# Measurement of Cyber Resilience from an Economic Perspective

by

Adam Rose and Noah Miller

Center for Risk and Economic Analysis of Terrorism Events (CREATE)

University of Southern California

Forthcoming in

Samrat Chatterjee, Robert Brigantic, and Angela Waterworth, Editors

*Applied Risk Analysis for Guiding Homeland Security Policy and Decisions*

Springer Publishers

June 30, 2017

**Abstract**

Businesses are becoming more vulnerable to cyber threats and cyber-based disruptions. This paper provides a framework for analyzing the costs of cyber resilience and synthesizes the academic literature and industry-specific information to provide a comprehensive initial set of cost and effectiveness estimates for many cyber resilience tactics. The framework is based on economic production theory, which reflects the ways businesses use cyber and other inputs to produce goods and services. The tactics are grouped into general categories such as input substitution and conservation, use of excess capacity and inventories, and geographic or cyber relocation. Our analysis indicates that the set of cyber resilience tactics is extensive, diverse, potentially very effective and relatively low cost. Additionally, resilience is examined for two key sectors on which cyber activity depends – electricity and production of cyber equipment -- to provide further insights and context on this issue.

**Keywords:** Cyber Threats, Economic Resilience Tactics, Costs, Effectiveness

**Measurement of Cyber Resilience from an Economic Perspective**

by

Adam Rose and Noah Miller[1]

## I. Introduction

All segments of society are becoming increasingly vulnerable to cyber disruptions from malicious actors, natural disasters, and technological accidents. Although significant efforts are being made to protect cyber systems from threats, increasing cyber usage and increasing frequency and potential magnitude of threats appears to be more than offsetting these initiatives. There is a growing realization in the cyber area, as well as in other domains, that we cannot protect complex systems against all threats, so some attention has shifted to recovering as effectively and quickly as possible from them. We define *economic resilience* as building the capacity to rebound, and implementing it post-event, in juxtaposition to the more commonly analyzed strategy of (pre-event) mitigation. Although, resilience cannot wipe away any initial damage, it can reduce business interruption, i.e., reduce losses in sales revenue, income and employment. Moreover, the direct reduction of these losses also prevents their effects from rippling up and down the supply chain.[2]

This paper provides a framework for analyzing the costs of cyber resilience and synthesizes the academic literature and industry-specific information to provide a comprehensive initial set of cost and effectiveness estimates for many cyber resilience tactics. The framework is based on economic production theory, which reflects ways businesses use cyber and other inputs to produce goods and services (Rose and Liao, 2005; Rose, 2009). The tactics are grouped into general categories such as input substitution and conservation, use of excess capacity and inventories, and geographic or cyber relocation. Our analysis indicates that the set of tactics is extensive, diverse, potentially very effective, and relatively low cost.

The following section defines economic resilience and operational metrics for evaluating its effectiveness. Section III summarizes our findings on the measurement of resilience in relation to cyber systems. Section IV summarizes unique aspects of resilience in relation to two major sectors with which cyber systems are interdependent – manufacturing of cyber equipment and electricity service systems.

---

[1] The authors are Research Professor, Price School of Public Policy, University of Southern California and Faculty Affiliate, Center for Risk and Economic Analysis of Terrorism Events (CREATE), USC, and Research Associate, Price School and CREATE, USC. They wish to thank Anne Wein for sharing interview data and references and for helpful comments on a previous draft, Jonathan Eyer, Satish Chikkagoudar and Thomas Carroll for their helpful comments on the latest draft, and Joshua Banks for his help in examining the relevant literature on resilience tactics.

[2] The Webster Dictionary definition of Cyber is: "relating to, or involving computers or computer networks (such as the Internet)." Some other definitions include information technology.

## II. Economic Resilience

### A. Basic Concepts of Cyber Resilience

The complex-systems literature offers three "resilience" or "security" related concepts (Rey 2015): robustness, resiliency, and dependability. A system exhibits *robustness* if it is able to continue delivering its service within acceptable levels despite an adverse event. A system is *resilient if* it is able to recover/resume operations after an adverse event of such magnitude that its service is affected. A system is *dependable* if it provides an acceptable level of service overall. Current definitions of cyber resilience typically do not distinguish these concepts and, in general, subsume all three. According to Bjorck (2015), "Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events," where the intended outcome is ensuring business delivery for most, if not all, enterprises and organizations. An *adverse cyber event* affects the *confidentiality*, *integrity* and/or *availability* of cyber systems, information, services, and/or processes. Therefore, as a consequence, cyber resilience encompasses aspects of information security, cyber security, business continuity and resilience, mission assurance, and organizational and operational resilience. MITRE's cyber resilience engineering framework describes four high-level engineering goals: anticipate, withstand, recover, and evolve. These goals cover situations before, during and after adverse cyber events. Systems are considered "safe to fail" if they recover and adapt to the cyber adverse conditions.

### B. Basic Concepts of Economic Resilience

In addition to the above definition of resilience within the cyber domain, there are many other definitions of resilience, but Rose (2009) and others have found more commonalities than differences between them. We offer the following general definitions of resilience, which capture the essence of the concept in general, and then follow them up with definitions that capture the essence of economic considerations. Following Rose (2004, 2009), and paralleling two seminal approaches to resilience in the literature on ecology, we distinguish two major categories of resilience:

In general, Static Resilience refers to the ability of a 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 timing and use of resources 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), and macroeconomic (operation of the economy, e.g., supply-chain adjustments, importation of critical inputs, fiscal and monetary policy). In this paper we focus on microeconomic resilience, but, in the spirit of economics, do so in terms of both supply and demand, i.e., from the perspective of both the supplier and customer.

Another important delineation in economic resilience, and resilience in general, is the distinction between inherent and adaptive resilience (see also 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 type in an electricity generating unit or the use of pre-established data back-up systems. Adaptive resilience is exemplified by undertaking efficiencies that were not previously thought possible or improvising technology.

