



North American  
Electric  
Reliability  
Council

# EMERGING RISK TO OUR ELECTRIC INFRASTRUCTURE



## A BUSINESS CASE FOR ACTION

The wealth of our nation and the quality of life of its citizens are built upon critical infrastructures, such as telecommunications, electricity, transportation, and financial systems, mostly owned and operated by private industry, states, and municipalities. During decades of delivering services to their customers, in the face of the worst natural disasters, these critical infrastructures have emerged as robust, resilient, and reliable with generally well-established programs and plans to assure continued delivery of service.

The electric infrastructure in particular has been tested from its inception by hurricane, earthquake, landslides, firestorms, and flood. Because of that continuous testing and application of “lessons learned” over the years, an electric infrastructure has emerged in the United States that is the envy of many other countries.

### CONVERGENCE OF CHANGE

However, change is converging on the electric industry, at a pace not seen before in its history. The world has changed politically, economically, and technologically. The Cold War ended. It is no longer a bipolar political world, but a multipolar one, where the threat and growth of terrorism has replaced more traditional warfare.

Major advances of American industry into global markets fueled a focus on sustaining competitiveness and managing costs. Many companies, forced to manage thinning profit margins in a global market place, placed pressure on the suppliers of their basic commodities, such as electricity, to reduce prices. At the same time, the demand and use of electricity grew to support more sophisticated service delivery and manufacturing processes operating at higher speed and accuracy.

Information Technology (IT) is more accessible than ever to a wider population. It is now possible to perform more wide-ranging and sophisticated tasks with fewer skills and less technical knowledge than previously possible. The nation has truly moved into the Information Age.

### THE INFORMATION AGE

A comprehensive dependence on information systems has brought immense benefits to industry and government. In particular, the United States has built an information and communications infrastructure many times more extensive and capable than that of any other nation.

In 1997, this dependence was reflected in the following:

- The number of computers installed in the U.S. was estimated at more than 180 million. This number represented 42% of the world's computing power; five times that of Japan, and seven times that of Germany.<sup>1</sup>
- Ninety percent of large U.S. companies and 75% of small ones, built their daily business activities around local area networks.<sup>2</sup>
- The U.S. accounted for more than 200 million connect hours per day, more than 170 million telephone access lines, 14 million fax machines, and sent information through networks made up of about 2 billion miles of fiber optic and copper cable.<sup>3</sup>
- More electronic mail was sent than letters via the United States Postal Service, and U.S. consumers bought more computers than automobiles.<sup>4</sup>
- Although the Internet was global in reach, 60% of its assets were concentrated in the U.S.<sup>5</sup>
- More than 400,000 commercial and governmental web sites are now online. Purchases over the Internet are projected to reach \$117 billion by 2002.<sup>6</sup>

<sup>1</sup> Petska-Juliussen, Karen and Juliussen, Egil, *The 8<sup>th</sup> Annual Computer Industry Almanac*, (Austin, TX: The Reference Press, Inc., 1996), 483.

<sup>2</sup> IDC/LINK, "The U.S. Electronic Distribution Infrastructure: Size, Ownership, Geography, and Vulnerabilities", a report prepared for the President's Commission on Critical Infrastructure Protection (1997), 4.

<sup>3</sup> International Telecommunication Union, *World Telecommunication Development Report 1996/97: Trade in Telecommunications* (Geneva), A-43.

<sup>4</sup> Internet Council, "State of the Internet: USIC's Report on Use and Threats in 1999", <[http://www.usic.org/currentsite/usic\\_state\\_of\\_net99.htm](http://www.usic.org/currentsite/usic_state_of_net99.htm)>.

<sup>5</sup> Petska-Juliussen, Karen and Juliussen, Egil, *The 8<sup>th</sup> Annual Computer Industry Almanac*, (Austin, TX: The Reference Press, 1996), 553.

<sup>6</sup> Rutkowski, Tony, "Internet Hosts – Overall Trend", General Magic <<http://www.genmagic.com/Internet/Trens/slide-4.html>>.

Far more than any other nation, information technology has reshaped U.S. commercial, governmental, and personal activities—how people work and live. This country has led the world into the Information Age. In doing so, U.S. economic competitiveness, governmental efficiency, and personal safety have become uniquely dependent upon information technology. It is the common thread, along with energy, especially electricity, which runs through all our critical infrastructures.

