Critical Infrastructure Interdependence: Cyber-Telecommunications Perspective

Testimony of Karl F. Rauscher

Founder and President

Wireless Emergency Response Team (WERT)
www.wert-help.org

Before the

House Select Committee on Homeland Security

Subcommittee on Cybersecurity, Science, and Research and Development

Subcommittee on Infrastructure and Border Security

Hearing on

Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness

September 4, 2003

Chairman Thornberry, Chairman Camp, Congresswoman Lofgren, Congresswoman Sanchez, Congressman Cox, Congressman Turner, and other Distinguished Members: thank you for the opportunity to speak today and provide a perspective from another critical infrastructure – the telecommunications and Internet services industry.

Introduction

My name is Karl Frederick Rauscher. I am the Founder and President of the Wireless Emergency Response Team, a non-profit organization supported by expert volunteers from the private sector and numerous government agencies. My experience related to today's subject matter includes . . .

- 18 years of communications industry experience at Bell Communications Research & Lucent Technologies Bell Labs
- I have led numerous highly successful improvement programs in quality and reliability. With a background of advanced concepts in software, systems, architectures and networks, I have invented software testing techniques that have delivered dramatic breakthrough quality improvements. I am a recipient of the Bell Labs President's Award for bringing the first telecommunications network switch to "6 9's" of reliability, which means 99.9999% uptime, or less than 30 seconds of downtime per year (independently verified with pubic data). In my 10 years at Bell Communications Research, I have personally uncovered over 1000 software design errors in programs running on live network systems. I have recently conducted Homeland Security research at an offshore software development outsourcing facility.
- As Vice Chair of the industry's Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC), I oversee the "deep dive" cause analyses that occur for each major network outage. These analyses are conducted voluntarily by the industry for the purpose of determining if existing Best Practices are sufficient to prevent similar, future events. The NRSC also provides an annual report on the health of the nation's public networks.
- As a member of the Telecommunications-Information Sharing and Analysis Center (ISAC), I am routinely involved in industry mutual-aid responses. I was directly involved in the communications industry's coordination and response to the recent Power Blackout – from the initial report assessments through ongoing after-action reviews.
- I have led combined government and industry efforts to produce over 500 Best Practices for network reliability and Homeland Security. The Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) Best Practices are the most comprehensive and authoritative guidance in the world for public communications. Best Practices, while totally voluntary, are implemented at a high level throughout the industry, and are consistently credited with preventing network service disruptions. In addition, I have led industry discussions on blended physical and cyber attacks.
- I am the Chair-Elect of the international IEEE Technical Committee on communications Quality and Reliability. I oversaw Best Practice guidance on ultra-high reliability and ultra-high security for world-class events, which benefited the Olympics, among others.
- I am on the Board of Advisors for the Center for Resilient Networks
- I have participated in the President's National Security Telecommunications Advisory Committee (NSTAC)

- Most importantly, I have access to the right people – those who are world-class experts, who will tell it like it is, and then take the necessary actions.

My perspective includes very human aspects of this discussion. In pressure-heated crises, I have brainstormed with brave first responders and listened to family members - pleading for everything to be done with technologies that they do not understand - to save their loved ones. In moments of heavy telephone silence, I have connected on a personal level with strangers in distant places – this has made a lasting impression on the vital need to connect the best minds of the industry with the most vital needs of its subscribers in an emergency.

Role of Wireless Communications in Disaster Response

On the morning of September 11, *wireless communications* were used by countless Americans in their usual ways.

And then evil terrorists emerged to make their dark mark on human history.

During those same moments, *wireless communications* were used by brave hostages in the skies to report the hijacking of their planes, then by expectant victims to speak their last "GOOD BYE" and "I LOVE YOU", and then by rescue teams as they rushed to bring aid.

Wireless devices, such as cell phones and PDAs, played a vital role on September 11 because they are popular, easy to operate, one of the few items carried everywhere by their users, and can still function when severe damage is done to surrounding infrastructure. Instruments routinely used for conducting business and nurturing relationships were then, in their final mission, being used to secure the safety of the United States of America, or bring two individuals together for a final, treasured moment.

That night, news reports stated that cell phones were being used to call for help from the rubble in New York City. At this point, the vision for a coordinated industry emergency response was conceived. In the following hours and days, an unprecedented wireless communications industry mutual-aid effort sprang into action to support Search and Rescue efforts at the World Trade Center disaster site. The Wireless Emergency Response Team was formed.

Due to the nature of the building collapse, the team was not able to rescue victims from the rubble. However, value was realized in several ways: keeping rescue teams from danger by quickly discrediting false reports, confirming those thought to be missing as safe, and helping to bring closure for family members. WERT's Final Report documents the key lessons-learned and recommendations, so that this capability can be enhanced and optimized. May God forbid that such a tragedy and horror would ever be visited on us again. But if it does, WERT will be ready to bring the best minds and resources of the wireless industry together to work hand-in-hand with traditional first responders on the never changing top priority after a disaster – saving human life.

The August 2003 Power Blackout

Observed Characteristics

Most of the characteristics of the recent Power Blackout were similar to crises already experienced by the communications industry.

