

Energy Surety?

By Geary W. Sikich

Copyright© Geary W. Sikich, 2003. World rights reserved.

Published with permission of the author.

Introduction

The North American electrical power grid is a key element of the U.S. infrastructure and is essential to the economy and security of the United States. However, despite our "high tech" economy good old fashioned power outages and failures are still with us, and appear to be an increasing likelihood due to rising electricity consumption, delayed utility investments in generating capacity, poor maintenance practices and mismanagement of assets (you do still remember Enron don't you?).

Blackout the *NEW* Threat to National Security?

The news media has made the blackout of 2003 sound like it is a new threat. Sowing fear, panic and chaos in the minds of viewers, like you, is their mantra. We should, as educated viewers, realize that the media is going to hype any event in order to secure the gold. That gold being ratings! So, let us take a brief walk down the historical path and look at blackouts.

1950 June 6: there is a widespread outage in the Bonneville Power Administration's system in the Pacific Northwest; power plants from British Columbia and Washington to Oregon, Idaho, and Utah and Montana affected.

1959 August 17: New York City experiences a blackout on one network area.

1961 June 13: New York City experiences a blackout in four network areas, caused by electric equipment failures. Midtown Manhattan hit hard.

Thousands Lack Power, Mostly on Lower East Side

"Giuliani said he would continue to seek compensation from Con Ed for police overtime accrued during the blackout, which he put at least \$1.5 million. He added that the cost to businesses and residents from lost goods or commerce was easily several times that, and he urged people to take up the utility's offers of compensation. Con Ed has offered reimbursement for lost perishables, up to \$100 for residents and \$2,000 for businesses. But the Mayor, offering free legal advice, encouraged residents not to sign anything."

excerpted from
New York Times, 7/9/99

Lessons From the Blackout

"Last week's blackout in northern Manhattan and power shortages in New Jersey provided timely reminders that the New York metropolitan region's power supply is not inexhaustible. On the contrary, a robust economy, combined with the increasingly widespread use of computers, fax machines and other high-tech devices, has created an appetite for electricity that could someday exceed the region's capacity to generate it. One answer is to build more power plants and transmission capacity. But that should be only one element in a broader strategy that seeks as well to conserve energy and exploit newer, more efficient technologies."

excerpted from
editorial, New York Times, 7/13/99

1965 January 28: most of Iowa and portions of five other Midwestern states are affected by a blackout; service is restored in only 2.5 hours and the blackout affected only 2 million people.

1971 August 18: in the afternoon there were three near-simultaneous outages in New York State; the New York Power Pool Center weathered the crisis with a minimum of problems; brief cutoff of power to the 200,000 customers of the Long Island Lighting Company.

1976 July 4: one million people in 85 percent of Utah, plus southwestern Wyoming, suffered no power from between 1.5 to 6 hours. Cause is a relay that malfunctioned in the switchyard of a Naughton generating plant near Kemmerer, Wyoming, according to Utah Power and Light Company. The incident does not receive wide press attention.

1977 August 13: New York City suffered a massive blackout. All five boroughs as well as areas in the northern suburbs of Westchester County were plunged into darkness as lightning downed major transmission power lines supplying power to the metropolitan area. While many dealt with the blackout in a peaceful and neighborly fashion, a number of communities erupted in violence. Looters broke into stores, taking merchandise, and destroying local businesses. In place of the evening glow ordinarily produced by the city's abundant electrical lighting, fires lighted the darkened skyline, leaving charred remnants of once lively neighborhoods. Within the short span of two days, police had arrested 3,766 looters and the city had suffered an economic blow that one estimate placed at more than \$300 million. Unlike the 1965 blackout, when the lights went out in 1977 the most distressed neighborhoods of the City endured what Time magazine called "A Night of Terror."

1989 March 13: At 2:44 am, a transformer failure on one of the main power transmission lines in the HydroQuebec system precipitated a catastrophic collapse of the entire power grid.