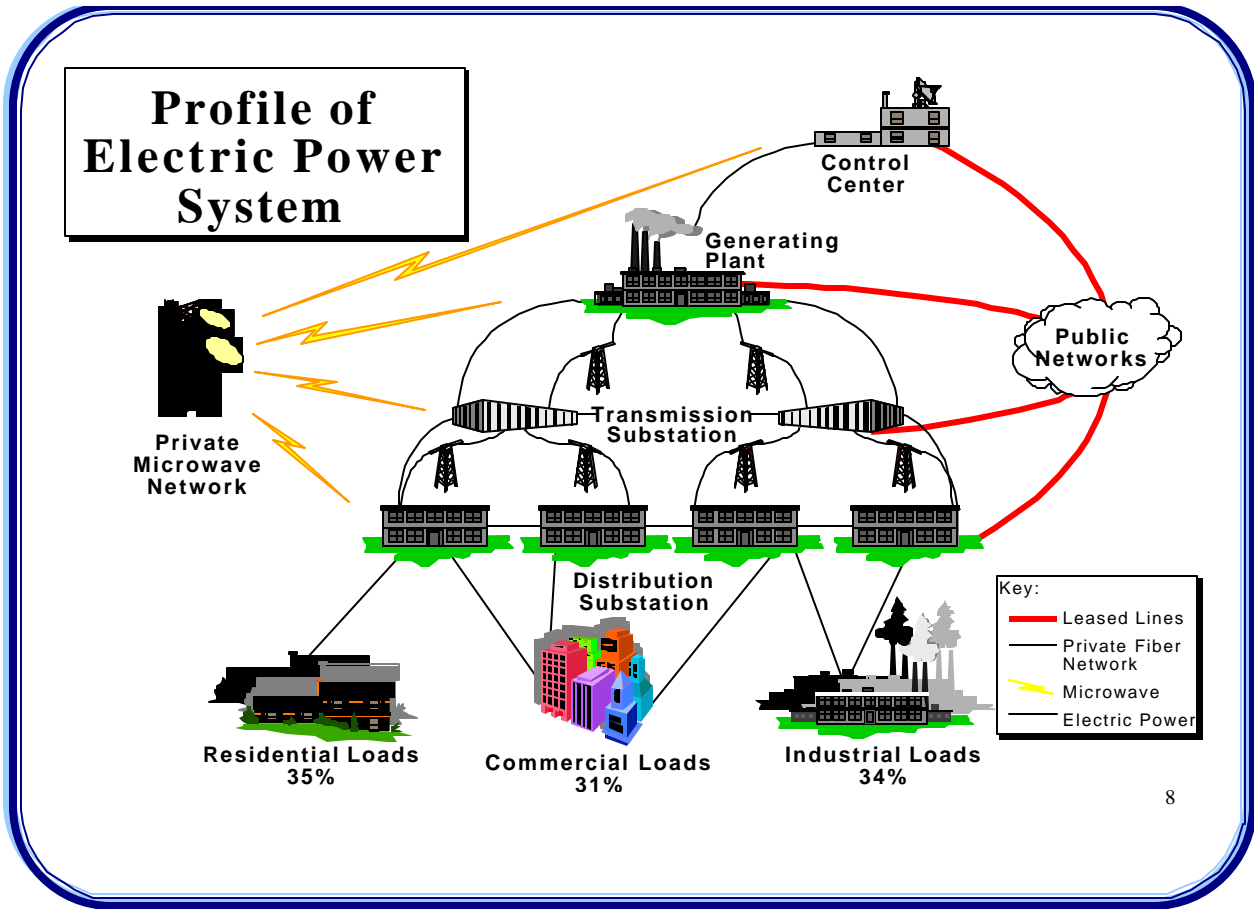


## THE ELECTRIC BUSINESS IN THE INFORMATION AGE

Electric industry restructuring and the desire to compete efficiently and effectively in a deregulated market place have driven and will continue to drive widespread, and heretofore unimagined, application of information technology to electric infrastructure operations, new types of businesses, and competition in this industry. In many instances, having access to information can be a determinant in whether an organization can successfully participate in new markets created by the electric industry restructuring.

