



North American
Electric
Reliability
Council

EMERGING BUSINESS RISKS TO THE ELECTRIC POWER INFRASTRUCTURE



A CASE FOR CHIEF EXECUTIVE OFFICER ACTION

The introduction of competition in the wholesale and retail electricity markets, coupled with an increased demand for electricity, has led to electric utilities' to rely more on information technologies (IT). In addition to ensuring a utility's ability to generate, transmit, and distribute electricity to its customers, information systems are increasingly effective vehicles for exploring new markets; executing strategic business decisions; achieving internal operating efficiencies; and tracking the people, products, and services on which a firm's success depends.

The reliability and security of these systems are critical to electric utility survival. Chief Executive Officers (CEO), boards of directors, and other senior-level executives responsible for overseeing the business operations of electric utilities need to understand the risks posed by this increased reliance on information technology. In addition, they also must manage and, where possible, mitigate these risks to their organizations and the industry through continuous communication and leadership. This management and mitigation responsibility requires close coordination with finance, customer services,

operations, and other senior-level officials in their firms, and coordination within the industry, to address a widening range of competitive and operational vulnerabilities, including information systems, security, and other cyber-related threats. CEOs, boards of directors, and other senior-level officials are vested with authority and have an obligation to manage risks and liabilities through due diligence and prudent management. As such, it is important that they recognize that IT is not only an enabler of competitive advantage, customer service, and investor confidence, but also a source of vulnerability or business risk.

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 |

Business Operational Survivability

Significant security risks stem from the interconnectedness of the communications networks that underpin utility generation, transmission, and distribution systems. Most of the approximately 3,200 electric utilities serving North America depend on IT networks, such as supervisory control and data acquisition (SCADA) systems, to manage generation, transmission, and distribution systems. These systems are linked to control networks and corporate management systems, many of which also are connected to systems outside the utility. In addition, the electric utilities participate in open markets, vastly expanding the size and complexity of the electric industry's IT infrastructure. Simply put, the electric industry, conducting arbitrage over real and virtual assets, relies on a nationwide network information systems to do business. These systems include Internet-based applications such as the Open Access Same-time Information System (OASIS), which facilitates the exchange of transmission availability information and on-line price negotiations.

Like commodities trading, the buying and selling of electricity would be virtually impossible without the efficiencies of IT. The array of mainframes, desktop clients, operating systems, and network protocols used by power marketers add to the complexity of the electric power industry's IT infrastructure. Consequently, as the newly competitive energy market matures, generation, transmission, and distribution systems will become increasingly subject to both IT- and market-related forces. This maturation will present new challenges to ensuring the reliability of the electricity delivery systems in North America.

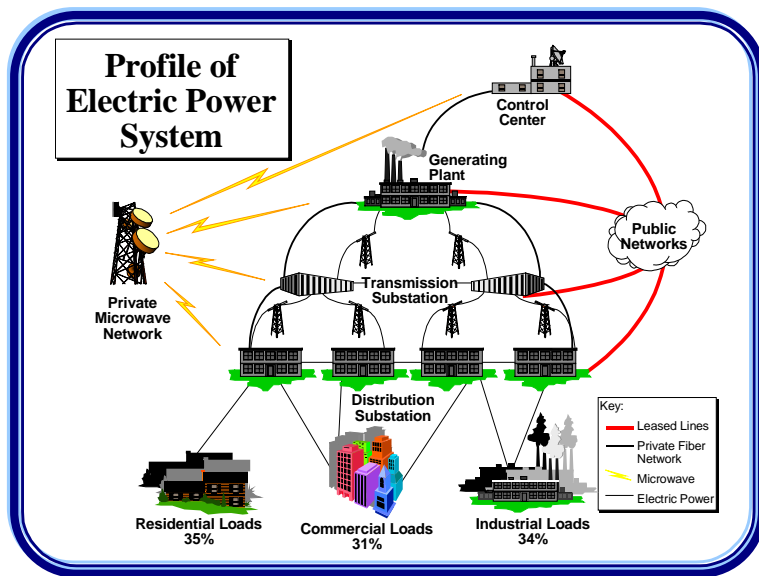
Business Competitiveness

Reliability and security have also come under pressure from financial interests. A utility's previous "obligation to serve" to some degree is being pressured by industry stakeholders. Many expect that a competitive market place will shift reliability from a mandated "obligation" to being a competitive feature of service in order to be in the electric business.¹ Many also see that the electric industry will become a highly competitive commodities business that is largely customer-driven and dependent on technological and operational efficiency. The Power Company of America expects annual trading volume of electricity to reach an unprecedented high of \$2.5 trillion by the year 2003.²