1996 July 2, 3: The Western Interconnection encompasses a vast area of nearly 1.8 million square miles. At 2:24 p.m. Mountain Advanced Standard Time (MAST) on July 2, 1996, a flashover occurred between a 345,000-volt transmission line and a tree that had grown too close to the line. Over 2 million customers were interrupted on July 2, representing about 10 percent of the total customers served throughout the Western Interconnection. On July 3, 1996, at 2:03 p.m. MAST, a similar chain of events began. The Jim Bridger-Kinport 345,000-volt line again experienced a flashover as the line came into close proximity with the same tree.

As one can readily see by reading the excerpts, power outages resulting in blackouts are nothing new. We have experienced them ever since utilities started to operate the electric grid system. So why make such a big fuss? Restoration of services generally occurs rapidly.

Why Should You be Concerned?

If restoration of services generally occurs rapidly, why should you be concerned? The media hyped *Blackout of 2003* saw power restored in less than a day for many areas. *Monday Night Football* was broadcast from Cleveland, where the possible source of the outage may have occurred (as this is written the cause is still being investigated). So, why should you be concerned? The answer is relatively simple. Because it can and will happen again!

If you are delusional enough to think that this was a fluke event, then you may wish to investigate a great land deal in South Florida (currently under irrigation) or take a look at that bridge for sale in New York City or was it San Francisco? The energy system in the United States of America is operating on thin ice. In 1986 I wrote the following as I was researching opportunities as part of a business plan development model.

ELECTRIC UTILITIES/NUCLEAR SERVICES

In the past several years the electric utility market has changed significantly. In the last six years we have seen the ending of a recession, the end of the Three Mile Island market boom and the emergence of non-traditional but highly qualified competitors which have changed the nuclear services market. We are now beginning to see the effects of the Chernobyl incident; as increased scrutiny is being placed on the operation of nuclear power plants throughout the world.

With some 66 nuclear reactors, of the 135 total reactors currently in the U.S., scheduled for permanent shut down by the year 2010; a significant effort will be required to perform this effort. Public interest groups and state regulators are indicating that utilities are not doing enough to adequately provide for future decommissioning costs. California's Public Utility Commission recently ruled that Pacific Gas & Electric Co. will need to put aside \$53.6 million annually for the next 28 years to fund the dismantling of its Diablo Canyon nuclear facility. Allowing for inflation, shutting the plant in 30 years will cost \$3.89 billion, almost as much as the \$5.8 billion that it cost to build the plant.

Further complicating the issue of plant decommissioning is the fact that as yet, the U.S. has not chosen a radioactive waste disposal site and the effects of inflation are very hard to predict. So far only the Shippingport plant in Pennsylvania, a 72,000 kilowatt plant has actually begun permanent decommissioning. The estimated cost is approximately \$100 million.

The issue of emergency preparedness at nuclear facilities poses special problems, which we have the expertise and experience in solving. The maximum private insurance available to utilities operating nuclear power plants might not come close to covering the property damage from a nuclear accident. It has been estimated that it would cost \$2 billion to decontaminate and remove damaged equipment from a plant after a Three Mile Island type incident. That cost would generally exceed the property insurance coverage carried by most utilities. And the \$2 billion would not cover the cost of repairing or tearing down the damaged plant. There is also the cost of buying replacement power in the interim, which must also be addressed.

According to the Nuclear Regulatory Commission (NRC), safety related electrical and mechanical equipment in nuclear power plants is currently judged on criteria that "have in many instances not

been thoroughly validated." Analysts also say that a number of yardsticks that are needed to evaluate plant safety. Certain designs have prompted the NRC and others to raise questions about safety problems.

GAS UTILITIES

40CFR parts 300 and 355, "Emergency Planning and Community Right to Know Act of 1986", title III of the Superfund Amendments and Authorization Act of 1986 (SARA); signed into law October 17, 1986 defines emergency planning requirements and recognizes the need to establish and maintain contingency plans for responding to chemical accidents which can inflict health and environmental damage as well as cause disruption in the community. Our analysis indicates that Gas utilities will be directly impacted by 40CFR300, as the use and storage of the chemicals listed in the regulation are common at many sites.

