



North American
Electric
Reliability
Council

MANAGING THE BUSINESS RISKS OF INFORMATION TECHNOLOGY DEPENDENCIES

~~~~~

## WHAT CAN AN ELECTRIC UTILITY'S CHIEF INFORMATION OFFICER Do?

---

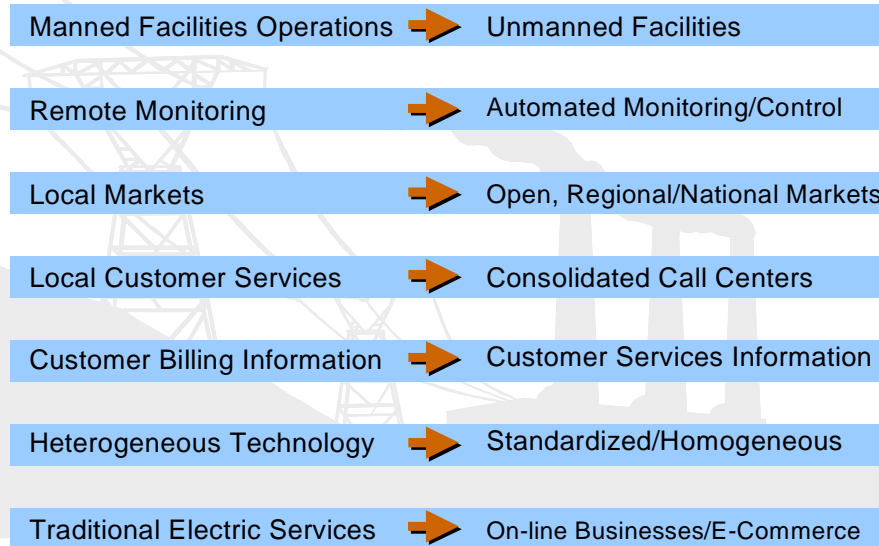
The demands of competing in newly deregulated electricity markets are leading utilities to intensify their already heavy dependence on information technology. In addition to helping electric utilities collect field data and issue the control commands needed to reliably generate, transmit, and distribute electricity, computer systems increasingly are being used to enter new markets, achieve business operating efficiencies, and communicate with customers and business partners. Therefore, the reliability and security of these information systems are more important to electric utilities' competitive posture than ever before. Chief information officers (CIO) are the management officials responsible for procuring and managing mission critical information systems. As such, they are in a key position to recognize the security risks posed by use of these technologies and lead action to institutionalize security as a significant criterion of information technology (IT) investment and policy decisions within their organizations.

~~~~~

Emerging Business Risks of IT Dependencies

The electric utility CIO's job has never been more challenging. The unprecedented extent of IT interdependencies both within and among electric utilities today has significantly expanded the number and scope of automated systems that might fall within the average CIO's purview. Accordingly, electric utility CIOs must cater to many constituencies within their organizations, each of which has a singular vision of how IT can strengthen the core business area for which it is responsible. However, few of these constituencies may be aware of the degree to which IT is a source of business risk as well as an enabler of business processes. To effectively manage their relationships with these constituencies, CIOs must not only understand the risks presented by their organizations' reliance on cyber systems, but communicate this understanding on an ongoing basis through formal and informal channels.

What Is Changing?



In this competitive business environment, CIOs often feel pressure from chief financial officers to maximize the organizational and business benefits from information technology investments. An industry trend toward standardization of computer systems reduces costs, but can also create potential new business risks. By relying on client-server-based applications using transmission control protocol/Internet protocol (TCP/IP) and other publicly documented protocols, electric utilities inadvertently expose themselves to a much larger population of potential hackers with the technical knowledge to successfully compromise such systems. Similarly, developing standards and inter-utility protocols, such as the Utility Communications Architecture (UCA) and Database Access Integration Service (DAIS) for data exchange, allows for the development of more sophisticated and interoperable systems. At the same time, however, this standardization makes technical information about these protocols accessible to a much larger number of individuals, in

cluding potential intruders.¹ This risk is exacerbated by utilities outsourcing to independent contractors and other vendors the customizing and maintenance of software and other products supporting their electric management systems.