### What Is Changing?

Manned Facilities Operations	➔	Unmanned Facilities
Remote Monitoring	➔	Automated Monitoring/Control
Local Markets	➔	Open, Regional/National Markets
Local Customer Services	➔	Consolidated Call Centers
Customer Billing Information	➔	Customer Services Information
Heterogeneous Technology	➔	Standardized/Homogeneous
Traditional Electric Services	➔	On-line Businesses/E-Commerce



8

### Operational Dependencies on Information Technology

There is already a dependency on information technology in the core operations of our electric supply and delivery systems and that dependency is forecast to grow.

“[M]ost of the 3,200 electric power utilities depend upon networks to manage and control their delivery of power. The electric power generation transmission and distribution systems are controlled in part by a multitude of Supervisory Control and Data Acquisition (SCADA) systems that monitor, report, and partially control and regulate the flow of energy. These systems...are linked to centralized centers and corporate management systems, many of which are also connected to the outside...”<sup>7</sup>

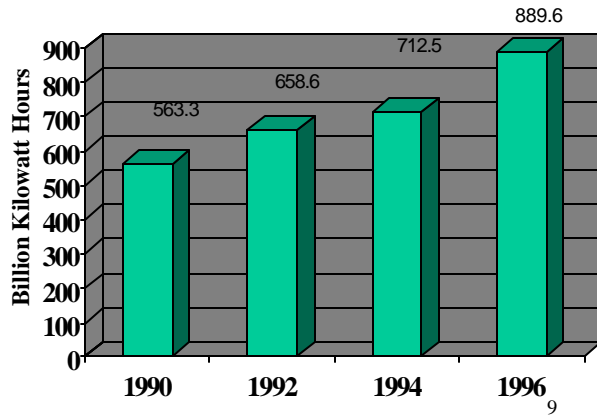
### Emerging Industry Markets and Market Restructuring

Deregulation is mandating participation in open markets. In the electric industry, the volume of kilowatt-hours in wholesale transactions grew dramatically from 1990 to 1996. These transactions are often part of emerging state or regional markets (such as the California electricity market) that include business conducted over the Internet, virtual private networks, and limited dedicated networks. Functions such as pricing, scheduling, bidding, metering, capacity limit notification, utilization and allocation, and settlements, as well as control of generation, transmission, and demand are being carried out over these networks. Energy wholesalers rely on information and access to markets to conduct various forms of arbitrage and to maximize financial gain. The electricity supply and delivery business is becoming electronic commerce.

<sup>7</sup> President’s Commission on Critical Infrastructure Protection, “A Case for Action” (1997), 7.

<sup>8</sup> President’s Commission on Critical Infrastructure Protection, “Critical Foundations: Protecting America’s Infrastructures” (October, 1997), A-33.

## Electric Wholesale Trade Volume



The development of generation and transmission capacity trading follows the model of the financial industry's commodity markets. The industries are comparable in their dependence on the reliability, availability, and integrity of their information systems. Daily, millions of dollars worth of electricity can be traded over networks, just as commodities such as wheat and corn are traded. The information technology dependency of the financial infrastructure of today and as it evolves may be an indication or even a model of how this part of the electric industry will evolve.

Failure to maintain confidentiality, integrity, or availability not only compromises a business strategy, but threatens the confidence of those participating in markets and can have disastrous effects by increasing market uncertainties and potentially inspiring government intervention or regulation.

"The movement of funds within the U.S. totally relies on computer-controlled systems and the public telecommunications networks that link them together. Each year, trillions of dollars of funds are transmitted over a small number of interdependent networks. These four networks — FedWire, the Clearing House Interbank Payment System (CHIPS), the Society for Worldwide Interbank Financial Telecommunications (SWIFT), and the Automated Clearing House (ACH)—

<sup>9</sup> Graph developed from data listed in U.S. Energy Information Administration, "Electric Trade in the United States 1996, Executive Summary" (1997), 4  
<[http://www.eia.doe.gov/cneaf/electricity/etus/exec\\_sum.html](http://www.eia.doe.gov/cneaf/electricity/etus/exec_sum.html)>.

transmit virtually all domestic electronic transactions, and many overseas as well."<sup>10</sup>