**C. Economic Resilience Metrics**

Following Rose (2004, 2009), we provide an admittedly crude but operational metric of resilience. *Direct Static Economic Resilience* (*DSER*) refers to the level of the individual firm or industry (micro- and meso-levels) and corresponds to what economists refer to as "partial equilibrium" analysis, or the operation of a business or household entity itself. *Total Static Economic Resilience* (*TSER*) refers to the economy as a whole (macro-level) and would ideally incorporate what is referred to as "general equilibrium" effects, which include all of the price and quantity interactions in the economy, macro-aggregate considerations, and the ramifications of fiscal, monetary and security policy.

An operational measure of *DSER* is the extent to which the estimated direct output reduction deviates from the likely maximum potential reduction given an external shock, such as the curtailment of some or all of a critical input. In essence, *DSER* is the percentage avoidance of the maximum economic disruption that a particular shock could bring about.

A major measurement issue is what should be used as the maximum potential disruption. For ordinary disasters, a good starting point is a linear, or proportional, relationship, as for example, between an input supply shortage and the direct disruption to the firm or industry. Note that while a linear reference point may appear to be arbitrary or a default choice, it does have an underlying rationale. A linear relationship connotes rigidity, the opposite of the "flexibility" connotation of static resilience defined in this paper. Analogously, the measure of *TSER* is the difference between a linear set of indirect effects, which implicitly omits resilience, and a non-linear outcome, which incorporates the possibility of resilience.

We illustrate the application of our resilience metric with the following case study by Rose et al. (2009), who estimated the national and regional economic impacts of the September 11, 2001, terrorist attack

on the World Trade Center. The researchers refined available data indicating that more than 95 percent of the businesses and government offices operating in the WTC area survived by relocating; the vast majority to Mid-town Manhattan or across the river in Northern New Jersey. Had all of these firms gone out of business, the potential direct economic loss in terms of GDP would have been $43 billion. However, relocation was not immediate, and, through its own survey, found it taking anywhere from a few days to as long as eight months for the vast majority of firms. Rose et al. (2009) calculated this loss in GDP at $11 billion. They were then able to apply the resilience definition provided above to estimate that the effectiveness of relocation as a resilience tactic in the aftermath of the 9/11 attacks was 72 percent ($43 minus $11, divided by $43). The study highlighted the importance of excess capacity as a resilience tactic.

The resilience metric has been used by other analysts to measure the effectiveness of resilience. For example, Kajitani and Tatano (2008) used it to measure the effectiveness of several resilience tactics in various sectors of the Japanese economy to a simulated earthquake. Similar studies of the effectiveness of individual or groups of resilience tactics have been undertaken by Barker and Santos (2009), Rose and Liao (2005), Rose et al. (2007), Rose and Wei (2013) and Rose et al. (2016). Rose and Krausmann (2013) have emphasized the importance of extending such analyses to measure the *cost*-effectiveness of various tactics and provided an overview of how the analyses could be used to compile an overall resilience index.

## III. Cyber System Resilience Tactics

To date, there is no comprehensive study of cyber resilience. There are several in-depth studies on protecting cyber systems from various types of attacks, including criminal, malicious, and terrorist threats. However, nearly all of these represent pre-event mitigation to reduce the chance of an attack or minimize the direct effect of an attack. Resilience, in our study, refers to actions taken in response to disruption from a disaster, i.e., post-disaster recovery (Rose, 2004; 2009). Of course, resilience is a process, and its capacity can be enhanced prior to disaster, but nearly all of these enhancements are not implemented until after the disaster strikes. Examples are the stockpiling of critical inputs, such as additional computers or computer and network hardware components, geographically distributing data- and computing-centers, or maintaining back-up generators (ideally in combination with uninterruptible power supplies), even though they will not be utilized until a disaster strikes. We also note that resilience differs with respect to suppliers of cyber equipment/services and their customers. In general, resilience on the supplier-side often involves expensive redundancies of equipment and systems, while

many of the resilience options on the customer-side are relatively inexpensive, and in fact can pay for themselves (prioritization of access to limited bandwidth, substitution of satellite-based phones, etc.). [3]

Table 1 is based on studies on microeconomic resilience options, or tactics, for businesses on the supplier and customer-sides. The general categories of resilience emanate from economic production theory, which is the conceptual basis for analyzing how a business transforms various inputs into the goods or services it produces (Rose and Liao, 2005; Rose, 2015; Dormady et al., 2017). Furthermore, the options can either be implemented beforehand, only to take effect when needed, e.g., ensuring flexibility in supply procurement, or be implemented after the fact, e.g., temporarily switching to satellite telephones in the case of lost cell- and hardline connections. The column headed "Possible Action" refers to specific resilience tactics that represent the build-up of resilience capacity prior to disaster or the response after the disaster strikes. The column "Cost of Resilience" provides a rough approximation of the cost of actually implementing resilience. The "Effect of Resilience" provides a general indication of the extent to which it can reduce business interruption losses. The cost and benefits of resilience tactics could only be quantified where some evidence could be found. The table attempts to be comprehensive in its coverage, but not all options will necessarily apply to all businesses; service-oriented businesses are unlikely to need stockpiles of production inputs, while manufacturing-oriented businesses are unlikely to need as much computing and telephone redundancy.[4]

We provide an example citation for the vast majority of resilience tactics. Citations are not included in cases where the tactic is non-technical and generally understood, such as minimizing non-essential uses, isolating cyber systems from other aspects of business operation to the extent possible, etc.

