Are We Prepared for the Economic Risk Resulting from Telecom Hotel Disruptions?

Authors:

Ginger Armbruster[a], Barbara Endicott-Popovsky[b], Jan Whittington[a,*]

[a]Department of Urban Design and Planning, University of Washington, 3949 15th Avenue NE, Seattle, Washington 98195, USA

[b]The Information School, University of Washington, 4311 11th Avenue NE, Seattle, Washington 98105, USA

**Corresponding author.* E-mail address: janwhit@uw.edu.

Submitted: January 14, 2012

Accepted: May 18, 2012

Abstract:

Large and small businesses in Seattle, Washington, as in most urban centers across the United States, increasingly rely on telecom hotels and related telecommunications centers to conduct business operations. What would be the economic impact to these businesses if a natural or man-made disaster were to make this infrastructure unavailable for a significant period of time? How long would it take for the owners of small businesses, which provide the foundation for economic recovery, to give up and move away? Are metropolitan regions prepared for this risk?

This paper draws on publicly available reports of telecom hotel investments to examine the economic risks that such telecommunications hubs pose at the regional scale. New York City and Seattle are two urban areas that depend on key investments in telecom hotels. In the Pacific Northwest, these assets are located downtown, primarily in the center of the urban real estate market of Seattle. Although the terrorist attacks of September 11, 2001 were directed at the World Trade Center in Lowe Manhattan, collateral damage to a major telecommunications hub brought outages during and after the attacks that highlighted the serious risk posed to small- and mid-sized businesses from disruptions in telecommunications service. The Seattle case study illustrates the potential to learn from the experience in Lower Manhattan and apply this knowledge across the United States. Regional economic analysis of the benefits of and the means to protect small- and mid-sized businesses can provide the basis for strategic investments that minimize economic loss and reduce recovery time.

Keywords:

Telecommunications hubs, telecom hotels, business continuity, risk

1. Introduction

The destruction of the World Trade Center complex in New York City on September 11, 2001 was an unprecedented disaster at many levels. The impacts included the tragic loss of life, the destruction of a national icon, as well as immediate and long-term negative impacts on the economy. Although the target of the terrorist attacks was the Twin Towers, collateral damage to a power substation in the World Trade Center Tower 7 (WTC 7) and a key telecommunications hub in the Verizon Building near WTC 7 resulted in the loss of communications services for a large part of Lower Manhattan during and after the attacks, which exacerbated the economic impact. The outage immediately increased the difficulty of coordinating the response to the disaster—more than 300 firefighters died after their communications systems were rendered non-operational [1]. According to a Department of Homeland Security report [2], the immediate impact of 9/11 nationally was a 0.5% drop in real GDP growth and a reduction of 598,000 jobs. Thompson [3] has projected these economic losses through 2004.

After 9/11, emergency management professionals asked whether the potential existed for similar telecommunications infrastructure disasters to cause significant economic disruptions to their local economies [4]. Accordingly, we identified a telecommunications hub in Seattle, Washington, similar to the one in Lower Manhattan, where a disruption could have serious economic effects on Greater Seattle, perhaps even the Puget Sound Region. Located in downtown Seattle, this Internet hub has evolved from its beginnings as a telephony hub to become a major component of the telecommunications backbone in the Pacific Northwest. Its presence raises the question: What would be the economic impact to Seattle's businesses if this hub were to be damaged or destroyed?

This paper applies findings from the telecommunications service disruptions in Lower Manhattan to the circumstances presented by the concentration of telecommunications assets in Seattle. The next section discusses the local and regional risks created when the physical infrastructures of telecommunications hubs are developed through private business logic and fortified through the national lens of risk management. This is followed by an examination of a large telecommunications hub in Seattle. When compared with the experience in Lower Manhattan, the Seattle case study presents a rationale for regional risk analysis, including a generalized model of public and economic risk that can be applied to regions across the United States. The paper concludes with policy recommendations and highlights steps that should be taken in the short term to address the risk.

2. Evolution of Telecom Hotels

Advances in telecommunications technologies have led to the rapid industrialization of the United States and have contributed to its unprecedented prosperity, beginning with the proliferation of telegraphy during the Civil War and exploding with the commercialization of the Internet in the 1990s [5]. As the U.S. telecommunications system emerged, laws and regulations were established to protect the public interest. However, at times, legislation and regulation have struggled to grasp the social, political and economic implications associated with new telecommunications technologies. The Telecommunications Act of 1996 is an example. It formally ushered in the deregulation of the telecommunications market, mandating that existing carriers make their assets, including networks, equipment and space, available to competitors [6]. The motivation for the mandate was economies of scale—at the time, it was not obvious that aggregation would potentially create single points of failure in telecommunications infrastructures.

As an example, the Pacific Northwest region, often considered to be the tenth largest economy in the world [7], is highly dependent on the telecommunications infrastructure that supports a vibrant high-tech sector, including major software, e-commerce and aerospace companies [8]. Currently, more than 1,000 carriers and Internet providers in Washington State support the technology sector [8]. These include local and national carriers, as well as commercial entities that own and operate the sub-oceanic cabling for international telecommunications.

As in many metropolitan areas across the United States, Internet connectivity for thousands of businesses in the Pacific Northwest takes place through Internet Connection Points—Network Access Points (NAPs), Internet Exchange Points (IXPs) or Metropolitan Area Exchanges (MAEs)—that provide access to the Internet backbone [9]. The first five NAPs in North America were established in the 1990s in Chicago, New Jersey, San Francisco, San Jose and Washington, DC [10]. IXPs evolved from and encompass the original NAPs. Over time, additional centers that market a range of co-located telecommunications and data storage services have proliferated across the United States (Table 1). It is not unusual for metropolitan areas to house ten or more such facilities, while also hosting a regional IXP.

<Put Table 1 Here>

The Internet was initially developed by U.S. government agencies with access afforded to universities and research centers. The privatization of Internet access and the transfer of its management began in the late 1980s and continued through the 1990s [12]. Access points were sold to private firms, mainly established telecommunications corporations. Economies of scale and market expansion motivated the 1996 Telecommunications Act requirement that telecommunications corporations share their assets with other firms. Without competition, economies of scale would result in the classic market inefficiencies associated with monopolies.

