ASA

Annie Searle & Associates LLC

Risk and the Communications Sector

By: Swati Chaturvedi

Keywords: Communications Sector Risk, Federal Communications Commission (FCC), National Communications System (NCS),Critical Infrastructure

Abstract:The Communications sector is one of the eighteen critical infrastructuresin United States and is vital for national security, public health and safety and economic prosperity. It alsoforms an integral component of the US economy impacting operations of government, industries across public and private sectors, and other critical infrastructures.These factors and recent technology advancements have exposed new risks for the Communications sector, demanding focus of both government and private sector on managing and reducing risks by striving to ensure that the nation's communications networks and systems are secure, resilient, and rapidly restored if impacted by a disaster.

Introduction

This research note discusses the key risks, hazards and vulnerabilities related to the Communications Sector on both the government side and the private sector side. Further, this research note will review the role of government agencies in regulating the Communications Sector, their effectiveness in exercising sector specific controls and their relationship with the private sector in coordinating efforts to reduce risk across the Communications sector. This research note will also examine the interdependencies between the Communications sector and other critical infrastructures. Lastly, this research note will present recommendations to improve and enhance the protection and resilience both on the side of government and the private sector.

Overview

Communications is one of the[1] eighteen critical infrastructures and key resources (CIKR) sector of the United States that is essential to the national security, public health and safety, economic prosperity and operations of government and all businesses. The Communications sector, consisting of wired, wireless, satellite, cable, broadcasting and

Internet, forms the communications backbone of the US economy impacting a variety of industries in both the public and private sectors.

The majority of the Communications sector in the United States is privately owned with the Federal Communications Commission (FCC) as the government agency and the U.S. Department of Homeland Security's (DHS) National Communications System (NCS)[2] forming its designated Sector Specific Agency (SSA). As the Communications sector's government agency, the FCC is responsible for designing policy frameworks, supporting emergency operations, ensuring public safety, universal availability and accessibility of basic telecommunications service to everyone and protecting interests of the consumer in the communications marketplace. NCS, on the other hand, works in collaboration with its partners to develop and implement the Communications Sector Specific Plan (CSSP)[3]for reducing the risk across the Communications sector and improving the protection and resilience-building programs and activities. CSSP lays out the coordinated protection strategy allowing the Federal Government to develop and execute plans for national security and public safety and permitting private companies to reduce operational risks, maintain

business continuity and achieve the sector goals by utilizing resources from both the public and private sectors.

Risks – Government Side

As the Communications sector government agency,the FCC faces a variety of risks from both the internal and external threats. Some of these risks are malware attacks, malicious email links, phishing, cyber criminals, hackers, insider threat, hactivists and terrorist attacks.

Cyber attacks and security breach incidents on government agencies such as United States Senate, Central Intelligence Agency (CIA), InfraGard and Arizona Department of Public Safety in the past yearsemphasize the risk of cyber attacks from cyber criminals and hackers through means of malware, malicious email links, phishing etc. for the FCC and its critical information systems.[4]

Just like any other organization, the FCC also runs the risk of insider threat from disgruntled employees and unauthorized staff access, which could lead to misuse of critical information, intentional misappropriation of the FCC assets, misuse of individual position or authority in the government agency to commit insider fraud.

The FCC also faces the risk of hactivism in which its computer and computer networks could be misused to protest political ends or promote political ideology by spamming political ideals and issues. These activities could disrupt national peace and lead to political upheaval in the country or certain sections of the society.

The importance of the Communications sector in national safety, economic prosperity and public wellness makes government agencies like the FCC and its partners a potential target of terrorist groups. Any terrorist attack on the FCC or its partners could directly impact 911 calls, national emergency alert systems and radio and television broadcast stations for news and updates that are vital to achieving a successful response to emergency operations.

Risks – Private Sector Side

As mentioned earlier, the Communications sector offers a wide range of services such as wired, wireless, satellite, cable, broadcasting and Internet through a fleet of its private companies. While few of the risks described above are also relevant to the Communications private sector, some others are specific to the private sector and are largely based on the communications service or the set of services provided by

a company. This research note willdiscuss risks for two private entities in the Communications sector – Comcast[5] and Sprint[6]. These risks can be extended to other companies in the Communications sector as well. Some of the risks relevant to these companies are – 1) Technological advancements 2) Loss of intellectual property 3) Security breach and cyber attacks on the communications network 4) Blurring dividing lines between the various communication services 5) Market competition and consolidation 6) Weak economic conditions and 7) Regulatory restrictions and additional costs. These risks are discussed in detail in the following sections.

Most private sector companies in the communications sector face the risk of technological advancements such as IP technology, 4G etc. arising due to significant changes and improvements in the digital technology. These changes cause uncertainty regarding future subscriber demands for the communication services, service pricing and ability of service providers to meet the technology advancements on a timely basis. Failure to effectively respond to these technology advancements can seriously impact the company's operations and business.