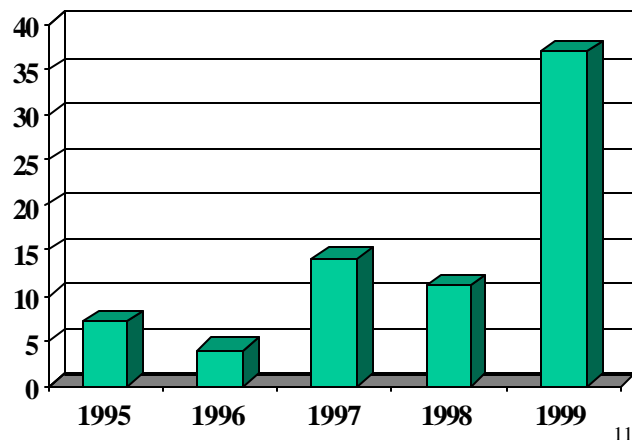
## New Requirements for Business Competitiveness

Many electric utilities have invested in highly sophisticated, information-intensive, consolidated, customer call centers and dispatch centers. These investments are intended to ensure responsiveness and assure confidence to the communities and customers that an electric utility serves. Disruption of the underlying computer and telecommunications systems that support these processes can disrupt a utility's service capability and rupture carefully nurtured customer relationships and public confidence. Consequences include regulatory scrutiny, financial penalties, and public embarrassment that can lead to loss of customer loyalty.

## Corporate Restructuring

Mergers, acquisitions, and partnerships (and their dissolution) have become much more common as organizations seek to better align themselves for future markets, capitalize on their strengths and complement their present business opportunities, and options. Many have engaged in offshore acquisitions or bids into foreign markets. New and evolving partners and subsidiaries may require new links, integration, or even compartmentation of existing networks and other information assets.

## Investor-Owned Utilities

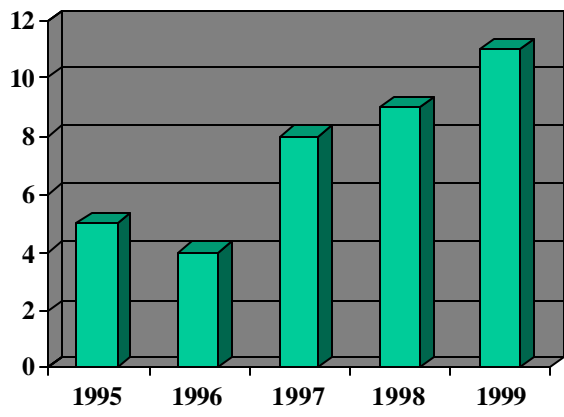


<sup>10</sup> President's Commission on Critical Infrastructure Protection, "A Case for Action" (1997), 7.

<sup>11</sup> Graph developed from data listed in American Public Power Association, "Investor-Owned Utilities: Mergers

One senior electric utility executive reported that his company dramatically increased its attention to the security of its information networks and assets when it began to engage in international energy business operations. For this corporation, acquiring foreign companies, some of which, in turn, had operations and holdings in countries known to be unfriendly to the United States, made tightening of information security a business necessity.

### International Mergers and Acquisitions U.S. Investor Utilities



12

## THREATS

Consequently, the impact of disruptions to information systems or corruption of information produced or transported by electronic systems supporting business activity and systems operations will become far greater in magnitude than at any other time in the history of the electric industry. The benefits of using information technology come with risks that have not previously been well recognized. Along with the benefits of information technology is the dramatic expansion of accessibility to tools and techniques that can be used to do harm by electronic means. Our national goal of necessity is to recognize and manage these risks when these tools are misused.