Additionally, companies are under pressure to change the manner in which they operate as a result of deregulation, soft energy prices and various pending litigation issues. Competition from foreign sources, such as Canada, for supply of raw materials has also caused upheaval in this sector.

EXPLORATION, PRODUCTION, REFINING & STORAGE

The decline in U.S. crude oil production in 1986 turned out to be worse than expected, while imports have increased by 22%. The U.S. decrease would have been worse, had not Alaskan production risen by approximately 400,000 barrels per day.

Crude oil production declined about 3.4% for the year; offsetting all production gains made by oil operators from 1982 - 1985. Average daily production fell in 1986, from 9.18 million barrels per day to 8.35 million barrels per day by year end. This reflects a 7.7% decline from 1985.

World oil production rose by nearly 6%, the biggest annual rise in nearly ten years. However, production was still below the peak of 65.8 million barrels per day reached in 1979. Imports in the U.S. rose by 1.1 million barrels per day in 1986, the highest level since 1980. Total imports of crude and petroleum products averaging 6 million barrels per day compared to 4.9 million barrels per day in 1985 - an increase of 21.8%.

At the same time the demand for petroleum products has increased. Gasoline demand was up 2.6% and residual fuel deliveries rose for the first time in ten years. Deliveries of kerosene and jet fuel reached new annual highs also as a result of the low prices.

All this translates into sharply reduced drilling and well servicing activities for 1986. The number of wells drilled in 1986 is expected to have declined by about 40%; a decline of about 25,000 wells from 1985. The number of seismic crews and working service rigs declined at least 50% for the period. As a result, future supplies, for the next two to three years, are being determined today by the depressed exploration, drilling and development activities.

A comprehensive Department of Energy report provides support for various tax incentives and regulatory changes designed to enhance the U.S. Energy industry. The study highlights the need to harness nuclear power, coal and natural gas reserves to protect against what the report predicts will be a near doubling of oil imports by the mid-1990's. The report also recommends an accelerated filling of the Strategic Petroleum Reserve in order to safeguard U.S. security. It clearly indicates that the current trends in production and consumption pose "a clear risk" to long term national security interests. By the end of 1995, according to the report, Persian Gulf producers will provide as much as 65% of the free world's total oil consumption.

Since I wrote those paragraphs in 1986 many things have changed. The US has reduced its refining capacity by over 50%, its pipeline capacity by over 20%. We import

gasoline as well as crude oil. As I write this, Arizona is in the midst of a gas crisis due to a pipeline event that has curtailed much of the gasoline shipped to the State. In the mid-1990's then President Clinton created the President's Commission on Critical Infrastructure Protection. The Commission was chartered to conduct a comprehensive review and recommend a national policy for protecting critical infrastructures and assuring their continued operation. Under Executive Order 13010, certain national infrastructures have been identified and designated as so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

On October 15, 1997 the Commission presented its report on critical infrastructure vulnerabilities to President Clinton. The report of the PCCIP states in its introduction:

"The United States is in the midst of a tremendous cultural change - a change that affects every aspect of our lives. The cyber dimension promotes accelerating reliance on our infrastructures and offers access to them from all over the world, blurring traditional boundaries and jurisdictions. National defense is not just about government anymore, and economic security is not just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between the private sector and the federal government."

The Critical Infrastructures studied consist of:

- Electric Power Supplies
- Gas and Oil
- Telecommunications
- Banking and Finance
- Transportation
- Water Supply Systems
- Emergency Services
- Continuity of Government

The Commission divided its work into five "sectors" based on the common characteristics of the included industries. The sectors are:

- Information and Communications
- Banking and Finance
- Energy (Including Electrical Power, Oil and Gas)
- Physical Distribution
- Vital Human Services

The Commission characterized the sectors, studied their vulnerabilities and looked for solutions. They prepared comprehensive working papers for each of the five sectors providing specific recommendations. Other sections of the report contain information on issues that were not sector specific.