Another significant security risk stems from the interconnectedness of the cyber networks that underpin the utility's generation, transmission, and distribution systems. Senior utility business managers (e.g., vice presidents of transmission, generation, or business planning) increasingly advocate linking their firms' operational control center and corporate information systems to better integrate business and operational processes. Moreover, increasing public demand for electricity is leading to greater integration between operational control networks and the transmission grid itself to maintain the highest levels of reliability and availability.

¹ National Security Telecommunications Advisory Committee, Information Assurance Task Force, *Electric Power Information Assurance Risk Assessment Report* (March 1997).

However, these interconnected automated systems present vulnerabilities that, if exploited, could disrupt the flow of electricity to a large number of customers. Cyber links between control systems and utility information systems, other utilities, power pools, control areas, etc. and remote maintenance and administration ports 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.² In addition to possible lost revenue from operations, such occurrences likely would have the lingering effect of reduced public confidence in the electric industry’s ability to deliver electricity reliably.

To differentiate their organizations in the face of increasing competition, customer service and energy trading managers also are using IT in new ways that add value for the customer and the utility. Many electric utilities have invested in highly sophisticated, information-intensive, consolidated customer call centers and automated dispatch centers. Utilities also are allowing their employees to access more customer data from a single computer platform. Customers are being billed, 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. In addition, technologies such as the Internet, virtual private networks, and other types of dedicated networks are fueling exponential growth in the number of wholesale electricity transactions. Power marketers are relying on Internet-based applications, such as the Open Access

Same-time Information System (OASIS), for access to information and markets.

Disruptions of or intrusions into the computer and communications systems that support essential customer service and energy wholesaling functions could rupture carefully nurtured customer relationships and public confidence. By corrupting customer service databases, a sophisticated hacker could hamper the timeliness and accuracy of customer billing processes, or obtain sensitive personal information about customers. Customer call center consolidation may make these customer service operations more vulnerable to denial of service attacks, which can sever important communications between electric utilities and their customers. Increased regulatory scrutiny, financial penalties, lawsuits, and public embarrassment could ensue, leading to a loss of customer loyalty. Breaches of the confidentiality, integrity, and availability of systems and data used in generation and transmission capacity trading could be equally harmful, causing market distortions and prompting government intervention or regulation. In short, security breaches of systems that do not even directly support the generation, transmission, and distribution of electricity can have effects so adverse and wide-reaching that they merit the attention of the firm’s chief executive officer and Board of Directors.

“Breaches in computer security cost 163 large U.S. companies and government organizations \$124 million in losses in 1998. And if that number seems low, remember that only a small fraction of companies report security breaches.”

**– CIO Magazine,
July 15, 1999**

² Ibid.

WHAT CAN A CIO DO?

As essential liaisons between operations and management personnel, CIOs are uniquely positioned to champion IT security issues within their organizations. Because non-technical threats to information systems security, such as disgruntled insiders, also influence corporate IT security strategy, CIOs have a key ability to bring together functional business managers from all parts of their organizations and ensure that a comprehensive strategy is developed. Accordingly, CIOs add significant business value to their roles by:

- Cultivating and maintaining close relationships with senior operations, telecommunications, physical security, human resources, and other relevant managers in their organizations in developing and implementing a comprehensive IT security plan
- Advocating the proactive enactment of IT security and employee use policies, including frequent updates to account for changes in the business and threat landscapes
- Raising internal awareness of IT security issues among all employees through ongoing security awareness programs and wide distribution of policies and procedures
- Incorporating IT security considerations in the acquisition, development, and installation of new IT systems or infrastructure as a standard practice,
- Proposing periodic audits of their organization's security infrastructures, including but not limited to their information technologies, by an independent source and giving priority to remediation work, and
- Sharing information with chief executives and their counterparts throughout the electric supply and delivery industry regarding threats, vulnerabilities, and other information security issues that necessitate inter- as well as intra-organization collaboration.

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.