Companies in the communications industry rely heavily on the use of intellectual property such as patents, copyrights and trademarks owned internally or through third party and vendors. Any legal challenges or claims regarding infringement of intellectual property could incur substantial liability in terms of time, money and resources affecting not only company's reputation in the market but also limiting its ability to compete effectively in the marketplace.

Security breach of the communication information systems could lead to misuse or loss of company data, customer information and vendor relations. On the other hand, the increased threat from cyber attacks, hacking and denial of service on the communication network could not only have a devastating effect on company's reputation and financial standing but could also seriously impact the national security and public safety. A few examples of cyber attacks and security breach incidents on private companies in the Communications sector in recent times are Fox Broadcasting Company, PBS and L3 Communications.

Joint ventures and recent advancements in the communications sector has blurred the traditional line among the communication services such as long distance, local, wireless, video, internet and

satellite by integrating these services into packages. These changing trends can impact the pricing models of the communication services affecting the company's financial strength, revenues, growth and profitability.

Mergers and acquisitions in the Communications sector have consolidated the Communications marketplace allowing few players to exercise increased control in the market and hence disrupting the balance in the national Communications ecosystem.

Weak economic conditions in the United States and globally impacts the customer spending pattern and may reduce their ability to subscribe to certain discretionary communications services such as cable, video streaming over internet and data plans for the mobile devices.

Federal agencies governing the Communications sector present risks of increased operating costs, stringent regulations and additional operating restrictions to the service operators in the private sector. Failure to comply with the regulations carries a further risk of penalties, fines, license revocation and other liabilities that could adversely affect

the business operations and market reputation for the companies in the private sector.

Controls

Some of the risks mentioned in this research note have to be dealt with internally by company specific controls.Others however require sector specific controls and are dependent on policies and regulations by the FCC, Sector Specific Agency NCC and their partners for mitigation. In order to do so, the FCC has laid out certain regulations to govern the Communications sector. Some of these regulations are discussed in this section.

Currently,the FCC requires wireless and broadcasting infrastructure owners to file information on the communications equipment location and type. The FCC mandates wireline, wireless, cable and satellite carriers and operators to annually submit data on infrastructure, network outages and financial standing allowing the FCC to measure competition and service quality. Furthermore, the FCC maintains a team of experts to analyze this data in an attempt to reveal troublesome trends in network reliability and security, assess cause of network outages and evaluate measures used to restore service.

Analysis of this data lets the FCC determine the adoption of best practices and devise revisions to further improve the communications network reliability and security across the sector.

Apart from this, the FCC is also responsible for allocating spectrum for public safety[7] and television broadcasting, commercial licensing of radio waves, regulation of obscenity, indecency and profanity of broadcast content, maintaining fair market practices and sound competition to protect consumer interest in the Communications sector.

Over time, the FCC has not only established sector specific regulations and controls but has also put these regulations to practice to govern the Communications sector, promote best practices and protect consumer interests. This section discusses few examples to demonstrate these regulations in action and determine their effectiveness. A recent example of this is the failure of AT&T and T-Mobile merger.[8] The FCC determined that approval of the merger of the two wireless operator giants would drastically reduce market competition and investment in the wireless space and questioned the underlying claims of serving public interest and necessity. Based on

their investigation and above considerations, the FCC ruled against the merger of AT&T and T-Mobile securing consumer interest in the Communications marketplace and proving effective in regulating the market dynamics. This however is not always the case. According to another recent example, the consumer watchdogs at Environmental Working Group accused the FCC of deliberately shielding information from the public about possible concerns related to cell phone radiationin response to pressure from the Cellular Telecommunications and Internet Association (CTIA). The FCC however, responded to these claims by saying that there is "no scientific evidence that proves that wireless phone usage can lead to cancer."[9] As a body responsible for regulating cell phones and the Communications sector, the FCC can prove to be more effective and reliable by providing relevant references related to the subject matter and appropriately advising the consumers of the potential risks of exposure to radiation and suggesting mitigations on how to avoid it.

Interdependencies

The Communications sector is closely linked to other critical infrastructures and shares interdependency with the Energy,

Information Technology, Banking and Finance, Postal and Shipping, and Emergency Services sectors.[10] Both the government agencies and private sector companies in the Communications sector rely heavily on the Energy sector for power to run the cellular towers, central offices and other critical communication facilities and infrastructure. The Communications sector also relies on the Information Technology sector for control systems, Internet and technology infrastructure, software, operating systems and anti-viruses. The Banking and Finance sector relies on telecommunications for the transmission of financial transactions and stock market operations. The Postal and shipping sector consumes the Communications services for tracking shipments and running their control systems. Lastly, the Emergency services depend on the telecommunications for receiving emergency 911 calls and accordingly disseminating resources, coordinating responses, alerting public and responding to emergencies. These interdependencies highlight the importance of the Communications sector and its criticality not only for its customers but also for other critical infrastructure sectors and their smooth operation.