Included in the report is a paper on *Shared Infrastructures: Shared Threats*, that is an analysis of the vulnerabilities and threats facing the critical infrastructures. While the report recognized the significance of physical threats, it concluded that government and industry have a significant amount of experience in dealing with them. It was the cyber threat that received most of the report's attention. Cyber issues dominated the analysis because networked information systems present fundamentally new security challenges.

What the Commission found was:

“The development of the computer and its astonishingly rapid improvements have ushered in the Information Age that affects almost all aspects of American commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers.”

The Chinese have a saying, *“Opportunity is always present in the midst of crisis.”* The Commission's report shows that America's critical infrastructures underpin every aspect of our lives and that these infrastructures are extremely vulnerable to old and newly identified threats. We need to recognize that the rules have changed. No longer can we react in the way we have been taught to think. If we do, we will not be able to address the threat(s) effectively.

Your Quandary: What to do?

How prepared is your company to deal with the loss of critical infrastructures, vital to its survival? How vulnerable is your company to the disruption of infrastructures critical to daily operations? Does your current business continuity plan address these questions?

At the heart of the critical infrastructure vulnerability issue is an opportunity for industry and government to begin developing and implementing an “integrated” approach to business continuity planning. This approach consists of:

- Analysis of Vulnerabilities
- Planning & Preparedness
- Resource Development
- Information Management & Sharing

Although no two Business Continuity Programs are exactly alike, these are critical aspects that must be addressed in any Business Continuity Program.

Critical infrastructure operators lack key information

By Maureen Sirhal, [National Journal's Technology Daily](#)

The nation's operators of critical infrastructures—such as electrical power grids, telecommunication centers and water-filtration plants—lack key information necessary to repair their systems in case of an emergency, found a new report by the FBI's National Infrastructure Protection Center.

Ask yourself, "Why do we need a Continuity Program with an "integrated" approach?" Put simply, such a program allows you to provide for:

- Effective coordination of activities among the organizations having a response, management and recovery role;
- Early warning and clear instructions to all concerned if a disruptive event occurs;
- Continued assessment of actual and potential consequences of the event;
- Continuity of business operations during and immediately after the event.

Analysis of Vulnerabilities

How do you reduce the vulnerability posed by a disruptive event? You need a system that will advise you of current, future and potential vulnerabilities. Such a system will allow you to identify early indicators of vulnerability. In order to accomplish this task, a survey of all operations should be undertaken. The survey should include:

- General Administrative Information
- Management Awareness and Control Programs
- Identification of Threats, Hazards Vulnerabilities, Risks and Consequences
- Business Characterization

The ultimate benefits to be gained from this type of survey are in terms of identifying areas in need of attention, establishing a list of vulnerabilities, determining what commitments your organization is comfortable with and documenting current efforts. Once the survey program has been developed and implemented, it must be evaluated and kept up-to-date.

This can be accomplished by reviewing actual responses and by conducting a detailed audit of each element of the business.

The survey program is the initial step, toward reducing vulnerability. Next, you must organize the operation. The management chain is critical to this process. You must ensure that all levels of management become part of the program.

This can be achieved in several ways:

- Make a senior manager directly responsible to top management and the board of directors. The formal assignment of a senior manager to the position of "Business Continuity Programs, Director," or some other appropriate title, can accomplish the initial portion of this item.

- Set aside specific time for reports on business continuity issues. This can be accomplished by preparing an agenda for senior staff and board of director meetings that includes a discussion of business continuity as a mandatory item. You have to give it more than lip service though. Also, you must make the discussion substantive. Provide more than the dull and tiring statistics on reportable events, etc.

This can be very effective and it gets the message out to all personnel that your company is serious about business continuity as a way of doing business instead of an adjunct to the business you do.