The first cyber resilience tactic presented in Table 1 is *Conservation*. Examples include reducing nonessential usage, restricting nonessential access, and recycling cyber equipment. For example, removing non-essential access increases the ability and speed of responding to a cyber breach or

[3] The focus of this paper is on restoring the availability of cyber resources, as opposed to restoring confidentiality and integrity of data, both of which are beyond the scope of this paper. The latter two objectives, however, are provided inherently by some of the resilience tactics listed in table 1. However, we do not distinguish these objectives or otherwise address them. Also, we acknowledge that some adverse cyber events relating to confidentiality and integrity may take a long period of time to detect, but that the loss of function (lack of availability) is more readily detectable. Also, we focus on cyber availability as separate from the issue of data restoration, which we do not address explicitly; because of the existence of so many types of data back-up systems this is becoming increasingly less of an issue.

[4] Some options, such as firewalls and increased monitoring, are listed to prevent any damage after the initial disruption. They could legitimately be referred to as "mitigation" measures, but fall into a gray area between mitigation and resilience as defined here, and are thus included.

general disruption by reducing the number of access points (CyberSheath, 2014). Note that Conservation is an especially attractive resilience tactic, since it often pays for, or even more than pays for, itself. However, it is limited in scope in terms of being able to reduce business interruption from disasters in other or related contexts (see, e.g., Rose and Lim, 2002; Rose et al., 2007), and there is every indication that this applies to the cyber realm as well.

*Input Substitution* has extensive possibilities in the case of cyber. It ranges from increased flexibility of systems to various substitutes and back-up capabilities (see, e.g., Chongvilaivan, 2012; Sheffi, 2005). Flexibility refers to both supply procurement and to the conversion of inputs into final goods and services. The former entails investment into business-relationships between corporate management and suppliers, which leads to combined efforts towards quickly overcoming supply-chain disruptions.[5] "Multi-sourcing" is a classic example. Conversion flexibility relates to machinery and processes, which

facilitates adjustment in resources and employees as necessary (Zolli and Healy, 2012). There are many examples of back-ups, including portable electricity generators. More dramatic examples include the use of "Cells on Wheels" following Hurricane Sandy, in which Verizon deployed several mobile cell-towers throughout New York City in response to a number of conventional cell towers going down (Richtel, 2009). A major source of customer-side cyber resilience is the existence of multiple communications systems that support input substitution. Fiber-optic, or hard-wired, systems are the most vulnerable to physical disasters in terms of damage and repair, followed by cellular data systems dependent on cell towers. Satellite providers are the most reliable in the face of any physical destruction, but are not as widely used and have vulnerabilities of their own with respect to technological accidents and solar weather. Of course, substitution potential must be tempered by possible delays in establishing alternative routes and limits to system capacity, which have frequently caused systems to crash in the aftermath of disasters (cf., Altman 2012; Vantage Point, 2013).

*Import Substitution* refers to bringing in goods and services in short supply from outside the region. It pertains primarily to the manufacturing of cyber equipment and various supply-chain effects.Setting up alternatives in advance, or at the minimum, researching options, can ensure smoother substitution of inputs following a disaster. Of course, it can be constrained by damage to transportation infrastructure, as often results from a natural disaster.

*Inventories* refer to stockpiling critical inputs for the production of cyber equipment, other supply-chain inputs, and cyber systems. Sheffi (2005) notes the classic example of Nokia being much better prepared for a disruption of semi-conductor supply inputs than its major competitor, Ericsson, and thus was able to significantly increase its market share in the aftermath of the disruption. Note that the cost of

[5]Supply-chain modification is also an example of a meso-level resilience tactic, as is the tactic of market-oriented non-interruptible service contracts to be discussed below.

inventories is not the actual value of the goods themselves, but simply the carrying costs. The goods themselves are simply replacement for the cost that would have been incurred had the ordinary supplies been forthcoming. That said, it should be further noted that carrying costs of electronic goods are typically much higher than other goods, as they depreciate quite quickly (and carrying cost is more than interest and storage costs, but also the cost of the obsolete inventory itself). Some companies, such as Dell, circumvent these carrying costs with a "Made-to-Order" business model, in which they typically hold only four days' worth of inventory, producing more as they receive orders.[6] At first glance this would seem a less-resilient business model, more prone to supply-chain disruption, but during the semi-conductor shortage in 1999 their "Made-to-Order" direct consumer marketing model allowed Dell to steer its customers towards products that it had on hand and products that were less affected by the shortage.

*Excess Capacity* overlaps to a great extent with system redundancy, which is primarily a supply-side resilience tactic. Typically, it is viewed as a rather expensive option, as, for example, in the case of back-up transformers for electric power systems. However, in-house data storage can provide easy, scalable data redundancy (Khasymski, 2015; Newegg, 2017), and cloud-based data backups provide an alternative and relatively inexpensive option (Amazon S3, 2017). Another possibility related to this resilience tactic is the development of uninterruptible internet service contracts, which could give firms the option to pay a small fee for being priority customers in the event of shortages in internet access.[7] Furthermore, including multiple redundant physical connection pathways in internet service provider (ISP) contracts, or overlapping contracts with different ISPs, could provide higher day-to-day speeds and larger bandwidth, in the case of overlapping contracts, while providing redundancy towards maintaining service should one or more ISPs or connection pathways experience service loss following a disaster (Peplink, 2017; Spiceworks, 2017). Finally, we recognize the inherent redundancy in the internet – data network system here (e.g., data centers can failover, data can be rerouted).

*Input Isolation* is referred to in the technical disaster literature by its complement -- "Importance" (see ATC, 1991). It pertains to the ability to separate aspects of the production process from dependence on lifeline utilities, including cyber systems. The Cybersecurity Framework, a federally developed set of guidelines for cyber standards and practices, provides resources to identify which aspects are essential and nonessential (NIST, 2014). Input Isolation obviously applies to many aspects of agriculture with respect to electricity and communications, but it is increasingly less of an option as an economy

[6]For some types of production and manufacturing this may also involve a cost due to lost economies of scale in production during normal times. This does not appear to be the case with Dell, for example, , and is likely due to the final-goods nature of their business. Because Dell's business model revolves around the individual assembly of specific sets of intermediate goods, sourced from suppliers, into a final good, there is more to gain from flexibility than from increased scale.