Recommendations

Rapid transformations in the Communications sector require continuous advancements in regulations on the government side as well as their implementation and adoption in the private sector side. Key recommendations for government sector on next steps towards responding to advancements and maintaining higher level of resiliency both on the government side and in the private sector are:

- Maintain pace with technology advances to devise new regulations and policies or upgrade the existing ones
- Develop and implement agile, effective, cost efficient and robust cyber security approaches to deal with the growing threat of cyber attacks and security breaches
- Enhance public safety infrastructure and emergency call service to enable transmission of text, image and video to introduce Next-Gen 911[11]
- Establish transparency in distributing information on issues in public interest such as health hazards from cellular radiations and usage, consumer rights etc.

While it is important that on the government side, the FCC implements the above recommendations, it is equally vital that as a Sector Specific Agency, NCS updates the Communications Sector Specific Plan (CSSP). Itis also advised that NCS improves collaboration with its partners to include appropriate measures and controls to reduce operational risks and improve the protection and resilience-building programs and activities. These controls can further prove to be more effective in reducing risk across the Communications sector if implemented industry wide by leveraging resources from both the public and private sectors.Based on this premise, the key recommendations for managing risk and maintaining business continuity on private sector side are:

- Maintain pace with technology advances to offer competitive services and prices
- Similar to government side, develop and implement agile, effective, cost efficient and robust cyber security approaches to deal with the growing threat of cyber attacks and security breaches
- Ensure compliance to changing regulations by increasing frequency of internal audits

- Protect intellectual property such as copyrights, trademarks etc. and avoid infringements by increasing awareness amongst employees and partners regarding effective management and use of intellectual property

On top of the above recommendations, it is highly advised that concrete efforts be put in the direction of improving collaboration and fostering relationship between the FCC, the NCS, State and local partners and private sector companies like AT&T, T-Mobile, Sprint, Comcast, Dish etc. to effectively manage risk and maintain a healthy ecosystem in the Communications sector.

References

[1]"National Infrastructure Protection Plan - Communications Sector." Homeland Security, Web. 5 June 2012.<http://www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf>

[2]"Communications Sector." National Communications System, Web. 5 June 2012. <http://www.ncs.gov/communications_sector.html>

[3]"Communications Sector-Specific Plan." *Homeland Security*. N.p., n.d. Web. 5 June 2012. <http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf>

[4]"Cyber Security Executive Update." *Federal Communications Commission*. N.p., 25 July 2011. Web. 5 June 2012. <http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-10/oct27-2011_FCC-cybersecurity-exec-summary_RNaylor.pdf>

[5]"2011 Annual Report on Form 10-K." *Comcast Corporation*. N.p., n.d. Web. 6 June 2012. <http://files.shareholder.com/downloads/CMCSA/1904032778x0x561695/79426950-eb48-4e46-a761-f999d155a226/BookmarkedComcast10K.pdf>

[6]"Annual Report on Form 10-K." *Sprint Nextel Corporation*. N.p., n.d. Web. 6 June 2012. <http://investors.sprint.com/Cache/1500039807.PDF?D=&O=PDF&IID=4057219&Y=&T=&FID=1500039807>

[7]Moore, Linda K. "CRS Report for Congress." 23 June 2005. Web. 6 June 2012. <http://www.au.af.mil/au/awc/awcgate/crs/rl32594.pdf>

[8]Velazco, Chris. "The AT&T/T-Mobile Merger Is Dead." *TechCrunch*. N.p., 19 Dec. 2011. Web. 6 June 2012. <http://techcrunch.com/2011/12/19/att-tmobile-merger-dead/>

[9]Sheppard, Kate. "Is the FCC Downplaying Potential Risks from Cell Phone Radiation?."*MotherJones*. N.p., 3 June 2011. Web. 6 June 2012. <http://www.motherjones.com/blue-marble/2011/06/fcc-downplaying-potential-risks-cell-phone-radiation>

[10]"Communications Sector: Critical Infrastructure." *Homeland Security*. N.p., n.d. Web. 5 June 2012. <http://www.dhs.gov/files/programs/gc_1189102978131.shtm>

[11]Jackson, William . "FCC's 5-step plan for deploying Next-Gen 911." *Government Computer News (GCN)*. N.p., 8 May 2012. Web. 6 June 2012. <http://gcn.com/articles/2012/06/11/next-gen-911side-fcc-5-step-roadmap.aspx>