Competition brings the expectation of a virtuous economic cycle of falling prices, investment in technology and reduced barriers to entry for new competitors.

Access points, and the competitors and related firms they host, are commercial enterprises. Their owners and operators promote and market the facilities using the same approaches as in other lines of business. Currently, any person interested in learning more about such centers could, through an online search, find an interactive map of centers across the United States. The person could click on a button on the map indicating the number of communication hubs, such as "meet-me rooms," telecom hotels and other data centers, in any metropolitan region. The links lead to pages with the complete addresses of each facility and profiles of the available services [11]. Companies that operate access points publicize this information to attract business. In Seattle, businesses that are interested in connecting to the Internet backbone have several options, but most of the options have found their way downtown, to the Westin Hotel [13].

2.1 Telecom Hotels

Telecom or carrier hotels, such as the Seattle Westin, are shared data center facilities where data communications media converge and interconnect. These data center facilities go by many names, including telecom hotel, collocation point, carrier hotel, data center, commercial Internet exchange, cyber hotel and network exchange center [14, 15]. The Telecommunications Act of 1996 opened collocation points for telecommunications exchange; meet-me rooms are similar in that the facilities allow telecommunications exchange between firms and their networks. Telecom hotels have opened to offer more space for telecommunications exchange along with the services provided by data centers [16]. These facilities service the data and networks of hundreds of organizations, large and small. Tenants include local exchange carriers, Internet service providers (ISPs), web hosting businesses, competitive access providers and a variety of non-telecommunications companies that require the facilities and services provided by a telecom hotel.

Like many telecom hotels, the Seattle Westin was originally designed for regular office use and was run by a hotel management company. It was not designed to house what has essentially become a public utility. Subsequent retrofitting to meet air conditioning, dust control, fire suppression and power requirements, including removing a bank of elevators to allow for the installation of fiber optic cabling, was conducted to transform the facility into a data center. In addition to providing the physical infrastructure for telecommunications, the telecom hotel offers staffing for on-demand tenant access and security.

Telecom hotels have been the subject of security concerns and study for more than a decade [16]. These facilities implement many security features and their customers are urged to carry out best practices and incorporate the risk of telecom hotel failure in their business continuity plans. Industry observers, however, have raised questions about whether these

accommodations are sufficient and whether customers who use these hubs are aware of the risks of failure to their businesses [17].

2.2 Market Forces

The concentration of U.S. telecommunications infrastructures in central geographic locations has evolved over time due to "specific market forces that include resource location, agglomeration economies, scale economies, community preferences and capital efficiency" [18]. The cost savings of collocation come from shared space, equipment and ongoing operational costs, such as staffing, cooling, electricity, security and fire suppression. In addition, the diversity of network protocols increases the variety of services that can be offered without increasing operational costs [18]. In this rapidly growing sector, software services grow faster than physical systems. Network protocols available today include, for example, Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Network (SONET), Synchronous Digital Hierarchy (SDH), Ethernet, Wavelength-Division Multiplexing (WDM) and the many protocols and technologies necessary for telephony.

Companies that use these data centers eliminate the costs of building or retrofitting their own facilities to meet air conditioning, dust evacuation and other requirements for housing telecommunications equipment. Although Internet services are increasingly popular, not all the tenants are ISPs; individual customers with high transmission requirements reduce costs by locating their communications in a data center or meet-me room using cross-cabinet jumpers to connect with the networks of business partners [13]. These centers also increase overall system reliability by providing ISPs with the opportunity to exchange data. If the network of one provider is unavailable, re-routing quickly provides alternative routes for network traffic.

The rapid expansion of online enterprises, facilitated in part by the emergence of networking technologies and the market presence of cloud computing, promises to escalate the flow of information resources through telecom hotels. Graphical user interfaces for web development with the scalable metering systems, virtualization technologies and data centers of cloud services provide unprecedented opportunities for individuals with relatively little specialized knowledge to create and manage online commerce enterprises. E-mail was an entrée. With streaming media, social networking and application developers competing for attention on personal devices, the public not only enjoys the main course, but is increasingly able to participate in the creation of online products. People flock to online sites to buy as well as to sell, barter and trade; even small shops at local street corners have web sites. Practically all this traffic flows through telecom hotels. As traffic grows, so does the demand for space from carriers. As carriers expand to accommodate the demand, they may establish new points of access. They also aggregate economic activity into existing telecom hotels.

2.3 Collocation and Collateral Damage

While the economic benefits of collocation are clear, significant risks are introduced as a result of concentrating critical resources in a single physical location. In 2003, a report by the President's National Security Telecommunications Advisory Committee (NSTAC) entitled, *Vulnerabilities Task Force Report—Concentration of Assets: Telecom Hotels* [16], specifically analyzed the risks presented by telecom hotels as a single point of failure. In particular, the report pointed out that the risks can be assessed from three different perspectives:

- **Federal Government:** The primary concern is that a single point of failure could impact the overall national infrastructure.
- **Telecommunications Industry:** The primary concern, from a company-centric view, is the overall impact of a loss of any asset on its infrastructure and customer services.
- **Users:** The primary concern is the impact on mission-supporting services.

These perspectives may overlap, but each view embodies incentives for investment and operational decisions that differ from each another, sometimes aligned and sometimes in conflict.

While the national infrastructure may survive a disaster at a local telecom hotel, regional infrastructures may not, with cascading effects throughout the local and regional economies as was seen in New York after the 9/11 terrorist attacks. Furthermore, while large organizations, whether public or private, may have disaster recovery plans that include measures to assess business risk of a telecom hotel being destroyed or taken offline, small organizations may not have the wherewithal to assess and mitigate the risk, or perhaps even realize that the risk exists.