- Make business continuity issues part of the strategic planning process. Government regulations are defining strategic implications for companies. Additionally, for publicly held companies, Security and Exchange Commission (SEC), in the section of the annual report entitled, "Management Analysis and Discussion" requires discussion of potential liabilities.

Another perspective on this issue really begets changing the "corporate culture," i.e., making business continuity a part of the way you do business.

- Communicate compliance through all levels of the organization through company policy and procedures. This can be accomplished through formal adoption of policy at the highest levels of the company.

This discussion is limited by the space available to a brief highlight of some approaches that can be undertaken. Each company will find its situation and circumstances to be unique to its corporate culture. Therefore, an in-depth analysis of your company's operating environment should be undertaken before developing a program or attempting to address the above items.

PLANNING & PREPAREDNESS

Planning and Preparedness used in the broadest context means any and all measures taken to prevent, prepare for, respond, mitigate and recover from a disruptive event. It's with this perspective that we begin to breakdown the aspect of Preparedness.

Preparedness consists of four critical aspects:

- Preparation and Prevention
- Detection and Classification
- Response and Mitigation
- Reentry and Recovery

Preparation and Prevention: Any set of activities that prevent a disruptive event from becoming a "crisis," reduce the chance of a disruptive event from occurring, or reduce the damaging effects of a disruptive event. Preparation and Prevention activities include, but are not limited to:

- Development and implementation of the Business Continuity Program
- Development and implementation of protocols to facilitate the Business Continuity Plan
- Development and implementation of training and simulations to validate the Business Continuity Program

Detection and Incident Classification: Actions taken to identify, assess and classify the severity of a disruptive event. Detection and Classification activities include, but are not limited to:

- Activation of Continuity Communication Systems
- Activation of the Business Continuity Plan
- Activation of the Response, Management and Recovery Organization

Response and Mitigation: Actions taken to save lives, prevent further damage and reduce the effects of the event. Response and Mitigation activities include, but are not limited to:

- Response, Management Recovery Organization operations
- Coordination of affiliated operations
- Continuity of business operations

Reentry and Recovery: Actions taken to return to a normal or an even safer situation following the event. Reentry and Recovery activities include, but are not limited to:

- Activation of the Reentry and Recovery Organization
- Coordination with Affiliated Recovery Organizations
- Activation of the Reentry and Recovery Plan

RESOURCE DEVELOPMENT

Development of your internal and external resources is the third component of the "integrated" approach. Training the Response, Management and Recovery Organization is one of the critical success factors that must be addressed if an adequate response is to be achieved. The development of the vulnerability analysis, preparation of the plan, involvement of all levels of management and establishing preparedness is only part of the overall process. To ensure an adequate response, a

trained organization is required. In addition to the development of resources through analysis, training and identification of external resources, a program to validate the proficiency of the organization is also needed. This can be accomplished by establishing a program that supplements the training with drills and exercises. The drill program can vary in degree of complexity.

INFORMATION MANAGEMENT & SHARING

The need to establish and maintain an ongoing dynamic Business Continuity Program is essential. The continuity process doesn't end just because you finished the plan, are in compliance, have involved management and trained the staff.

In order to facilitate planning requirements, a record of all initiatives should be retained. These records serve to document the accomplishments, requirements, commitments and reports relating to various program requirements. The identification of commitments in the areas of compliance, preparedness and training is vital. The establishment of a defined information management system structure will ensure that documentation will be available when needed.

Senior management must be kept well informed. Information is a corporate asset. Information is expensive. It must be shared and managed effectively. Information management is also critical during a crisis. The need for active systems to provide information on materials, personnel, capabilities and processes is essential.

Conclusion

Today, many people feel that the world has changed as a result of the events that took place on September 11, 2001; that we need to rethink our concepts of continuity and crisis management. An employer can be considered negligent if they do not take the reasonable steps to eliminate or diminish known or reasonably foreseeable risks. And following September 11, the range of known threats, hazards and risks is widely perceived to have broadened.