1. The duration was similar to very large power outages, for example the result of large ice storms
2. The hot and humid seasonal climate was challenging for electronic equipment
3. There were rolling blackouts and requests for load shedding

Other characteristics, while familiar, were turned up a few notches in intensity and resulted in more pressure on our industry:

4. While ice storms, heavy snowfalls and hurricanes have been widespread, the August Blackout was even more widespread, affecting multiple major U.S. cities.
5. The cause was unknown
6. Many people have cordless phones in their home that could not function
7. Because of the times we are living in, New Yorkers were more jittery, intensifying their need for wireless communications

The third set of characteristics was mostly new, and their study will be the source of new lessons-learned from this event:

8. The most notable being that, like September 11, this was a widespread catastrophic event that was *unanticipated* (unlike ice and snow storms, or hurricanes)
9. Also, there were multiple cyber threats in play around this time
10. Air and other public transportation was halted
11. There were new levels of pressure on fuel suppliers, who are critical in supporting back-up power generators

Wireless Network Observations

During the first half-hour after the power was lost, enormous spikes in the number of call attempts were seen – up to one thousand percent of normal traffic levels. During the next several hours, traffic hovered around one hundred percent above normal levels. Any service problems during the early timeframe were likely due to congestion caused from this very unusual demand.

For the most part, the wireless systems and networks were working as designed. When commercial power was lost, cell towers drew power from back-up batteries until power was restored or until the battery power was consumed. The wireless industry will factor new insights gleaned from this historic event into future risk assessments and emergency planning capabilities.

New Areas That Worked Well

Mobile Text Messaging

The WERT Final Report points out that during times of heavy congestion, a text message (e.g., SMS) attempt is more likely to succeed than a voice call because there are lower requirements for bandwidth. Interestingly, mobile text messaging also has consumes less power in both the network and the handset. It is encouraging that early reports indicate that there was marked increase in the use of text messaging during the Power Blackout.

Telecom –ISAC and Electricity Sector ISAC Interactions
Inter-ISAC interaction was effective. This was an immense demonstration for the potential of what could be accomplished with ISAC-to-ISAC coordination.

Other Lessons Learned

- It is better to have one national point of government-industry information sharing through the various sector's ISACs for efficiency and accuracy
- Homes should have a corded phone as an emergency back-up, because the batteries of cordless phones can run out
- Businesses should conduct risk assessment to determine the criticality of back-up power capabilities to their operations

Government – Industry Partnerships
Make no mistake about it: The communications industry is a fiercely competitive battlefield. Yet a remnant of something tremendously precious survives. Through the divestiture of the 1980s and the Telecommunications Act of 1996, a precious aspect of the culture of the traditional telephone company lives on – it is one that ascribes to itself an obligation to the safety of society.

As the head of a non-profit volunteer organization, the spirit that was exhibited by thousands on September 11, and the recent Power Blackout, is tremendously encouraging. WERT has captured some of that spirit in harnessing the expertise, will and compassion of so many volunteers, along with their companies' or agencies' support. Two years ago, for 3 weeks, we knew that, if there were victims in the rubble with cell phones, we may be their only hope. WERT volunteers did everything possible to listen for any signal from a possible survivor. By continuing to fulfill the mission of WERT, the wireless industry shows itself good stewards of its powerful technologies.

The President has called on the people to be volunteers. In addition to soup kitchens and mentoring programs, critical infrastructure technology experts have figured out what they can "do for their country" in these anxious times. There are countless individuals who give of their vacation time, evenings and weekends because of their sense of duty and love for this country. They develop Best Practices and standards, conduct research, provide explanations to government officials and are on call 24 by 7 for the next crisis.

Industry-Government partnerships are supported by significant volunteer effort and are highly effective.

Dependence on Cyber and Wireless Capabilities
There are awesome advantages for a society connected by high-speed mobile communications. More information, in a variety of formats (voice, data, video) will be delivered. Wireless communications and the Internet play increasingly important roles in society, and particularly in emergency response. In the not-to-distant future . . .

- A firefighter may have hands-free constant communication with his team
- His vital signs may be monitored remotely from the safety of a distant command center

- As he carefully walks from room to room, infrared imaging data from the floors and walls may be combined with that of other firefighters to alert those in harm's way to possible danger.

The possibilities are endless, for every aspect of society. On the horizon is a world where cell phones, household appliances and even vehicles are nodes on many interconnected networks.

But with this increased connectedness, come inherent vulnerabilities and risks of an imperfect cyber world. The consequences of a software design error can have far reaching effects throughout society. Previous testimony has articulated numerous concerns related to cyber security vulnerabilities, threats, and proposed solutions. In the context of this testimony, I offer several points.

In addition to strengthening reactionary measures - our cyber threat detection and response capabilities - the appropriate investment needs to be made for longer term fixes that address the root of all these problems. Those bailing water out of the boat tend to get a lot of attention because they can show results. We need the patience and resolve to plug the holes and/or build other boats. What are often referred to as "vulnerabilities" in the cyber community are usually the manifestation of a software design error. The kind of thinking that reserves the term "vulnerability" for those characteristics that are truly intrinsic weaknesses of the programming language and operational environments will provide a better grasp of how to get control of this situation. Following on this, I expect that those bold enough to develop new, robust paradigms for programming and those applying classical quality control principles will make major contributions in this area.

Conclusion

The next time you click your "SEND" button to send an email, I ask you to consider the previous effort of the message-bearing marathon runner of ancient Greece. We are now living what has only been dreamed of for centuries before us – and we are just about there – being able to communicate in any fashion, at any time, at any place.

May it be that when a generation from now looks back on how we faced these cyber and physical challenges, that the scientists and engineers were found to be unimaginably innovative; may our leaders be found to have been enablers of life, liberty and the pursuit of happiness; and may the horrors of terrorism and cyberhackers . . . be only distant memories.

I hope that my insights offered today on the recent power blackout, government-industry partnerships, and dependencies on wireless and cyber infrastructure will be useful to the committee.