If this projection holds true, electricity will become the United States' most heavily traded commodity. Consequently, power marketers and utilities are competing aggressively for a substantial share of the market. Like the financial industry's commodities market, which may be a harbinger of how the electricity market will evolve, electricity worth billions of dollars will be traded over computer-controlled networks and telecommunications systems. Failure to maintain the confidentiality, integrity, and availability of these transactions could not only compromise an electric utility's business strategy but, if widespread, could also threaten the confidence of those participating in the electricity markets.

¹ John D. Mountford and Ricardo R. Austria, "Keeping the Lights On!" *IEEE Spectrum* (June 1999): 34.

² Tami Cissna, "Wholesale Electric Power Sales Are Increasing—Is Anyone Profiting?" *Electric Light & Power* (August 1998): 42.



Customer Relationships

Competition also promotes an increased focus on customer service. Today's electricity customers are no longer "rate payers." Rather, they are free to choose their electricity service provider.

To enhance customer service and differentiate their firms, many electric utilities are investing in highly sophisticated call centers and service dispatch operations. Customers are being billed, paying bills, and examining their account histories electronically. As a result, corporate databases store vast amounts of customer information, including credit card numbers, bill paying histories, peak-usage times, consumption rates, and service records. Corruption of these systems, coupled with disruption of the underlying computer and telecommunications networks that support them, could not only disrupt a utility's service capability, but also rupture the very relationships the systems are designed to preserve. By corrupting customer service databases, a sophisticated hacker could not only hamper the timeliness and accuracy of customer billing processes, but also obtain sensitive customer information. In addition, the increasing use of links between control systems

and corporate information systems offer intruders multiple points through which to gain access to utility networks. A knowledgeable intruder, aided by publicly available "hacker" tools, could issue false commands to a utility's energy control systems causing system operators to receive incorrect system status information or causing disturbances on the electricity supply and delivery

systems.³ Consequences of such events could include increased regulatory scrutiny, financial penalties, and loss of public and customer confidence.

Public and Investor Confidence

Because many investors are unsure as to which electric utilities will compete successfully in the newly deregulated power market, increased business risks and greater stock price volatility will likely abound. Valuations will not only depend on share price and bond ratings, but will also reflect investor perceptions regarding how well an electric utility is managed, including the utility's ability to respond to competitive pressures and other market challenges.

In the Information Age, a utility's ability to compete and deliver services and products "faster, better, cheaper" relies on underlying information systems and their proper management. Failure to secure and effectively manage critical information systems can lead to disruption of business operations and customer services and undermine public

³ National Security Telecommunications Advisory Committee, Information Assurance Task Force, *Electric Power Information Assurance Risk Assessment Report* (March 1997).

and investor confidence. Because such occurrences not only affect revenue, but inevitably reduce public and investor confidence in business decisions and the management of the utility,

CEOs, boards of directors, and other senior-level executives will need to pay special attention to the management and security of IT systems.

WHAT CAN A CEO DO?

The Year 2000 program conversion provided some valuable lessons learned. Specifically, CEOs, boards of directors, and other senior-level officials can—

- Understand the level of dependency of core service and product delivery processes on IT and the possible consequences to business operations if they were to be disrupted — in other words, understand their organization’s evolving business risk profile with its dependency on information systems
- Request and review information security benchmarks from other entities in the electric and other industries to ascertain the level of risk to which their organization is exposed. Require evaluation of mitigation and contingency plans designed to manage risks and their possible consequences to customers, the communities in which the organization operates, and the expectations of shareholders and other stakeholders
- Review their organization’s electronic interfaces with third parties, including the electric industry’s national grid. Determine what risks need to be managed to protect their organization and its public image and to maintain public confidence in 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
- Encourage, as organizational policy, the sharing of experiences and practices within and among industries to maintain customer and public confidence, as well as to help reduce costs associated with security efforts
- Invest authority in a leader for their organization’s security efforts, giving that person direct reporting responsibility and accountability for aggressively establishing, overseeing and implementing security policies.

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.