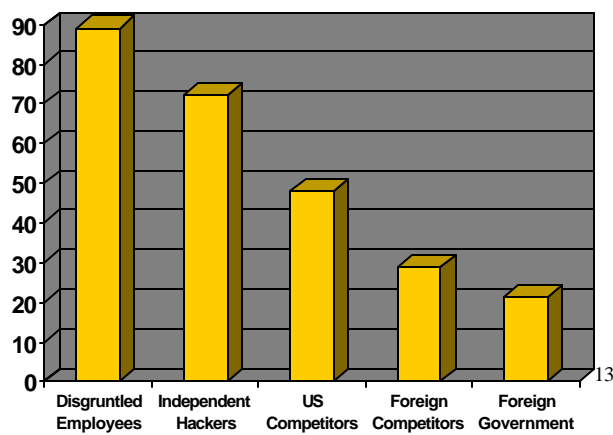
Tools that can be used to disrupt or deny service or to corrupt or destroy electronic information are more accessible on the

Internet now than ever before. Hacking activity in our current culture is more likely to be celebrated in books and movies than to be condemned as a form of trespassing or intrusion on privacy. The technology of hacking has advanced to the point that many tools that required in-depth knowledge a few years ago have become highly automated and user-friendly. Hacking tools and techniques have even been posted on electronic bulletin boards on the Internet, available to anyone with a computer, a modem, and Internet service. Very sophisticated tools are packaged with easy-to-follow scripts, a “threat-in-a-box.” Moreover, perpetrators cannot be easily or quickly identified or categorized, adversely affecting the level and speed of response and remediation.

Those who can use these tools and techniques range from the recreational hacker — who thrives on the thrill and challenge of breaking into another’s computer — to the national security threat of information warriors intent on achieving strategic advantage.

Common to all threats is the insider. Millions of dollars could be spent on technology to protect an infrastructure, but well-placed insiders or disgruntled employees can bypass technological safeguards. Consequently, the insider represents a special challenge.

### Likely Sources of Attack



13

and Major Acquisitions” (December, 1999)  
<<http://www.appanet.org/ppeui/mergers.html>>.  
<sup>12</sup> Ibid.

<sup>13</sup> CSI/FBI 1998 Computer Crime and Security Survey

# Information Age Threat Spectrum

National Security Threats	<b>Info Warrior</b>	<b>INFORMATION WARDS</b>	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	<b>National Intelligence</b>		Information for Political, Military, Economic Advantage
Shared Threats	<b>Terrorist</b>		Visibility, Publicity, Chaos, Political Change
	<b>Industrial Espionage</b>		Competitive Advantage Intimidation
	<b>Organized Crime</b>		Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	<b>Institutional Hacker</b>		Monetary Gain Thrill, Challenge, Prestige <sup>14</sup>
	<b>Recreational Hacker</b>		Thrill, Challenge

## THE EMERGENCE OF SUBSTANTIVE NEW BUSINESS RISK

The application of information technology to electricity supply or delivery organizations brings substantial benefits. However, as these organizations increase reliance on information systems, the disruption or corruption of those systems now can become substantive business issues that chief executive officers (CEO) and boards of directors traditionally worry about:

- Business operations survivability.
- Customer relationships and new business competitiveness.
- Public and investor confidence.

Without appropriate attention to the security of these systems and the information they support, the risk profiles of electricity supply and delivery organizations can change dramatically. And these risks can easily remain unidentified, as organizational dependence on new technology grows.

## Business Operations Survivability

As information systems are more highly integrated into the core service or product delivery process of an electricity supply or delivery organization, a disruption of the information systems can put the entire business' survival at risk. In April 1998, a disgruntled employee unleashed a logic bomb that destroyed a New Jersey firm's files critical to the operations of its production lines. It not only disabled the operations of the company, it corrupted the firm's backup files, precluding any recovery or reconstitution. The firm lost its market leadership and was eventually forced to lay off a large portion of its production line employees.<sup>15, 16</sup>

<sup>14</sup> President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures", (October, 1997), 20.

<sup>15</sup> \_\_\_\_\_, "Companies grapple with limiting employee abuse", *USA Today*, April 28, 1998, 1.

<sup>16</sup> Gaudin, Sharon, "The Omega Files", *Network World*, June 26, 2000

<<http://www.nwfusion.com/research/2000/0626feat.html>>.

## Customer Relationships and New Business Opportunities

Because Americans have more confidence in their infrastructure than any other country in the world, there is lower tolerance for disruption. Expectations for electric service performance are elevated to the point that many take high levels of service performance for granted. Much of the growth of e-commerce is projected to come from migration by traditional companies, including electricity service providers, offering new service features and products and doing business differently to stay competitive. Unreliable or inefficient service will drive a customer to a competitor where a competitive marketplace exists, or in a regulated marketplace to file a complaint with a regulator. Such actions usually result in a financial penalty for the organization involved. Bad customer relationships inevitably increase costs of operations, and in the case of shareholder-owned utilities, lower profits.