Small businesses are fundamental to local economic success—as the incubators of larger business organizations and the economic elements that comprise the ecology of firms in any successful agglomeration economy. The Bureau of Labor Statistics [19] confirms that more than half of all jobs in the United States are provided by businesses with fewer than five employees. In fact, the recent signs of economic recovery seen in the U.S. (fourth quarter of 2011) stem from efforts of mid-sized firms with fewer than 250 employees to hire more workers. Analysis provided in a retrospective CRS Report to Congress [20] found that the 9/11 attacks dislocated, disrupted or destroyed nearly 18,000 businesses in and around the World Trade Center. The vast majority of these were small businesses. While research has yet to focus on this issue, small businesses are the most vulnerable to service disruptions, if for no other reason than the fact that they tend to have lower cash reserves. It is also reasonable to assume that the longer the disruption, the greater the likelihood that a business will shut down permanently.

The NSTAC report [16] also emphasized the importance of best practices in business continuity planning to prevent the economic effects of telecom hotel failure. Townsend and Moss [21] note that while it is "incumbent on the individual carriers to consider back-up and alternative networking in the context of their business continuity plans," it is important that as a part of the business continuity planning process, any business that is dependent on Internet connectivity independently determine whether or not its carriers are in compliance with safety and security requirements. While large businesses may be able to accomplish this and most likely have incorporated the risk associated with loss of connectivity through telecom hotels into emergency planning processes, small businesses may not be in a position to do so.

Evaluating the consequences of a telecom hotel failure to a local and regional economy requires a focus on the impacts to small- to mid-sized businesses. These businesses increasingly rely on telecom hotels as gateways to the Internet and, as evidenced by the events after 9/11, the businesses may have difficulty surviving a catastrophic event. Yet, these businesses are needed to spur economic recovery in the wake of a disaster.

2.4 Analytic Approach

The following sections of this paper draw from several published reports to understand the risk of a telecom hotel failure, in general, and at the Seattle Westin, in particular. An in-depth risk identification and assessment approach is proposed. The approach may be applied to any economic region, although it is particularly relevant to the Pacific Northwest. The resulting analysis is then used to frame the problem and suggest potential solutions.

3. Risks Unique to Telecom Hotels

The following sections characterize the risks associated specifically with telecom hotels. These risks form the basis for further investigation.

3.1 Location

Telecom hotels are vulnerable to many different types of events—man-made and natural—that can lead to catastrophic widespread outages and the non-availability of services [16]. For a coastal city such as Seattle these include earthquakes, severe weather conditions, flooding, civil disorder, terrorist activities and intentional hardware or software damage inflicted by criminals and disgruntled employees [17]. In addition to accidental or intentional direct physical damage, a telecommunications failure may occur as collateral damage from another event—witness the non-availability of the Lower Manhattan telecommunications network after the 9/11 attacks. As the NSTAC states "like any other building, a telecom hotel can be threatened due to its location, by inherently dangerous activities of its neighbors, through the interruption of other underlying infrastructures, or because a neighboring facility might be a terrorist target" [16].

Threats to software, like threats to hardware, may arise from sources internal or external to telecom hotels [22]. If one of the most meaningful strategies for reducing the impact or probability of damage from attacks to cyber-physical systems is the ability to isolate infected segments from the rest of the network, then, perhaps, telecom hotels are not always best served by locations in downtown corridors and by marketing efforts that seek to maximize interconnections at a single site. Furthermore, the idea that disconnection from a network can preserve functionality suggests spatial planning, both inside and outside these buildings.

3.2 Business Model or Public Utility?

Certain vulnerabilities are introduced to a telecom hotel based on the business model used to run the hotel. The Internet backbone has become a public utility, i.e., a business that provides a public necessity. For about a century, this definition has covered entities such as water, electricity, natural gas and telephone service. With Internet penetration in the United States approaching 80% [23], the Internet now is arguably a business necessity. Numerous firms rely entirely on the Internet for their business models; individuals do their banking over the Internet, pay bills and shop online, and even consult online physicians. Meanwhile, the business models of online entertainment, through social networking services and gaming platforms, are integrating with banking functions by developing and promoting services through their own exclusive online currencies. Yet, telecom hotels are still operated in many ways like businesses, rather than public utilities, altbeit with increased security requirements. Some of the practices associated with running a telecom hotel like a business may place the Internet components they house at increased risk.

One problem is that most telecom hotels are "mixed-use" buildings—high-rises with other tenants who rent office space for non-data-center related activities [24]. Security requirements for these tenants and their attention to safety and compliance issues may not be as rigorous as those followed by data center tenants in the same building.

Another problem is that facilities such as the Seattle Westin actively market their data center services. This includes maintaining a company website that provides information about the physical location, facility descriptions, photographs and details about the services offered and security measures implemented [13, 25]. A current list of customers is also posted—they include well-known carriers such as AT&T, Seattle SIX, AT&T Canada, Centurylink, Verizon, Frontier Communications and more than 130 other large and small service providers, including Amazon and Microsoft [25]. Needless to say, this information could be very useful to any party who intends to do harm.

3.3 Interconnectedness of Infrastructures

Townsend and Moss [21] note that "cities rarely escape even highly localized disasters without at least some physical damage to the telephone network." Because of the interdependency

and collocation of infrastructures, damage incurred by a major telecommunications facility can spill over to induce catastrophic damage to other infrastructures like the electrical and transportation systems (or vice versa) with combinatorial local or regional economic impacts.

When assessing the potential impacts of a telecom hotel failure and the "tentacle" nature of the services they provide, the cascading effects on a region through other infrastructures must be considered. For instance, disruptions to the telecommunications system can spill over into the banking sector where customers may be unable to operate ATM machines.

Methods for modeling the effects of interdependencies between infrastructure networks, as well as between networks in their regional economies, build on and modify input-output analysis [26,27], adjusting for the actual engineered designs of systems when such data is available [28,29]. Recent efforts to discern the status of regional econometric analyses with input-output models, however, also caution researchers to seek out natural experiments, conduct supporting research for the conceptualization of the models used, and find a basis in theory for interpreting results [30-32].

