



North American
Electric
Reliability
Council

MANAGING THE BUSINESS RISKS OF INFORMATION TECHNOLOGY DEPENDENCIES:

~~~~~

## WHAT UTILITY OPERATIONS EXECUTIVES CAN DO

The U.S. electric industry is transitioning from one dominated by large vertically integrated utilities to one populated by competitive generation entities and regulated transmission and distribution entities. These changes are rendering the electricity supply and delivery infrastructure increasingly complex. In response to these changes, electric utilities are intensifying their already heavy reliance on information technology (IT) systems to manage the intricacies of (1) electricity transmission and distribution systems, (2) trading operations, and (3) customer services. Growing dependence on IT for maintaining business operations means that utility operations executives need to ensure that critical information systems are secure, reliable, and available. Otherwise, IT systems could become a weak link in the reliability of utility business operations.

### THE EMERGING BUSINESS RISKS OF IT DEPENDENCIES ~

Information technology systems are essential tools for managing electric utility operations. These systems include the control systems and communications networks that support electricity transmission and distribution systems, trading operations, and customer services. However, these increasingly complex and critical IT systems are vulnerable to failure or intentional disruption, exposing utilities to greater threats and business risks than ever before. Information technology systems should be protected, but in a competitive business environment electric utilities may feel pressure to keep costs low by minimizing investments in areas such as information systems security. Despite these budget pressures, operations managers—persons responsible for maintaining the functionality and reliability of electric utility systems—need to understand the risks posed by increased reliance on IT, communicate these risks to other senior utility executives, and allocate appropriate resources to manage and, where possible, mitigate such risks.

### What Is Changing?

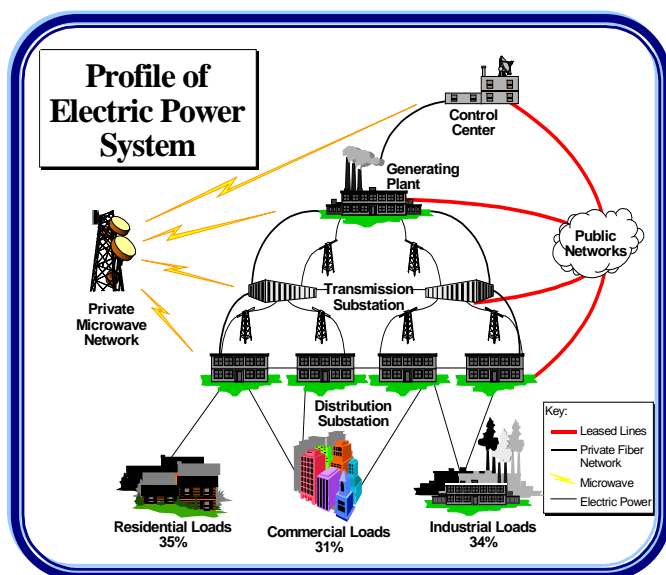
- Manned Facilities Operations → Unmanned Facilities
- Remote Monitoring → Automated Monitoring/Control
- Local Markets → Open, Regional/National Markets
- Local Customer Services → Consolidated Call Centers
- Customer Billing Information → Customer Services Information
- Heterogeneous Technology → Standardized/Homogeneous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

### ELECTRICITY TRANSMISSION AND DISTRIBUTION SYSTEMS ~

Electricity supply and delivery systems are controlled by energy management systems (EMS), which generally consist of elements such as: a supervisory control and data acquisition (SCADA) system; energy management applications and databases; and a user interface (UI) system. An intrusion into an electric utility's control center could have far reaching effects. For example, a knowledgeable intruder 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. Although utilities are well prepared to deal with a few isolated disruptions, a coordinated attempt to penetrate several critical information systems simultaneously may overwhelm a utility's resources and result in severe outages.<sup>1</sup>

Electric utility substation operations are also susceptible to electronic intrusion. As deregulation and competition drive utilities to reduce costs and provide a higher quality of service, many utilities are automating substation operations – employing intelligent electronic devices – so equipment can be remotely accessed. A knowledgeable intruder could issue spurious commands to shut down or even possibly damage equipment.<sup>2</sup>



Because penetration of utility transmission and distribution IT systems requires technical sophistication and specific knowledge of utility applications and procedures, the pool of potential intruders is relatively limited. However, recent trends in the electric utility industry could make critical information about electric systems available to a larger number of individuals, thus vastly increasing

the probability of intrusion. These trends include a shift from proprietary mainframe control systems to open systems and standard protocols, as well as a migration to public communications as a means to interconnect utility business facilities and utility control centers. For example, the Utility Communications Architecture (UCA) and Database Access Integration Service (DAIS) have already become widely used industry communications and database protocols for information exchange over electric utilities' IT networks.<sup>3</sup> In addition, many utility systems rely on client-server-based applications using transmission control protocol/Internet protocol (TCP/IP) and other publicly used protocols.