Market research indicates that only a small portion (5%) of businesses today have a viable plan, but virtually 100% now realize they are at risk. Seizing the initiative and getting involved in all phases of business continuity can mitigate or prevent major losses. Just being able to identify the legal pitfalls for the organization by conducting a business continuity audit can have positive results.

Blackout in foggy San Francisco

"A trolley cars sits on Market Street in San Francisco after a power failure stopped the cars mid-route. Trains, planes and cars were halted."

excerpted from
Mercury Center, 12/8/98

Today we cannot merely think about the plannable or plan for the unthinkable, but we must learn to think about the unplannable or plan on more headlines like the one above.

About the Author

Geary W. Sikich is the author of "*It Can't Happen Here: All Hazards Crisis Management Planning*" (Tulsa, Oklahoma: PennWell Books, 1993). His second book, "*Emergency Management Planning Handbook*" (New York: McGraw-Hill, 1995) is available in English and Spanish-language versions. His third book, "*Integrated Business Continuity: Maintaining Resilience in Uncertain Times*," (PennWell 2003) is available on www.Amazon.com. Sikich is the founder and a principal with Logical Management Systems, Corp. (www.logicalmanagement.com), based in Munster, IN. He has extensive experience in management consulting in a variety of fields. Sikich consults on a regular basis with companies worldwide on business-continuity and crisis management issues. He has a Bachelor of Science degree in criminology from Indiana State University and Master of Education in counseling and guidance from the University of Texas, El Paso.

References and Endnotes:

<http://blackout.gmu.edu/highlights/news.html>

Blythe, Bruce and Terri Butler Stivarius, Negligent Failure to Plan: The Next Liability Frontier?

Davis, Stanley M., Christopher Meyer, *Blur: The Speed of Change in the Connected Economy*. (1998).

National Infrastructure Protection Center, "National Structures" (www.nipcc.gov).

National Infrastructure Protection Center, "Shared Infrastructures Shared Threats" (www.nipcc.gov).

Perera, Valerie C. and Sikich, Geary W., "Controlling Crisis Will Determine Corporate Survival." *The Corporate Lawyer*, Illinois State Bar Association, November, 2002.

Sikich, Geary W., "Managing Crisis at the Speed of Light." Disaster Recovery Journal Conference (1999).

Sikich, Geary W., "Business Continuity & Crisis Management in the Internet/E-Business Era." Teltech (2000).

Sikich, Geary W., "What is there to know about a crisis." *John Liner Review*, Volume 14, No. 4 (2001)

Sikich, Geary W., "September 11 Aftermath: Seven Things Your Organization Can Do Now." *Disaster Recovery Journal*, Winter 2002, Volume 15, Number 1.

Sikich, Geary W., "The World We Live in: Are You Prepared for Disaster?" Crisis Communication Series, Placeware and ConferZone web-based conference series – Part I, January 24, 2002.

Sikich, Geary W., "September 11 Aftermath: Ten Things Your Organization Can Do Now." *John Liner Review*, Winter 2002, Volume 15, Number 4.

Sikich, Geary W., "Graceful Degradation and Agile Restoration Synopsis." *Disaster Resource Guide* (2002).

Sikich, Geary W., "Aftermath September 11th, Can Your Organization Afford to Wait." New York State Bar Association, Federal and Commercial Litigation, Spring Conference, May 2002.

Sikich, Geary W., "September 11th, Can Your Organization Afford to Wait?" GlobalContinuity.com, May 2002.

Sikich, Geary W., *Integrated Business Continuity: Maintaining Resilience in Times of Uncertainty*. PennWell Publishing, (2003).

Sirhal, Maureen [National Journal's Technology Daily](#) Critical infrastructure operators lack key information

United States Government Printing Office, *Report of the President's Commission on Critical Infrastructure Protection* (1997).