3.4 Implications of Continuous Access

One of the features that the Seattle Westin advertises—continuous access and security of the building—is also a vulnerability. This purported security feature introduces a potential human failure point. Screening, training and auditing people who staff these buildings are required and, even when implemented, are not always successful in eliminating lax behavior or bad actors [17]. A control room at an electric utility is protected through multiple layers of physical security and is further protected through isolation of the facility itself. Vetting for access is rigorous. This is not necessarily the case for telecom hotels. As suggested in the NSTAC report [16], the most significant vulnerability to telecom hotels is from humans with access, as "it is important to recognize that any one individual with malicious intent accessing any critical telecommunications facility could represent a threat."

Similarly, the dependence of connection points and data centers on supporting systems within the building, such as heating, ventilation and air conditioning (HVAC) systems, as well as the power that supports them, offer several sources of vulnerability. Whether they are intentional or accidental, mechanical and electrical failures can threaten air conditioning, for instance, and these systems are coincidentally critical to telecommunications and data center functions.

The economic value of the data stored in and flowing through telecom hotels should also raise concerns. As the value of the data increases, so does the motivation for espionage, whether through external software attacks or internal compromises of software and hardware [22]. Unless barriers to access are also raised, the comparative value of attempts to gain access will increase. As the economic value of the data grows, so does the projected cost of disruption, outage and failure.

3.5 Emergency Situations

Despite rigorous planning, disasters put enormous strain on the entire telecommunications system. People attempting to reach family members, emergency responders and businesses can cause the system to fail due to congestion. Anticipating this system stress and planning for alternatives in case of the destruction of any one component are complex tasks. Any risk management plan for user organizations and for a regional carrier must take this into account. Loss of connectivity will result in business and economic losses, but these may be compounded by stresses on the system, depending, of course, on the disruptive event.

An additional observation regarding the aftermath of the 9/11 attacks is that, while telecommunications infrastructures do have inherent redundancies, the reality is that "because of the time and funding needed to repair or replace systems, service disruptions caused by physical destruction also tend to be more severe and last longer than those caused by disconnection or congestion" [21].

The long term implications and economic impacts of direct or indirect damage to Internet services must also be included in the assessment of system vulnerabilities. Townsend and Moss [21] describe a four-phase process of recovery from disasters that disrupt telecommunications services: (i) emergency response; (ii) repair and reestablishment of services; (iii) reconstruction; and (iv) redevelopment. As a rule of thumb, each successive phase is believed to take ten times longer than its predecessor, although other factors underlie this rubric. The restoration of power, for instance, is usually required before services can be reestablished. Many disasters only require emphasis on response and recovery. The mantra of response is fuel, security and access to the site by the carrier. In the case of the World Trade Center after 9/11, all that was gone and no carrier access was possible [33].

The ability of Seattle businesses to avoid the losses experienced by their counterparts in Lower Manhattan would depend, among other things, on the relative ability of telecommunications service providers and their hosted firms to re-route traffic and reinstate databases from backup systems, handle surges in capacity from increased calls and queries in the wake of a disaster, and reduce downtime. In general, more active response and recovery capabilities should allow any carrier and its customers to benefit from shorter downtime of the network. Shorter network downtime should lessen the "pain" for the business owners who are economically dependent.

Forecasts of these circumstances can benefit from records maintained by carriers and large ISPs about the configurations of their networks and routing systems, as well as their customer bases. The fact that Internet service is still often delivered to homes and small businesses via old coaxial cables reaffirms the economic principles associated with a natural monopoly—namely, that it is fundamentally uneconomical to invest in redundant infrastructure in the "last mile" to customers. As a result, outages of hubs in hub-and-spoke systems have the potential

to disrupt services for large numbers of businesses and households, depending on the configuration of the network. This is the main tension between the economics of redundancy and vulnerability. The Seattle Westin was recently joined by two other telecom hotels in the downtown area. As the landscape becomes increasingly populated with telecom hotels and related service centers, telecommunications and other service providers are expected to invest in redundancies.

On the other hand, the ability to forecast the economic impact of any particular disruption in telecommunications service also depends on data pertaining to the relative dependence of businesses on the services that are disrupted. This line of research is not as well specified, in part, because of the rapid changes in collocation, online business models and aggregation of businesses in facilities such as telecom hotels. There are many components to telecommunications systems and many businesses have their own private data centers. Thus, it is reasonable to ask, in the case of a telecom hotel outage or failure, what is at risk and what is disrupted? For example, small- and mid-sized businesses may be entirely dependent on the services of an ISP at a telecom hotel, partially dependent on bricks-and-mortar and online commerce with some redundancies, or practically independent, as in the case of shops that maintain a web presence for marketing purposes without e-commerce. And, as noted above, businesses can be expected to differ considerably in their capacity to build redundancies in their own system architectures and through the contracts that they maintain with online providers, as well as by incorporating other best practices in their business continuity planning.

Firms that can afford to plan for business continuity are reminded that redundancy, resilience and back-up capabilities for continuity of operations are critical to survival. This is the risk that a business assumes. However, many businesses run on a 3-4% margin and risk catastrophes without the benefit of a business continuity plan or investments in back-up systems. After the famous wind storm in King County, Washington in 2005, numerous businesses that had no service for as little as one week went under [33]. Given the low operating margins of small businesses, implementing the back-ups needed to survive the disaster were simply too expensive.

The tenants of telecom hotels have a wide range of capabilities and business models. Small ISPs may charge less for their services and thus are compelling choices for small- and mid-sized firms. Small ISPs are not likely to implement the level of disaster response provided by a large carrier such as AT&T or Verizon. A small ISP may be a tenant at a telecom hotel, for instance, but not have the resilience to recover from an event quickly (or ever). A large carrier may be a more expensive business solution, but when there is trouble with the service, downtime will also be expensive [33].