Information security risks are exacerbated by utilities increasingly outsourcing to independent contractors and other vendors the customizing and maintenance of software and other products supporting their distribution IT systems, thereby giving legitimate IT system access to larger numbers of people. Information technology systems are particularly vulnerable to attack by such insiders. In 1998, for example, a New Jersey engineering firm filed for bankruptcy after a disgruntled employee who had legitimate system access unleashed malicious computer code that destroyed the primary and backup computer files critical to operating the firm's production lines. This episode illustrates the importance of basic management controls to mitigate risks from legitimate access to systems.

**TRADING OPERATIONS** ~ The advent of wholesale electricity generation and open access transmission markets fueled the development of generation and transmission capacity trading, which functions like commodity markets. This trading fosters a greater dependence on the availability, reliability, and integrity of information systems. Power marketers, manipulating physical and virtual assets and conducting arbitrage to maximize financial gain, rely on Inter-

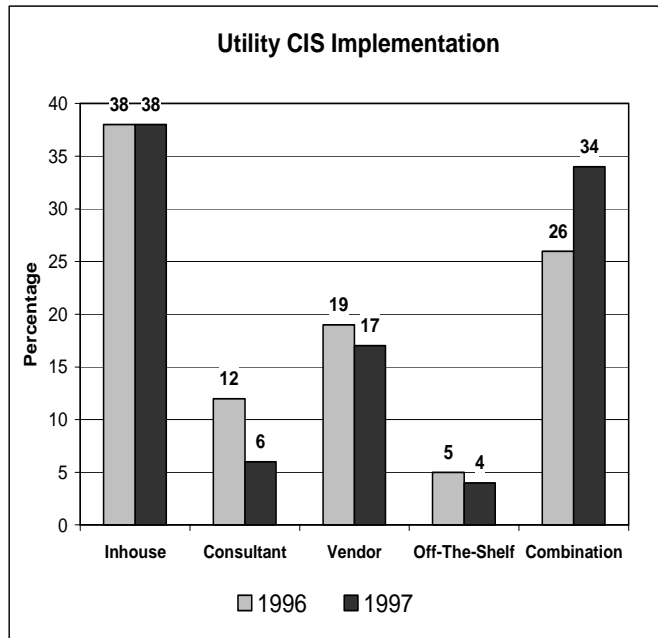
<sup>1</sup> David Jones and Ronald Skelton, "The Next Generation Threat to Grid Reliability – Data Security," *IEEE Spectrum* (June 1999): 46–48.

<sup>2</sup> National Security Telecommunications Advisory Committee, Information Assurance Task Force, *Electric Power Risk Assessment Report* (March 1997).

<sup>3</sup> David Jones and Ronald Skelton, "The Next Generation Threat to Grid Reliability – Data Security," *IEEE Spectrum* (June 1999): 46–48.

net-based applications, such as the Open Access Same-time Information System (OASIS), for access to information and markets.

**Figure 1**



Source: Steven J. Maslak, "Replacing a Customer Information System." *Public Power* (September-October 1999): 45.

