riptech℠

Information Security Challenges in the Electric Power Industry

Talking Points

- **Executive Summary**
- **Growth of Information Systems in the Electric Power Industry**
  - Traditional Systems
  - E-business Initiatives
  - New Lines of Business
- **Network Security Vulnerabilities of Today**
- **Impacts of Security Breaches**
- **Remediation Strategies**
- **About Riptech**

Executive Summary

The introduction of competition in the electric power industry, combined with increased public demand for power, has resulted in greater reliance by power utilities on information systems and networks. Already crucial to the control and management of power from generation through to end use, information systems are also allowing utilities to manage other aspects of their businesses more efficiently. Customer management, supplier communications, and even the buying and selling of power to third parties, are becoming increasingly reliant on the use of information networks.

Just as information system expansion has occurred, information security vulnerabilities have shown a corresponding increase. Efforts to allow easier access to operational, customer, and supplier information, combined with the expansion of corporate IT boundaries as the result of merger and acquisitions, vastly increases the security vulnerabilities of power company networks. As a result, the impact of a security breach goes beyond operational concerns, and can have a devastating impact on the financial well-being of a company.

In an effort to explain the state of information security in the electric power industry, this paper highlights several trends that have established information networks as critical assets for utility companies. The paper identifies several key information security vulnerabilities and explains the potential impacts of each. Lastly, this paper identifies steps electric power companies can take to create an effective information security strategy.

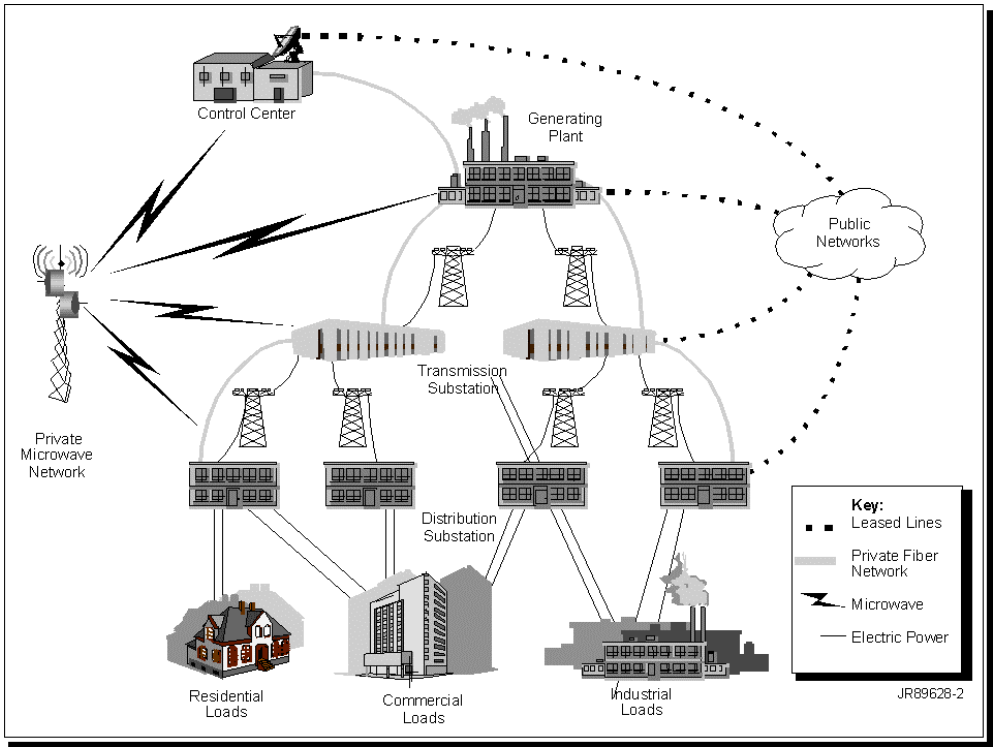
Growth of Information Systems in the Electric Power Industry

The structure of the electric power industry is undergoing a monumental transformation. As the industry transitions to a deregulated environment, companies are fundamentally restructuring not only the ways they conduct business, but also the types of business they conduct. Information technology is both a cause and a means for this restructuring, as power companies are looking to the Internet to streamline core business operations such as customer service, power and outage management, and supply procurement. As a result, electric power companies are becoming more reliant on robust, expansive, and open information systems.

Traditional Systems

Information networks have controlled electric power company core operations since before industry deregulation. These networks allow companies to maintain centralized monitoring of their energy management systems (EMS) and "move" power from generation to the end user. As shown in Figure 1 below, EMS systems encompass large numbers of transmission and distribution substations, which are often spread out over large distances and require centralized management. In order to provide a centralized management and monitoring capability, power companies deploy supervisory control and data acquisition (SCADA) systems, which allow a control center to collect electric system data from nodes placed throughout the power system. Using this data, SCADA systems can initiate alarms to operations personnel and relay control commands to the field.

FIGURE 1—Traditional Electric Power Company Communications and Control Layout



Source: "Electric Power Information Assurance Risk Assessment Report." *NSTAC Information Assurance Task Force* (March 1997)

Due to the immense size of modern power grids, the use of SCADA systems is widespread in the electric power industry and is considered an absolute necessity for effective energy management. Most of the approximately 3,200 electric power utilities serving North America depend on SCADA systems to manage power generation, transmission, and distribution. With 30,000 to 50,000 data collection points in an average SCADA system, centralized management of network data has become crucial to ensure power system reliability and maximize staff efficiency.