3.6 Who is in Charge?

The question of who is in charge is difficult to answer. The Internet emerged as a government investment in national defense. It offered a means of communication that was far more resilient than others that had been conceived. But once it started, privatization proceeded rapidly. Over time, various not-for-profit groups of industry representatives and volunteers have contributed to the governance of the Internet. For a collection of physical infrastructures that are quickly becoming fundamental to economy and society, organizations on the national stage may be aware that the time is ripe to reassess and affirm modern demands for business continuity, both in the public and private sectors. One analyst [34] notes:

"Many of the current regulatory approaches were drafted in an era before the introduction of high speed trading in the financial markets, before the "smart" grid, before the spread of wireless communications networks comprising billions of devices, and before terrorism became a daily feature of the headlines."

In the early years of development of the Internet, the focus was primarily on making the technology fast, functional and available, not safe and secure from outside threats. Since the Internet is becoming recognized as a public utility, the risks to those who rely on the Internet as if it were a utility are being borne by users—with or without their understanding of the risks that they are assuming.

In terms of the ownership of telecommunications infrastructures in telecom hotels, meet-me rooms and similar facilities, carriers are often in charge. One can reasonably assume that the decisions carriers make concerning business continuity planning and investment in resilient architectures and organizational capabilities are driven by their desire to maintain customer satisfaction, service level agreements and legal obligations.

That said, rubrics of recovery and the reality of 9/11 demonstrate why a disaster demands a balance between public and private roles and responsibilities. The national government can organize to provide fuel and safe access to facilities for large carriers in the wake of a disaster. But the disaster may also leave businesses without anything that resembles a facility to access. In the meantime, plans for regional and local resilience seem to beg more questions for the businesses that are too small to rise to the national stage.

4. Regional Risks and Remedies

The 2003 report by the NSTAC Vulnerabilities Task Force [16] identified the system risks of concentrating assets in telecom hotels, especially as they relate to government-run agencies that are reliant on public infrastructures. According to the report, "the telecommunications industry analysis has shown it is unlikely that the loss of assets in a telecom hotel would cause a nationwide disruption of the critical telecommunications infrastructure." From the perspective of the federal government, there are sufficient redundancies in the architecture of the national telecommunications system to sustain the loss of a telecom hotel without disrupting the entire

system. Most telecommunications carriers can use alternative network traffic routes and, in any event, the rest of the infrastructure would continue to be operational.

While the NSTAC assessment is that telecommunications infrastructures have enough inherent redundancy to sustain the loss of a major component such as the Seattle Westin, there are alternate viewpoints. One analyst [18] posits that "the private sector does not properly account for the full social costs of critical infrastructure failure or those individual companies (that) cannot independently and significantly influence geographic concentration in a critical sector."

Additionally, the private sector may not be able to assess the risks presented by the complexities of the telecommunications infrastructure [34]. Letting the private sector resolve the resilience question in a free-market manner may present a problem, because in fact "the government is uniquely positioned to facilitate the gathering and integration of information regarding the large-scale dynamics of complex systems and the threats they face, and to work with industry to identify solutions that increase reliability and security" [34].

There are limits to the ability of the government to collect and expose this level of corporate infrastructure mapping. The government is currently not in a position to collect, update and maintain such databases, nor is it in a position to make corporate investment decisions outside of its own spending and regulatory authority. Government is also limited by the reluctance of carriers and related firms, such as ISPs and cloud providers, to report data. This complicates the performance of detailed risk and infrastructure analyses. Absent concerted private support for government action, it is unlikely that the information that is necessary would be exposed to the public-facing community.

Private firms can and do react differently to the need to share information about resilience in general, and forecasts or plans for disaster recovery, in particular. Cloud providers such as Google, Microsoft and Amazon quietly invest in massive data centers along the Internet backbone in the Pacific Northwest, an area known for stable, public sources of hydroelectric power. In a recent *New York Times* article [35], an executive from Google acknowledged that "[c]ompanies are historically sensitive about where their operational infrastructure is." In the absence of shared data, only piecemeal accounting is possible.

Whether as a result of a business imperative or the legal requirement that telecommunications carriers house competition, the public disclosure of the locations of telecom hotels is a striking contrast with the secrecy with which cloud providers cloak their assets. Between the two approaches, the regional networked landscape appears divided.

4.1 Regional Economic Model

According to Villasenor [34], individual businesses are able to assess their own business continuity requirements, but are not able to determine the needs of an entire region. This is the

province of government. Whether one agrees with Villasenor's assignment of responsibility or not, a model is needed for a collaborative regional and user risk assessment that would capture the vulnerabilities and risks to a specific regional economy of loss or disruption of a telecom hotel. Such a model would: (i) incorporate the unique risks that are inherent in the reliance on the Internet connectivity that traverses a telecom hotel (some of the more obvious of which are described above); (ii) integrate lessons learned from prior telecommunications failures along with various studies that have addressed different aspects of the problem, primarily from the federal government perspective; and (iii) assess the economic consequences of these risks from two perspectives, that of the region impacted and that of the individual users within the region whose business models rely on a telecom hotel.

Government agencies and large firms have been aware of the risks posed by telecom hotels for more than a decade and have undoubtedly produced numerous models to forecast the impact from any disaster or disruption to the services they provide. The research agenda in this paper is one that benefits from prior modeling efforts, merges knowledge from the natural experiments afforded by historical accidents and disasters, and sharpens the focus on the impacts to and needs of small- and mid-sized businesses. For instance, modeling efforts should be accompanied by survey research in the region served by the telecommunications facility, in order to adequately characterize the dependencies between businesses in the local and regional economy and the services provided by the telecom hotel in question.

Publicly available data about the Seattle Westin affirms the need to forecast the impact of disruptions in telecom hotel services. The rapid growth of cloud computing and related services for online business models will magnify the demand for the same forecast, yet evidence of impacts to small- and mid-sized businesses in the aftermath of the 9/11 attacks suggests that the focus of attention should, perhaps, turn to the portions of the economy that are most vulnerable to these disruptions and most valuable in the final phase of recovery from a telecommunications disaster—redevelopment.