Annual trading volume of electricity could reach an unprecedented high of \$2.5 trillion by the year 2003, which would make electricity the most heavily traded commodity in the United States.<sup>4</sup> 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 trading market will evolve, electricity worth billions of dollars will be traded over computer-controlled networks and supporting public telecommunications systems. Failure to maintain the confidentiality, integrity, and availability of these transactions could not only compromise a utility's business strategy but, if widespread, could also threaten the confidence of those participating in the power markets.

### CUSTOMER SERVICE OPERATIONS ~

Deregulation and competition in electricity markets have caused utilities to expand their use of IT to manage increasingly complex

business relationships and to perform such functions as pricing, scheduling, bidding, metering, capacity limit notification, utilization and allocation, and settlements. Customers are receiving bills, paying bills, and examining their account histories electronically. Utility databases store vast amounts of customer information, including credit card numbers, bill paying histories, peak-usage times, rates of electricity usage, and service records. A variety of packaged, client-server-based customer information systems (CIS) are available, which can be installed at a fraction of the cost of custom-designed solutions.<sup>5</sup> As with other IT systems, however, such commercial off-the-shelf solutions may be more susceptible to intrusion than custom systems because critical information about these systems is available to a larger number of individuals. Figure 1 illustrates that although use of in-house CIS remains common, a growing percentage of utilities are implementing systems with a combination of consultants, vendors, and off-the-shelf components.

Although disruption of customer service systems might not directly impact the physical delivery of electricity, it could rupture carefully nurtured customer relationships and public confidence. Denial of service attacks, similar to the well-publicized incidents against Internet businesses,<sup>6</sup> also could be directed against utility customer service websites or call centers. If customer service operations were adversely affected for a substantial period of time, the utility could lose business as unsatisfied customers switch to competitors. In addition, by corrupting customer service databases, a sophisticated hacker could hamper the timeliness and accuracy of customer billing processes or obtain sensitive customer information. Such failures to deliver services or protect customer privacy could result in increased regulatory scrutiny, financial penalties, lawsuits, and public embarrassment.

<sup>5</sup> Steven J. Maslak, "Replacing a Customer Information System." *Public Power* (September-October 1999): 42.

<sup>6</sup> Matt Richtel, with Sara Robinson, "Several Web Sites Attacked Following Assault on Yahoo." *New York Times* (February 9, 2000).

<sup>4</sup> Tami Cissna, "Wholesale Electric Power Sales Are Increasing—Is Anyone Profiting?" *Electric Light & Power* (August 1998): 42.

Electronic intruders can attempt to access utility control systems through several interfaces, including links to utility business information systems, links to other utilities, power pools or control areas, links to vendor support services, and remote maintenance and administration ports. Many utilities protect their systems with firewalls and dial-back modems, but these measures are not

sufficient to guard against increasingly sophisticated hackers. The technology of hacking has advanced to the point that many tools that required in-depth knowledge just a few years ago are now highly automated, user-friendly, and readily available on the Internet. As a result, many security measures that were effective a few years ago may now offer limited protection of IT systems.

## WHAT CAN AN ELECTRIC UTILITY DO?

As executives responsible for maintenance of electricity transmission and distribution systems, trading operations, and customer services systems, utility operations managers have a responsibility to plan for these new challenges to critical IT systems that support their operations. Specifically, utility operations executives can:

- Cultivate and maintain close relationships with the Chief Information Officer and senior human resources, physical security, telecommunications, and other relevant managers to develop and implement comprehensive utility-wide standards and requirements regarding IT security measures
- Work with the company's IT organization to periodically conduct intensive security evaluations and to identify mission critical systems within utility information networks
- Evaluate and deploy relevant security practices and technologies, such as penetration testing and intrusion detection systems
- Raise internal awareness of IT security issues among all employees through ongoing security awareness programs and wide distribution of policies and procedures
- Ensure that other senior managers, including the Chief Executive Officer and Chief Financial Officer, are aware of the risks to information systems, the potential costs of electronic intrusions, and the importance of adequate investment in information system security
- Participate in industry-wide efforts to share security-related experiences and practices and information about threats to, and vulnerabilities of, information systems. Such cooperation will help maintain customer and public confidence in a utility's electric and business operations and reduce overall security-related costs.

---

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.