[7]This option was not previously allowed under net-neutrality laws. However, given the recent changes to those laws, and the success of these premiums in other domains, such as electricity service provision, it is worth considering.

## Table 1. Microeconomic Resilience Options for Businesses

| Category | Action/Investment | Cost of Resilience | Effect of Resilience | Source |
|---|---|---|---|---|
| *Conservation* | | | | |
| • reduce non-essential use | re-organization of data and optimized distribution[1] | roughly pays for itself | low to moderate | |
| • remove non-essential access | remove non-essential administrator access[3] | roughly pays for itself | low to moderate (increases ability and speed of responding to a breach by reducing access points) | |
| *Input Substitution* | | | | |
| • paper records, traditional couriers | re-contract[3] | low to moderate | low to moderate at small scale | |
| • enhance flexibility of input combinations | supply procurement flexibility[1] | low (investment in aligning corporate-supplier relationship) | low to moderate (quickly overcome disruptions through greater cooperation between businesses) | Chongvilaivan (2012) |
| | process conversion flexibility[1] | low (investment in standardized processes, identical machinery) | low to moderate (ease of relocation) | Chongvilaivan (2012) |
| • wireless-to-wired, and wired-to wireless internet and phone access | use text messaging or social media[2] | low to moderate | low to moderate | |
| | Cells on Wheels (COWs)[2] | moderate (rental contract; or, price of device + long term storage and transportation) | moderate to high | Richtel (2009) |
| | satellite phones[2] | low to moderate ($189 - $300 monthly rental charges; $6 - $9 per minute) | moderate to high (most reliable method of communication) | Verizon (2015) |
| | femtocells (small mobile cellular base station)[3] | low (small scale: <$100) | moderate to high (restores cell coverage; improved battery life for devices) | Ricknas (2010) |
| | cellular signal boosters[3] | low (small scale: ~$850; large business: ~$3,500; industrial scale: ~$4,000) | moderate to high (restores cell coverage; improved battery life for devices) | SureCall (2015) |
| | voice over IP telephone lines[3] | low to moderate ($2,500 - $15,000 for initial installation + $40 - 65 per line/month) | moderate (requires an internet connection) | Chacos (2012) Kremlace (2012) |

| Category | Action/Investment | Cost of Resilience | Effect of Resilience | Source |
|---|---|---|---|---|
| *Import Substitution* | | | | |
| • mutual aid agreements | cooperative agreement[1] | low | low to moderate | |
| • re-routing of goods/services | data-center failover[1] | low<br>(slowdown in internet services) | moderate | |
| • supply-chain management | multi-sourcing strategy[1] | moderate<br>loss of quantity discount; higher admin costs; reduces strength of established partnerships; competition leads to lower costs | moderate | Linthorst (2006) |
| *Inventories (Stockpiles)* | | | | |
| • pool resources | cooperative agreements[1] | very low | low to moderate | |
| • stockpile products and other essentials | "safety" stock[1] | low to moderate<br>(carrying cost only; but higher than normal as cyber equipment depreciates quickly) | low to moderate<br>(safety net for disruption of supply; lower costs when purchased in bulk) | Sheffi (2005) |
| • stockpile product inputs | build-to-order (stockpile inputs & parts instead of finished products)[1] | low<br>(revise how business operates; some loss of economies of scale) | low to moderate<br>(allows business to more efficiently use stockpile to meet customer demand while input supply chains are reestablished) | Papadakis (2006)<br>Chongvilaivan (2012)<br>Sheffi (2005) |
| | direct consumer marketing (in conjunction with built-to-order model)[1] | low<br>(cost of training/updating marketers & customer service staff) | low to moderate<br>(allows promotion of products that were unaffected by supply chain disruption) | Sheffi (2005) |
| • batteries | install battery storage[1] | low<br>($250/kwh capacity; base 100kwh, expandable up to 10mwh) | moderate<br>(allows for 100kwh - 10mwh worth of electricity to be stored) | Kassner (2015) |
| *Excess Capacity* | | | | |
| • maintain in good order | maintain in good order[1] | low | low to moderate | |
| • system redundancy | Redundant Array of Independent Disks (RAID); on- or off-site[1] | low<br>($200 - $10,000+ for small/medium RAID setup; $25,000 - $100,000+ for enterprise level setup; for off-site add cost of storage and connection) | low to moderate | Khasymski (2015)<br>Newegg (2017) |
| | e-mail and work mirroring software; off-site[1] | low<br>($150 - $1,000 per server + $0.50 per user/month | moderate<br>(requires a working internet connection) | Gros (2003) |