In Seattle, as well as in other regions, related avenues of research are emerging that could complement this effort. First, the telecommunications industry has grown; there are now several additional telecom hotel locations in Seattle and in areas south of the city. Mapping these facilities and their services, backup plans and customer lists would contribute to a better understanding of overall risk exposure and the alternatives to customers and operators of the Westin facility in case of emergency. Additionally, an investigation into the interconnectedness of NAPs would assist in determining the backup capabilities between regional and national networks. The 2011 earthquake-tsunami in Japan demonstrates that a cascade of negative events subsequent to a mega-disaster is difficult to anticipate. Nevertheless, a detailed examination of the response plans for such an event would be helpful in determining local, regional and national resilience to cascading failures in the Northwest triggered by a major Internet backbone failure.

We anticipate that research in keeping with this agenda will find that businesses and organizations whose Internet traffic converges at the Seattle Westin are divided in their understanding of the risks posed to the customers who use the facility. Most likely, large entities that traverse the Westin hub have robust business continuity and disaster preparedness plans that account for the risk of an aggregated facility, but the thousands of small businesses whose network traffic also flows through the Westin are likely unaware and unprepared for a disaster to the facility that could put them out of business. This impact to small businesses would have a measurable effect on the economy of the region.

The model could be validated in coordination with cyber security professionals, most likely from academia and research centers, whose collaborations straddle private businesses and government agencies. The model would then be applied to assess the vulnerabilities and risks associated with similar telecommunications hubs across the United States.

4.2 Benefits of Regional Risk Analysis

The model and its supporting research results would assist businesses in incorporating telecom hotel risks in their disaster recovery and business continuity planning activities. Also, they would enable telecom hotels to convey key concepts of risk to their clients, especially smaller businesses that may not fully understand the related vulnerabilities.

While some attention has been paid through the Department of Homeland Security to the development of regional plans that explore the risks associated with major man-made or natural disasters to the Pacific Northwest, the challenges involved in instituting strong public-private partnerships for risk exploration are well known, especially given the experiences with the various Information Sharing and Analysis Centers (ISACs). Instead, this paper describes the parameters necessary for developing a robust evaluation of the economic consequences of a telecom hotel failure that could be used to influence the development of effective policy for protecting the public interest in the Internet backbone through more resilient business practices and governmental guidance or support.

Finally, economic modeling of the impact of a telecom hotel failure on local and regional businesses would be useful in determining the true local and regional costs of centralizing resources. It would be especially helpful to study the impact of a long-term partial reduction in the availability of services, or slow down, a likely scenario in the event of rebuilding or recovery after a disaster. The elements of meaningful research are introduced in this paper, and the next step is to evaluate competing methodologies for identifying vulnerabilities and assessing economic risk at the local and regional scales for organizations large and small, whose dependence on the Internet for business operations is on the rise. These elements—dependence on the telecommunications network, in general, and the Westin hub, in particular, for businesses individually and in aggregate, in local concentrations and throughout the region, for supply chains and services critical in emergency situations—should serve as guideposts for

economic analysis. On the basis of the economic analysis, businesses and governmental agencies can then revisit their options for reinvestment in the physical infrastructures that are increasingly vital to business operations.

4.3 Policy Recommendations

The vulnerable nature of small- and mid-sized businesses and the fundamental role they play in post-disaster redevelopment sheds light on policies intended for both private and public audiences. Critical infrastructures cannot become everything without the risk of them becoming nothing. Thus, it is unreasonable to expect the economic needs of one region to occupy the national stage. What our analysis suggests is that a richer understanding of the dependencies and feedback loops between small- and mid-sized business and the physical facilities, such as telecom hotels, on which they are dependent is an important component of regional plans for disaster recovery for regions across the United States and, indeed, perhaps, the key to reducing the time between disaster and redevelopment. This regional perspective suggests changes in communication and accountability between organizations at many levels for many reasons.

Policy could recognize the enhanced ability of large firms to address business continuity. Large firms enjoy seats at table-top exercises and are encouraged to become cooperative partners with government agencies in the relatively data-rich environment of planning for national security and critical infrastructure protection. What if the contractual obligations of large firms with their small- and mid-sized counterparts reflected this ability?

What if small- and mid-sized businesses, when contracting with larger firms for telecommunications, Internet and cloud services were explicitly told the extent of the risk they would have to shoulder? It is entirely possible for any given business to explicitly delineate risk without divulging the exact nature of vulnerabilities. What if, to go one step further, large firms were compelled to offer data back-up and reinstatement guarantees and financial compensation for service disruptions, even in the case of a disaster? Financial compensation could be a joint effort between public and private interests. The answers to these questions focus squarely on the short window of time—the two weeks or so of an outage—during which vulnerable small- and mid-sized businesses cease to exist. What if claims of 99.999 percent reliability were to become contractual obligations of liability?

One may assume that telecommunications firms, major ISPs and cloud providers are prepared to address the needs of a region. Perhaps, though, this is not the case. As capable as private firms are, there is no form of organization more compelled to act in the long-term interest of the public than government. Today's political atmosphere may or may not be conducive to proposals for infrastructure reinvestment, but it is important to remember that the Internet was a government project executed for the national interest. If the protection of regional economies demands greater redundancy in web architectures than what private firms provide,

then it would seem that governmental investment in redundancy is necessary. If the increasing value of the data in telecom hotels to the economy and society demands greater investment in software and hardware security than what the firms provide, then government action to compel or support such investments would seem prudent for the public interest.

For regional as well as national security reasons, information sharing is in the public interest. The more information about weaknesses in existing system architectures made available to an entity, the more an entity would be able to minimize investment in redundant physical infrastructures. Business claims of proprietary information arise from concerns about corporate espionage or fear of customer reaction to vulnerabilities. These could be strong incentives for any business to keep data about weaknesses out of sight from customers and government agencies. Businesses that keep data out of sight may also have simply underinvested in the study of issues such as business continuity and disaster planning.

The public availability of the locations of telecom hotels promises to inspire regional dialog amongst all interested parties. Policymakers can and should explore the upside and downside of secrecy about networked telecommunications infrastructures and data centers for services on the Internet. Policies that bring all organizations closer to the commitment of resources commensurate with recognition that telecom hotels and the Internet, in general, serve as public utilities will truly serve the public interest.

