, Implementation and Outreach.* Washington, DC: National Academy Press.

National Research Council (2017). *Enhancing the Resilience of the Nation's Electricity System*, Washington, DC: National Academy Press.

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. *The Electricity Journal*, *27*(2), 52–60.

Orum, A. (2014). The metropolis, in Sasaki, M. Goldstone, J., Zimmermann, E. & Sanderson, S. (eds.), *Concise Encyclopedia of Comparative Sociology*. Leiden: Brill Publishing. Pp. 174–181.

Pimm, S. L. (1984). The complexity and stability of ecosystems. *Nature*, *307*(5949), 321–326.

Rose, A. (1995). Input-output economics and computable general equilibrium models. *Structural Change and Economic Dynamics*, *6*, 295–304.

Rose, A. (2004). Defining and measuring economic resilience to disasters. *Disaster Prevention and Management: An International Journal*, *13*(4), 307–314.

Rose, A. (2007). Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environmental Hazards*, 7(4), 383–95.

Rose, A. (2009). *Economic resilience to disasters*, Community and Regional Resilience Institute Report No. 8, Oak Ridge National Laboratory, Oak Ridge, TN, 2009. Retrieved from: http://www.resilientus.org/publications/research-reports/

Rose, A. (2015). Macroeconomic consequences of terrorist attacks: Estimation for the analysis of policies and rules, in C. Mansfield and V. K. Smith (eds.), *Benefit Transfer for the Analysis of DHS Policies and Rules*. Cheltenham: Edward Elgar. Pp. 172–201.

Rose, A. (2017). *Defining and Measuring Economic Resilience from a Societal, Environmental and Security Perspective.* Singapore: Springer.

Rose, A., & Liao, S. Y. (2005). Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science*, *45*(1), 75–112.

Rose, A. & Lim, D. (2002). Business interruption losses from natural hazards: Conceptual and methodology issues in the case of the Northridge earthquake. *Environmental Hazards: Human and Social Dimensions*, *4*, 1–14.

Rose, A., & Miller, N. (2017). Measurement of cyber resilience, *Center for Risk and Economic Analysis of Terrorism Events (CREATE).* Los Angeles, CA: University of Southern California.

Rose, A., & Oladosu, G. (2002). Greenhouse gas reduction policy in the United States: Identifying winners and losers in an expanded permit trading system. *The Energy Journal*, *23*(1), 1–18.

Rose, A. Z., Oladosu, G., Lee, B., & Asay, G. B. (2009). The economic impacts of the September 11 terrorist attacks: A computable general equilibrium analysis. *Peace Economics, Peace Science and Public Policy*, *15*(2), Article 6.

Rose, A., Prager, F., Chen, Z., & Chatterjee, S. (2017). *Economic Consequence Analysis*: *The E-CAT Software Tool.* Singapore: Springer.

Rose, A., & Wei, D. (2013). Estimating the economic consequences of a port shutdown: The special role of resilience. *Economic Systems Research*, *25*(2), 212–232.

Rubenstein, J. M. (2014). *A Profile of the Automobile and Motor Vehicle Industry: Innovation, Transformation, Globalization*. Digital Library.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. Boston: Boston Consulting Group, 9.

Short, J. (2012). *Globalization, Modernity and the City.* London: Routledge.

Sue Wing, I., Rose, A., & Wein, A. (2015). Economic consequence analysis of the ARkStorm scenario. *Natural Hazards Review*, *17*(4), A4015002.

AU: Please provide publisher location for this reference.

Sue Wing, I., Wei, D., Rose, A., & Wein, A. (2018). Economic impacts of the HayWired earthquake scenario, Scientific Information Report, US Geological Survey, Menlo Park, CA.

Sugrue, T. (2007). Motor city: The story of detroit. *History Now*, The Gilder Lehman Institute of American History.

Swaine, J. (2008). Georgia: Russia 'conducting cyber war'. *The Telegraph*, August 11. Retrieved from: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

Tierney, K. (1997). Impacts of recent disasters on businesses: The 1993 Midwest floods and the 1994 Northridge earthquake, in B. Jones (ed.), *Economic Consequences of Earthquakes: Preparing for the Unexpected*. Buffalo, NY: National Center for Earthquake Engineering Research. Pp. 189–222.

Tierney, K. (2007). Businesses and disasters: Vulnerability, impacts, and recovery, *Handbook of Disasters*. Heidelberg: Springer.

Xie, W., Rose, A., Li, S., He, J., Li, N., & Ali, T. (2018). Dynamic economic resilience and economic recovery from disasters: A quantitative assessment. *Risk Analysis*, *38*(6), 1306–18.