| Category | Action/Investment | Cost of Resilience | Effect of Resilience | Source |
|---|---|---|---|---|
| | cloud-based backup servers; off-site[1] | low<br>(cloud server: $0.004 - $0.061 per GB/month & $0.0036 per 100,000 transactions) | moderate<br>(allows for easy connection to data if relocation is necessary) | Microsoft (2015)<br>Dell Servers (2015)<br>Amazon S3 (2017) |
| | tape backups; off-site[1] | low<br>($1,500 - $25,000 per month) | moderate<br>(much cheaper than RAID storage) | Gros (2003) |
| | distributed data centers with data center "failover" capabilities[1] | low to moderate<br>(included in cloud-based options, otherwise cost of additional facilities and RAID storage) | moderate | Wein (2015) |
| • maintain capacity | multiple internet service connection pathways or internet service provider (ISP) contracts[1] | low<br>(can be built into current ISP contracts for minimal cost, or cost of additional ISP contract, $1,000 - $15,000/month + $250 - $16,000 for routing equipment) | moderate<br>(maintains internet connections in the case of an ISP losing connectivity. Single provider mean-time to recovery ~4 hours, but can be up to a week) | Peplink (2017)<br>Spiceworks (2017) |
| • maintain service | uninterruptible internet service premiums[1] | low<br>(usually 5% or less) | low to moderate<br>(ISP will prioritize returning service to the business over other customers) | AT&T (2017)<br>Comcast (2017) |
| *Input Isolation* | | | | |
| • decrease dependence | permanent or temporary shift to non-cyber means[2] | low to high<br>(industry specific) | low to high<br>(industry specific) | |
| • segment production | identify less essential cyber needs[2] | | | |
| *Relocation* | | | | |
| • physical move | arrange for facilities in advance[1] | low to moderate | high | Rose et al. (2009) |
| • telecommuting | remote desktop / VPN connections[2] | worker productivity change / business cost dependent on sector<br>($100 - $15,000+ / year for 25 – 5,000+ concurrent users) | moderate<br>(allows work to continue off-site as long as server remains online) | Cisco Systems (2017) |
| *Production Recapture* | | | | |
| • overtime/extra shifts | extra work after system is restored[3] | low<br>(overtime pay) | high<br>(production and sales are not lost) | Park et al. (2011) |
| • restarting procedures | uninterruptible power supply (UPS) with generators[1] | low<br>($4,000 - $15,000; plus cost of fuel and generators for as long as power is down) | moderate | Datacenter UPS (2015)<br>Bruschi et. al. (2011)<br>Liebert Corporation (2004) |

| Category | Action/Investment | Cost of Resilience | Effect of Resilience | Source |
|---|---|---|---|---|
| *Technological Change* | | | | |
| • change processes | cloud computing[1] | low<br>(replace on-site computing power and applications with cloud-based services;<br>$0.006 - $14.00 / hour depending on specific needs; general purpose $0.53 / hour) | moderate to high<br>(re-establishing internet connection becomes all that is necessary to continue computer based work) | Amazon EC2 (2017) |
| • alter product characteristics | increase flexibility of production[1] | low to moderate | low to high | |
| *Management Effectiveness* | | | | |
| • succession/continuity | train; increase versatility[1] | low | low to moderate | |
| • increased awareness/information sharing | cybersecurity framework[1] | low<br>(<175 full time employee hours to implement, otherwise resources are free) | low to moderate | Casey et al. (2015)<br>NIST (2014) |
| | Homeland Security Information Network[1] | low<br>(average cost of $43.80 per month per user) | low<br>(provides a platform to share sensitive information, collaboration tools, virtual meeting space, documents & alerts) | IT Dashboard (2015)<br>DHS (2015) |
| • emergency procedures | ensure emergency lines of communication with local government[3] | low<br>(minimal training; lines of communication) | low<br>(provides little resilience in and of itself, but may help in identifying the issue and enacting the correct measures) | Samuelson (2013)<br>Chen (2013) |

[1] Requires pre-event action to build up resilience for post-event implementation.

[2] Does not necessarily require pre-event action, but rather is only instituted post-event.

[3] While not strictly requiring pre-event action, would likely be more effective if built up beforehand.

advances in terms of technological sophistication. While it is typically inherent in the system or production process, it can also be applied in the aftermath of the disaster through improvisation.

*Relocation* is a tactic that increases resilience by physically moving the business' operations to a location away from the affected area. This requires not only the arrangement for alternate facilities with sufficient capacity, but is also facilitated by the standardization of processes and operations to allow for movement. Relocation would also include tele-commuting if the nature of the business allows for it, with cloud-based computing and data storage further increasing the ease of implementing this option.

*Production Recapture* refers to the ability to make up lost production by working extra shifts or over time after communication services and other capabilities are restored. It might involve replacement of expensive equipment that has been damaged, but otherwise the cost is only that of overtime pay for workers (Park et al., 2010). It is further facilitated by hastening the restarting of services such as electricity and internet access. This in turn can be promoted by other resilience tactics, such as Uninterruptible Power Supplies (UPS), a form of input substitution, which provide an emergency power source until back-up generators can be started or central power service is restored.

*Technological change* is a tactic that can increase resilience capacity, especially if it imparts additional flexibility into production systems both before and after the disaster hits (Zoli, 2011). It can also refer to important improvisations in the way goods and services are produced in the aftermath of a disaster. One example would be switching from on-site servers and computing power to off-site, cloud-based, storage and applications. In this example, because everything is stored in the cloud, a local disruption of cyber infrastructure would only affect workers' ability to connect to the cloud. For instance, if a business lost power, employees could return home and still access their files and work via the cloud.

*Management-effectiveness* refers to any improvements in decision-making and expertise that improve functionality, primarily by using existing scarce resources more efficiently. Much of it refers to improvisation, but some relates to established emergency-management plans and information services. The Cybersecurity Framework is one such service that provides a platform for information to be shared between businesses on current threats and the tools available to counter and rebound from these threats. Typically, it is a relatively inexpensive option, with costs limited solely to the implementation of the Framework.

## IV. Resilience for Cyber-Related Sectors

There is an increasing awareness of interdependence among infrastructure types and interdependence across the economy as a whole. Specifically, efforts at resilience, as well as mitigation, will not succeed as planned if other aspects of business operations are not functioning or if critical inputs into cyber activities are disrupted. In this section we briefly summarize some aspects of resilience pertaining to two major sectors that directly support cyber activity: manufacture cyber equipment and electricity services.

**A. Resilience in the Manufacturing of Cyber Equipment**

The measurement of resilience in the manufacturing of cyber equipment is a straightforward application of the approach laid out in Rose (2009) and applied in several contexts (e.g., Wein and Rose, 2011; Rose et al., 2017). It involves the same general categories of resilience on the supplier-side and customer-side listed in Table 1, but of course most of the particular options differ. Resilience tactics are generally applicable whether the disruption in manufacturing is caused by property damage or lifeline outages, though the tactics can differ in terms of their relative effectiveness in these two contexts.