In summary, policies should include:

- Changes to regulations to compel private industry to incorporate estimates of regional economic vulnerability impact in business continuity planning.
- Regulatory requirements that inform businesses of potential regional vulnerabilities and a framework for medium- to long-term business continuity planning in light of the realities.
- Investigation of the potential for contractual obligations between carriers and businesses and alternative institutional arrangements to address the risk from outages to small- and mid-sized business.
- Regulatory requirements for wider participation in table-top emergency exercises that include catastrophic contingency scenarios.
- Investments to ensure the security and redundancy of Internet architectures that address vulnerabilities at the regional scale and bridge the cost/benefit business strategies of privately-held telecommunications infrastructure entities.
- Investigation of the potential for sunshine laws for public disclosure and the secret disclosure of system architectures to organizations that act in the public interest.

4.4 Next Steps

In the short term, research is needed to understand the magnitude and nature of economic risk to the regions of the U.S. from telecom hotel outages, carrying through to scenarios of disaster, response, recovery and redevelopment that highlight the ability of small- and mid-sized businesses to stimulate post-disaster economic growth.

If a process for scoping the regional economic impact could be captured in advance of a disaster, then the information could inform medium-term and long-term recovery planning. Such projections could provide a credible means for estimating the cost and benefits of creating infrastructure redundancies.

As the case of the Seattle Westin illustrates, telecom hotels are models for businesses that make the details of their operations publicly available. In contrast, cloud providers such as Google are dedicated to a strategy of hiding their massive investments in data centers in plain sight. There is no time like the present to engage in thoughtful dialog about the benefits and pitfalls of these two radically different approaches, and the possibility of information sharing for the expressly public purpose of regional continuity planning.

Finally, vulnerabilities in telecom hotels or in regional infrastructures that exist simply because of under-attention or under-investment need to rise higher in the agendas of local and regional business leaders and policymakers. This is may well be an urgent issue as the cloud computing paradigm explodes.

5. Conclusions

Telecommunications hubs, in the form of telecom hotels, offer economic advantages that attract collocated investments in data centers and meet-me rooms. Meanwhile, cloud computing technologies are paving the way for growth in these hubs by lowering the barriers to entry and expansion of online business. By their nature, however, telecommunications hubs concentrate assets and tentacle into other infrastructures, increasing the risk of cascading impacts from a disaster. Across the United States, national agencies and large firms are presumed to use this knowledge to plan and organize for business continuity.

However, the concentration of key components of the telecommunications infrastructure in telecom hotels represents a significant vulnerability at the local and regional scale. As demonstrated in New York on 9/11, the partial or complete destruction of a major hub can create significant disruptions to local and regional businesses. Local reliance on the Internet backbone is significant and continues to grow. Telecom hotels are private businesses that market services. They are also highly visible and accessible targets for terrorism. While federal agencies are concerned with the national availability of the Internet to provide necessary services, they leave considerations of local and regional resilience to the private sector as part of business continuity planning. Private sector entities most likely lack the knowledge and

ability to plan for a disaster that could affect an entire region. It is, therefore, imperative to develop a model that could clarify and quantify the risks inherent in the dependence on telecom hotels from local and regional perspectives.

References

[1] *National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Norton, New York, 2004.

[2] B. Roberts, The Macroeconomic Impacts of the 9/11 Attack: Evidence from Real-Time Forecasting, Office of Immigration Statistics Policy Directorate, Department of Homeland Security, Washington, DC (www.dhs.gov/xlibrary/assets/statistics/publications/ois_wp_impacts_911.pdf), 2009.

[3] W. Thompson, Jr., One Year Later: The Fiscal Impact of 9/11 on New York City, Office of the Comptroller City of New York, New York, (comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf), 2002.

[4] New York State Department of Public Service Office of Communications, Network Reliability After 9/11: A Staff White Paper on Local Telephone Exchange Network Reliability (www.neutraltandem.com/documents/NetworkReliability.pdf), 2002.

[5] American Social History Project, (C. Clark, N. Hewitt, R. Rosenzweig, N. Lichtenstein, J. Brown, D. Jaffee), *Who Built America? Working People and the Nation's Economy, Politics, Culture, and Society, Volume 2: From the Gilded Age to the Present*, Pantheon, New York, 2008.

[6] Federal Communications Commission, Telecommunications Act of 1996, Washington, DC (www.fcc.gov/telecom.html)

[7] Go Northwest! About the Northwest Economy, Spokane, Washington (www.gonorthwest.com/Visitor/about/economy.htm), April 4, 2012.

[8] W. Beyers, The Economic Impact of Technology-Based Industries in Washington State, Department of Geography, University of Washington, Seattle, Washington (www.technology-alliance.com/documents/TA_EconomicImpact_2010_FINAL-WEB.pdf), 2010.

[9] R. Horak, *Telecommunications and Data Communications Handbook*, Wiley, Newark, New Jersey, 2007.

[10] B. Stewart, Internet Network Topology, The Living Internet (www.livinginternet.com/i/ia_tools_top.htm), 2012.

[11] Data Center Map, ActiveWebs, Aarhus, Denmark (www.datacentermap.com/usa), May 17, 2012.

[12] Centerspan, What is the Internet? (www.centerspan.org/tutorial/net.htm).

[13] H. Newby, Meet Me in Seattle, in *Fatpipe*, NA Publishing, Ann Arbor, Michigan, pp. 40-42 (www.telx.com/ArticlePDF/Meet%20me%20in%20seattle%20june%202003.pdf), 2003.

[14] M. Ordonez, Critical Infrastructure Protection: How to Assess and Provide Remedy to Vulnerabilities in Telecom Hotels, Master's Thesis, Naval Post Graduate School, Monterey, California (http://edocs.nps.edu/npspubs/scholarly/theses/2006/Sep/06Sep_Ordonez.pdf), 2006.