Electric utilities, just as many other industries, maintain a great deal of information on customers and employees to provide better services. The general public now has a growing awareness of the implication of this information on privacy. As evidenced in the growing debate on privacy on the Internet, customers and employees of organizations have increasingly firm expectations on how information about them is managed and protected. An implicit assumption is that these organizations will protect and assure the confidentiality of the information they hold. Failure to meet these expectations also can rupture customer relationships and may cause the utility to incur the risk of liability for not adequately protecting sensitive customer or employee information if an information system is breached or corrupted. The privacy issue is likely to become for the first decade of the new millennium what environmental protection was as a business issue for the 1980s. The latter literally reshaped industries and business practices for decades and will continue to do so for decades to come.

## Public and Investor Confidence

Investor confidence, as reflected in share price and bond rating, depends on assurance that an organization is being managed prudently and with due care. Disruption of information systems on which the efficiency and quality of service delivery depend directly affects the perception of an organization's investors and its customers of how well it is managed. Dependence of business operations on information systems inevitably causes the standard of prudent management and due diligence to include the security of critical information systems.

Auditing teams are becoming more savvy about the role of information systems in business operations and more acutely aware of the need for more security and prudent management control of these systems. Fixing program code for Year 2000 (Y2k) and its subsequent accountability illustrates this evolution. Failure or inadequate effort to address the issue has been judged to make an organization substantially riskier. This belief was reflected in the Security and Exchange Commission's requirement for an organization to report on the status of its Y2k conversion efforts for critical business operations to its shareholders.<sup>17</sup>

In mid-1998, a European-based hacker invaded one Internet service provider's network in the U.S. and disabled eight out of ten servers. Due to the service provider's lack of appropriate security controls, the invader also downloaded the personal and financial information for each customer amounting to about 11,000 credit card account numbers. He proceeded to threaten the service provider with distribution of the customers' credit card information and future network disruption, unless the service provider submitted to his blackmail demand.<sup>18</sup> Subsequently, the hacker was captured and prosecuted, but the implications for disrupting public and investor confidence in the organization were profound.

---

<sup>17</sup> U.S. Securities and Exchange Commission, 17 CFR Part 240 (August 12, 1998).

<sup>18</sup> Closed Cases File, 1996-2000, United States Secret Service.

## WHAT CAN A CEO DO?

The Year 2000 program conversion provided some valuable “lessons learned”. It also built a needed foundation for critical infrastructure protection and management of information security. The initial investment in this foundation has been made. Any additional effort will likely be incremental and reinforce what has already begun. Specifically, a CEO can focus attention through the following:

- Understand the level of dependency of core service and product delivery processes on information technology within the organization, and determine the possible consequences to its customers, the communities in which it operates, and the expectations of its shareholders and other stakeholders, if those information systems were to be disrupted.
- Ask about the mitigation and contingency plans put in place to manage these risks. Know what business risks the organization has accepted in the way it manages its information technology systems. Ask for and review information security benchmarks of other similar organizations in the electric industry, and other industries, and compare the level of risk the organization is incurring.
- Review the organization’s electronic interfaces with third parties, including other electricity supply and delivery system entities, and determine which risks need to be managed. This activity is to protect not only the organization and its public image, but to maintain public confidence in both the organization and the electric industry as a whole.
- Encourage the integration of information security into the overall policies and procedures for managing and protecting organizational assets.
- Establish an organizational policy to encourage the sharing of experience and practices within and between industries to maintain customer and public confidence, as well as help to reduce the costs associated with the security effort.
- Invest authority in a leader for the organization’s security efforts, giving that person direct reporting responsibility and accountability for aggressively establishing, overseeing, and implementing security policies. Ask for reports regarding the inherent risks of new enterprises and investments.

---

Note: This document was developed under the direction and with the participation of electric industry representatives of the Critical Infrastructure Protection Forum of the North American Electric Reliability Council (NERC), supported by staff from the Critical Infrastructure Assurance Office, U. S. Department of Commerce and staff from the U. S. Department of Energy.