Prior studies have shown that Production Recapture and Relocation are the relatively strongest forms of resilience in this context. However, Production Recapture is highly dependent on the duration of the recovery. Customers are willing to wait a few weeks, or even months, for delivery of product inputs, but will look to other suppliers beyond that. Given the duration of recovery (more than one year for major disasters), recapture could be relatively small. Recapture factors in HAZUS (FEMA, 2013) range from 40 to 99 percent for the first 3 months, with the larger factors pertaining to manufacturing. Rose et al. (2011) assumed that recapture factors decline by 25 percentage points each quarter and hence drop to zero if a business has not recovered within a year (see also Park et al. 2011). Relocation on the other hand is much more likely to be prominent, but this is somewhat dependent on standardized processes, as well as the degree of excess capacity (both production line and office space) available at the time of the disaster, which in turn often depends on the health of the regional economy. Note that the analysis above also applies to further downstream customers of cyber services. This includes manufacturers, as well as other sectors down the supply chain that have critical inputs, other than cyber inputs, disrupted.

**B. Resilience in the Electricity Sector**

Electric power outages lasting more than an hour in various locales of the US are relatively frequent occurrences, mainly due to weather conditions. Major disasters can cause widespread outages of longer duration; for example, parts of the City of Los Angeles electricity system were down for as many as 36 hours following the Northridge earthquake in 1994. Even more serious have been technological accidents, the most dramatic of which was the Northeast Blackout of 2003, which affected more than 50 million people. The business interruption impacts have been estimated as running into the billions of dollars by several analysts (see, e.g., Zimmerman et al., 2005). The increased dependency of society on electricity suggests that, on the surface, losses would be even higher from similar events in the future. However, several studies have identified the strong potential of various resilience tactics to reduce these impacts (see, e.g., Rose et al., 2004; Rose et al., 2007; Kajitani and Tatano, 2008, Santos, 2009; Sanstad, 2015).

Several resilience tactics are available on the supplier side (see, e.g., Lave et al., 2005). These include relatively expensive options, such as spare transformers, as well as less expensive options, such as expediting service restoration (basically dynamic economic resilience in the form of recovering more quickly).

On the customer side, there are more wide-spread and less expensive options. The measurement of resilience in response to electricity outages is somewhat related to options discussed in Section III. Nearly all of the same general categories of resilience are applicable, and some of the specific tactics do not differ much. A few differences include the fact that electricity is difficult to store, excess capacity is not applicable, and technological change options are more limited. Recent advancements in battery technology could, however, make electricity storage a viable option in the near future, with products like the Tesla Powerpack currently in the enterprise consumer testing phase (Kassner, 2015). Thus again, on the customer side, there are more wide-spread and less expensive options.

Rose et al. (2007) identified major resilience tactics and measured their effectiveness directly and indirectly (through upstream and downstream supply-chain effects) for a simulated terrorist attack in Los Angeles that could cause a 2-week blackout. Unlike many natural disasters, which can cause widespread destruction, a terrorist attack on an electricity system enables us to evaluate it in isolation. Of course, some of the implications of resilience in this context would then have to be modified for the case of a natural disaster as discussed below. The basic findings by Rose et al. (2007) are presented in Table 2. They pertain to the partial equilibrium (PE), commonly referred to as direct, and general equilibrium (GE), commonly referred to as the combination of direct and indirect, effects of changes in resilience parameters discussed below.

Unlike other inputs, conservation of electricity is a very limited option. Rose et al. (2007) estimate it as 5 percent based on a refinement of survey data by Tierney (1997). Increased (adaptive) interfuel substitution[8] has the potential to increase the elasticity of substitution between electricity and various fuels by 10 percent.

Inventories (customer storage) have not been a major option in the case of electricity until recently. Electricity isolation differs by sector, ranging from levels of 70 percent in various transportation-related sectors to zero percent in various manufacturing sectors (ATC, 1991). On-site alternatives to centralized electricity delivery, or distributed generation, differ by location, but for the City of Los Angeles values ranged from 10 percent in most sectors to 50 percent in sectors with very large firms (e.g., Petroleum Refining), sensitive production processes (e.g., Semi-conductors), or where implementation is relatively easy (e.g., office buildings for most sectors).

Production rescheduling also differs by sector, with very high rates for those sectors whose deliveries are not sensitive to short outage durations (e.g., Durable Manufacturing) and low rates for those whose are (e.g., Hotels and Restaurants) (Rose and Lim, 2002; FEMA, 2015).

[8] The existing substitution possibilities represent “inherent” resilience, and the increased substitution possibilities (increased elasticity of substitution values) represent “adaptive” resilience.

## V. Conclusion

This paper presents a framework for analyzing and estimating various types of resilience related to the cyber and cyber-related sectors. We provided ranges of estimates of the cost and effectiveness of a broad set of resilience "tactics" through a synthesis of the academic literature, including some of the author's own research, and industry-specific information. Overall, our analysis indicates that the set of cyber resilience tactics is extensive, diverse, potentially very effective and relatively low cost.

Overall, however, there is sufficient information to draw some major conclusions. First, it would appear that various types of back-ups for equipment, power sources, data storage, and opportunities for working remotely are readily available, and at relatively low cost. Further, the broad range of research on resilience in manufacturing is directly applicable to that of cyber equipment, as is the literature on electricity outages in general. Much of the literature focuses on outages and shorter durations, so some adjustments need to be made for devastating events from which recovery could take a year or more.

**References**


Altman. L. 2012.
http://www.continuityinsights.com/articles/2012/03/satellite-communications-myths-costs-capabilities

Amazon Web Services. 2017. Amazon Simple Storage Services (S3) Pricing. Retrieved 03/28/2017,
https://aws.amazon.com/s3/

Amazon Web Services. 2017. Amazon Elastic Compute Cloud (EC2) Pricing. Retrieved 03/28/2017,
https://aws.amazon.com/ec2/

Applied Technology Council (ATC). 1991. *Seismic Vulnerability and Impacts of Disruption of Lifelines in the Coterminous United States*, report ATC-25. Redwood, CA: Applied Technology Council.