[15] H. Newby, Guide to Key U.S. Carrier Hotels, The Tel^{x} Group, Inc., New York (www.slideshare.net/flyingpotato/guide-to-key-us-carrier-hotels-by-hunter-newby-telx), (September) 2007.

[16] National Security Telecommunications Advisory Committee (NSTAC), Vulnerabilities Task Force Report—Concentration of Assets: Telecom Hotels, Washington, DC (www.ncs.gov/nstac/reports/2003/Telecom%20Hotels.pdf), 2003.

[17] J. Savageau, Telecom Risk and Security Part 3 – Human Factors, Convergence Technology Council, Honolulu, Hawaii (john-savageau.com/2009/10/13/telecom-risk-and-security-part-3-%e2%80%93-human-factors), October 13, 2009.

[18] P. Parfomak, Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options, CRS Report for Congress, Congressional Research Service, Washington, DC (www.fas.org/sgp/crs/homesec/RL33206.pdf), 2008.

[19] Regional Economics Institute at Colorado State University, Job Growth from Mid-Sized Businesses, Fort Collins, Colorado (csurei.wordpress.com/2012/04/16/job-growth-from-mid-size-businesses), 2012.

[20] G. Makinen, The Economic Effects of 9/11: A Retrospective Assessment, Report for Congress, Economic Policy Government and Finance Division Report, CRS Report for Congress, Congressional Research Service, Washington, DC, p. 38 (www.fas.org/irp/crs/RL31617.pdf), 2002.

[21] A. Townsend and M. Moss, Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications, New York University, New York (www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf), 2005.

[22] M. Rice, J. Butts, R. Miller and S. Shenoi, Applying public health strategies to the protection of cyberspace, *International Journal of Critical Infrastructure Protection*, vol. 3(3-4), pp. 118-127, 2010.

[23] Miniwatts Marketing Group, Internet World Stats: United States of America Internet Usage and Broadband Usage Report, Bogota, Columbia (www.internetworldstats.com/unitedstates.htm), January 17, 2012.

[24] J. Savageau, Telecom Risk and Security Part 2 – The Carrier Hotel SuperNode, Convergence Technology Council, Honolulu, Hawaii (john-savageau.com/2009/10/12/telecom-risk-and-security-part-2-%e2%80%93-the-carrier-hotel-supernode), October 12, 2009.

[25] The Westin Building, Seattle, Washington (www.westinbuilding.com).

[26] C. Lian, J. Santos and Y. Haimes, Extreme risk analysis of interdependent economic and infrastructure sectors, *Risk Analysis*, vol. 27(4), pp. 1053-1064, 2007.

[27] R. Miller and P. Blair, *Input-Output Analysis: Foundations and Extensions*, Prentice-Hall, Englewood Cliffs, New Jersey, 1985.

[28] A. Rose, J. Benavides, S. Chang, P. Szczesniak and D. Lim, The regional economic impact of an earthquake: Direct and indirect effects of electricity lifeline disruptions, *Journal of Regional Science*, vol. 37(3), pp. 437-458, 1997.

[29] A. Rose and S. Liao, Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions, *Journal of Regional Science*, vol. 45(1), pp. 75-112, 2005.

[30] D. McMillen, Perspectives on Spatial Econometrics: Linear Smoothing with Structured Models, Journal of Regional Science, 52 (2) (2012) 192-209.

[31] S. Gibbons and H. Overman, Mostly pointless spatial econometrics? *Journal of Regional Science*, vol. 52(2), pp. 172-191, 2012.

[32] M. Partridge, M. Boarnet, S. Brakman and G. Ottaviano, Introduction: Whither spatial econometrics? *Journal of Regional Science*, vol. 52(2), pp. 167-171, 2012.

[33] M. Roskind, Personal communication, National Communications System, Cybersecurity and Communications, Department of Homeland Security, Washington, DC. April 15, 2012.

[34] J. Villasenor, Securing an infrastructure too complex to understand, The Brookings Institute, Washington, DC (www.brookings.edu/opinions/2011/0923_infrastructures_villasenor.aspx), 2011.

[35] J. Markoff, Hiding in plain sight, Google seeks more power, *New York Times*, June 14, 2006.

Table 1: Internet Exchange Points and Data Centers in the United States [11].

State	Internet Exchange Points (IXPs)	Number of Data Centers per State	Major Urban Concentrations of Data Centers
Alabama		5	
Arizona	Phoenix	22	Phoenix: 19
Arkansas		2	
California	Bay Area (3)/LA	148	Bay Area: 37/LA: 47
Colorado		25	Denver: 21
Connecticut		8	
Delaware		2	
District of Columbia		6	
Florida	Tampa/Miami	52	Miami: 20
Georgia	Atlanta	32	Atlanta: 20
Hawaii		2	
Idaho		6	
Illinois	Chicago	49	Chicago: 49
Indiana		21	Indianapolis: 9
Iowa		8	
Kansas		7	
Kentucky		11	
Louisiana		5	
Maine		2	
Maryland		15	Baltimore: 6
Massachusetts	Boston	26	Boston: 19
Michigan		29	Detroit: 16
Minnesota		12	
Mississippi		3	
Missouri	Kansas City	22	St Louis: 12
Montana		2	
Nebraska		8	
Nevada		9	
New Hampshire		3	
New Jersey		36	Hudson County: 19
New Mexico		4	
New York	NYC	84	NYC: 44
North Carolina		23	Charlotte: 10
Ohio		41	Columbus: 14/Cincinnati: 10
Oklahoma		12	
Oregon	Portland/Eugene/Medford	13	
Pennsylvania	Pittsburgh	27	Pittsburgh: 10/Philadelphia: 11
Rhode Island		2	
South Carolina		6	
South Dakota		3	
Tennessee		21	Nashville: 9
Texas	Dallas	97	Dallas: 44/Houston: 30
Utah		15	Salt Lake City: 9
Vermont		4	
Virginia	Ashburn	32	Ashburn: 9
Washington	Seattle	42	Seattle Metropolis: 32
Wisconsin		14	
Wyoming		3	