Barker, K., and Santos, J. (2009). "Measuring the Efficacy of Inventory with a Dynamic Input–Output Model," *International Journal of Production Economics* 126(1): 130–43.

AT&T. 2017. Enterprise Business Network Services. Retrieved 03/28/2017,
https://www.business.att.com/enterprise/Portfolio/network-services/

Björck, F., et al. 2015. "Cyber Resilience Fundamentals for a Definition," *New Contributions in Information Systems and Technologies*, Springer: 311-316.

Bruschi, J., P. Rumsey, R. Anliker, L. Chu, & S. Gregson. 2011. "Best Practice Guide for Energy-Efficient Data Center Design," Department of Energy, Washington DC.
http://energy.gov/sites/prod/files/2013/10/f3/eedatacenterbestpractices.pdf

Casey, T., Fiftal, K., Landfield, K., Miller, J., Morgan, D., and Willis, B. 2015. "The Cybersecurity Framework in Action: An Intel Use Case," Intel Corporation, Santa Clara, CA.
http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

Chacos, B. 2012. "VoIP buying guide for small business," *PC World Magazine*, April 14. Retrieved from:
http://www.pcworld.com/article/260859/voip_buying_guide_for_small_business.html?page=2

Chen, B. 2013. "F.C.C. Seeks Ways to Keep Phones Alive in a Storm," *New York Times*, February 5. Retrieved from:
http://bits.blogs.nytimes.com/2013/02/05/f-c-c-revisits-communications-failures-after-hurricane-sandy/

Chongvilaivan, A. 2012. "Thailand's 2011 flooding: Its impact on direct exports and global supply chains," *ARTNeT Working Paper Series*, No. 113. https://www.econstor.eu/dspace/bitstream/10419/64271/1/715937650.pdf

Cisco Systems. 2017. Cisco AnyConnect Secure Mobility Client: Much More Than a VPN. Retrieved 03/28/2017,
http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html

Comcast. 2017. Comcast Business Solutions. Retrieved 03/28/2017, https://business.comcast.com/enterprise

Comcast representative. 2012. "Reply to: Anyone using Comcast Ethernet Network Service for their WAN infrastructure?" Spiceworks community forum, retrieved 03/28/17,
https://community.spiceworks.com/topic/277954-anyone-using-comcast-ethernet-network-service-for-their-wan-infrastructure

CyberSheath Services International. 2014. "The Role of Privileged Accounts in High Profile Breaches," May.
http://lp.cyberark.com/rs/cyberarksoftware/images/wp-cybersheath-role-of-privileged-accounts-6-2-14-en.pdf

Dell. 2015. “Dell PowerEdge Servers,” http://www.dell.com/us/business/p/servers?~ck=bt

Dell. 2015. “Datacenter UPS,”
http://accessories.us.dell.com/sna/category.aspx?c=us&l=en&s=bsd&cs=04&category_id=7071

Department of Homeland Security (DHS). 2015. “Homeland Security Information Network - Critical Infrastructure,” May. https://www.dhs.gov/critical-infrastructure-0

Dormady, N., A. Roa-Henriquez, and A. Rose. 2017. “Static Economic Resilience Production Theory and Resilience Tactic Framework.”

FEMA. 2015.
http://m.fema.gov/get-tech-ready-additional-tips

Goldman, D. 2012.
http://money.cnn.com/2012/10/29/technology/mobile/cell-phone-sandy/

Green N., T. Bentley And D. Tappin 2014. A Multi-Level Analysis of Telework Adoption and Outcomes within Organisations Following a Natural Disaster. Ergonomics, Work & Health Ltd, New Zealand. Retrieved from:
http://www.ergonomics.org.nz/LinkClick.aspx?fileticket=S_FdRN6qWpc%3D&tabid=39

Gros, M. 2003. “Taking Care of Business – Small, midsize and large companies have different disaster-recovery needs and budgets. The CRN Test Center details a wide range of solutions to help your customers weather the storm,” *Computer Reseller News*. Retrieved from:
http://go.galegroup.com/ps/i.do?id=GALE%7CA108267908&v=2.1&u=usocal_main&it=r&p=AONE&sw=w&asid=e4066cd2123764c27c43f5afc6f2ba82

IT Dashboard. 2015. “DHS - Homeland Security Information Network (HSIN).”
https://itdashboard.gov/investment?buscid=134

Kajitani, Y., and H. Tatano. 2009. “Estimation of Lifeline Resilience Factors based on Empirical Surveys of Japanese Industries,” *Earthquake Spectra* 25(4): 755-76.

Kassner, M. P. 2015. “Tesla’s Powerpack proposes battery powered data centers.” Datacenter Dynamics, London. Retrieved from: http://www.datacenterdynamics.com/critical-environment/teslas-powerpack-proposes-battery-power-for-data-centers/93974.fullarticle

Khasymski, A., and M. Rafique. 2015. “Realizing Accelerated Cost-Effective Distributed RAID,” in A. Khasymski and M. Rafique (eds.), *Handbook on Data Centers*, New Paltz, NY: Springer, pp. 729 - 752.
http://link.springer.com/chapter/10.1007/978-1-4939-2092-1_25

Kremlacek, R. 2012. “How Much Does a Business VoIP Installation Actually Cost?” *TeleDynamic*, May 22. Retrieved from: http://www.teledynamic.com/blog/bid/139621/How-Much-Does-a-Business-VOIP-Installation-Actually-Cost

Liebert Corporation. 2004. “Choosing the Right UPS for Small and Midsize Data Centers: A Cost and Reliability Comparison,” Liebert Corporation, Columbus, OH. http://www.upsystems-inc.com/sites/default/files/resources/cost-and-reliability.pdf

Linthorst, M., and J. Telgen. 2006. "Public Purchasing Future: Buying from Multiple Suppliers," in K. Thai and G. Piga (eds.), *Advancing Public Procurement: Practices, Innovation and Knowledge-Sharing*, Boca Raton: PrAcademics Press, pp. 471-482. http://www.utwente.nl/bms/iebis/staff/linthorst/67_linthorst_telgen_edited_acc.pdf

Microsoft. 2015. “Backup Pricing.” http://azure.microsoft.com/en-us/pricing/details/backup/

National Institute of Standards and Technology (NIST). 2014. “Framework for Improving Critical Infrastructure Cybersecurity.” http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Newegg. 2017. Network Attached Storage (NAS) Products. Retrieved 03/28/2017, https://www.newegg.com/Network-Attached-Storage-NAS/Category/ID-241

Papadakis, I. 2006. “Financial Performance of Supply Chains after Disruptions: An Event Study,” *Suuply Chain Management*, 11(1): pp. 25-33. http://libproxy.usc.edu/login?url=http://search.proquest.com.libproxy1.usc.edu/docview/216866096?accountid=14749

Park, J., J. Cho, and A. Rose. 2011. "Modeling a Major Source of Economic Resilience to Disasters: Recapturing Lost Production," *Natural Hazards* 58(2): 163-82

Peplink. 2017. Peplink Router Products. Retrieved 03/28/2017, https://www.peplink.com/

Rey, G. Z., et al. 2013. “Cooperation models between humans and artificial self-organizing systems: Motivations, issues and perspectives,” Resilient Control Systems (ISRCS), 2013 6th International Symposium on, IEEE.

Richtel, M. 2009. “Inauguration Crowd Will Test Cellphone Networks,” *New York Times*, January 18. Retrieved from: http://www.nytimes.com/2009/01/19/technology/19cell.html

Ricknas, M. 2010. “Femtocell Prices Have Dropped Below $100, Says Vendor,” *PCWorld*, March 30. Retrieved from: http://www.pcworld.com/article/192855/article.html

Rose, A. 2004. “Defining and Measuring Economic Resilience to Disasters,” *Disaster Prevention and Management*, 13(4): 307-14.

Rose, A. 2009. *Economic Resilience to Disasters*, Community and Regional Resilience Institute Report No. 8, Oak Ridge National Laboratory, Oak Ridge, TN.

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, UK: Edward Elgar.

Rose, A. 2017. “Benefit-Cost Analysis of Economic Resilient Actions,” in S. Cutter (ed.) *Oxford Research Encyclopedia of Natural Hazard Science,* New York: Oxford.

Rose, A. and E. Krausmann. 2013. “An Economic Framework for the Development of a Resilience Index for Business Recovery,” *International Journal of Disaster Risk Reduction* 5(October): 73-83.

Rose, A. and D. Lim. 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. and D. Wei. 2013. “Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience,” *Economic Systems Research* 25(2): 212-32.

Rose, A., G. Oladosu, and S. Liao. 2007. “Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout,” *Risk Analysis* 27:13-31.

Rose, A., G. Oladosu, and D. Salvino. 2004. "Regional economic impacts of electricity outages in Los Angeles: A computable general equilibrium analysis," in M. Crew and M. Spiegel (eds.), *Obtaining the Best from Regulation and Competition.* Dordrecht: Kluwer.

Rose, A., S. Liao and A. Bonneau. 2011a. "Regional Economic Impacts of a Verdugo Earthquake Disruption of Los Angeles Water Supplies: A Computable General Equilibrium Analysis," *Earthquake Spectra* 27(3): 881-906.

Rose, A., D. Wei and A. Wein. 2011b."Economic Impacts of the ShakeOut Scenario," *Earthquake Spectra: Special Issue on the ShakeOut Earthquake Scenario* 27(2): 539-57.

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

Rose, A., G. Oladosu, B. Lee and G. Beeler Asay. 2009. "The Economic Impacts of the 2001 Terrorist Attacks on the World Trade Center: A Computable General Equilibrium Analysis," *Peace Economics, Peace Science, and Public Policy* 15: Article 6.

Samuelson, T. 2013. "After Sandy, Questions Linger Over Cellphone Reliability," *NPR*, April 29. Retrieved from: http://www.npr.org/sections/alltechconsidered/2013/04/29/179243218/after-sandy-questions-linger-over-cellphone-reliability

Sheffi, Y. 2005. *The Resilient Enterprise*. Cambridge, MA: MIT Press.

SureCall. 2015. "Cellular Signal Boosters for Commercial." Retrieved from: http://www.surecall.com/product/cellphonebooster/15/0/0/CommercialBoosters

Vantage Point 2013.
http://apps.fcc.gov/ecfs/document/view?id=7520956711

Verizon. 2015. "Satellite Phone FAQs." http://www.vzwsatellite.com/faqs

Webb, G., Tierney, K., and Dahlhamer, J. 2000. "Businesses and Disasters: Empirical Patterns and Unanswered Questions," May 1. *Natural Hazards Review*, 1(2): pp. 83–90. http://ascelibrary.org/doi/abs/10.1061/(ASCE)1527-6988(2000)1:2(83)

Wein, A. 2015. Personal communication.

Wein, A., and A. Rose. 2011. "Economic Resilience," *Earthquake Spectra: Special Issue on the ShakeOut Earthquake Scenario*, 27(2): 559-73.

Zimmerman, R., Lave, L., Restrepo, C., Dooskin, N., Hartwell, R.,Miller, J., Remington, W., Simonoff, J., & Schuler, R. (2005). *Electricity Case: Economic Cost Estimation Factors for Economic Assessment of Terrorist Attacks*. New York University, Wagner Graduate School, Institute for Civil Infrastructure Systems, New York, NY.

Zolli, A. and A. M. Healy. 2012. *Resilience: Why Things Bounce Back*. New York: Free Press.