Recognizing the importance of their EMS and SCADA systems, most power companies constructed these networks separately from other corporate systems. Early SCADA systems were effectively "walled off" through the use of unique power supplies, special disaster recovery plans, and separate system development protocols. Over time, however, the convergence of power company networks and the demand for remote access to these systems has rendered many SCADA systems accessible through non-SCADA networks.

E-Business Initiatives and the Transformation of The Traditional Network Architecture

Over the past five years, the increased use of Internet technologies has transformed the way business is conducted in almost every major industry in North America, and the electric power industry is no exception. E-business strategies are enabling power companies to operate cost-effectively, communicate more efficiently, and create innovative business practices. Meanwhile, the advantages of an effective e-business strategy are becoming increasingly important, as power companies are forced to compete in a deregulated environment. The table below highlights a few of the key business areas that utilities have improved through the use of e-business and Internet strategies.

TRANSFORMATION OF EXISTING BUSINESS PROCESSES

Customer	Customer Information Systems (CIS)	Many utilities are replacing outdated CIS with new systems that focus outwardly on customers and are more accessible. Over half of present utility CIS systems are older than 10 years.
Supplier	E-procurement systems	Utility companies are joining together to take advantage of the efficiencies of online procurement of utility supplies. Pantellos, now an independent company and leader in utility procurement, was formed through the cooperation of 21 large companies.
Operations	Work and outage management systems (WMS/OMS)	With growing competition forcing more attention on customer service plus the threat of "performance-based rates" on the horizon, utilities across North America are scrambling to install WMS/OMS. Tightly integrating WMS/ OMSs improves response time, reduces manpower, and enhances productivity.

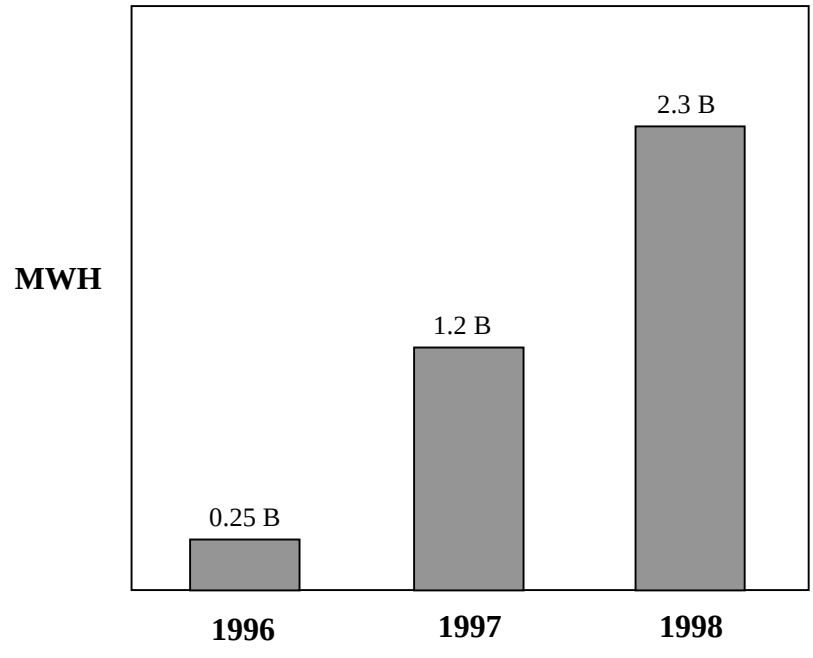
Source: "Replacing A Customer Information System," *Public Power*, October 1999

While the benefits of e-business initiatives are obvious, many utilities are only beginning to acknowledge the dangers that inevitably result when networks become more accessible to a wider range and number of users. Linking corporate systems together to provide access to customers, suppliers, and other third parties will significantly increase the vulnerability of sensitive and proprietary information contained in these systems.

Introduction of New Lines of Business

In order to compete successfully in a deregulated market, many electric power companies are seeking new sources of revenue growth through investment in opportunities that involve "nonelectric" functions, which formerly resided outside of their core business. These ventures are rapidly evolving from small start-ups into medium-sized and large stand-alone corporations. The most noteworthy of these ventures – power marketing– is heavily reliant on information systems. For instance, one major power market transaction platform, launched in 1999, conducted more than 130,000 transactions during its first 26 weeks, with a daily transaction value of up to $1.5 billion per day. Over half of these transactions are performed online. Figure 2 illustrates the growth of power marketing over the past 3 years.

FIGURE 2—GROWTH OF POWER MARKETING (1996-1998)



Source: Edison Electric Institute, January 2000

Network Security Vulnerabilities in the Electric Power Industry

As a result of their widespread use of SCADA systems for network management, power companies are currently vulnerable to internal and external network attacks. Because corporate networks and SCADA systems are linked at most utilities, the security of the SCADA system is often only as strong as the security of the corporate network. With pressure from deregulation forcing the rapid adoption of open access capabilities, vulnerabilities in these systems are increasing rapidly. The quotation below illustrates the magnitude of this problem:

FIGURE 3—SCADA SYSTEMS AT RISK

"A knowledgeable intruder, aided by publicly available 'hacker' tools, could issue false commands to a utilities energy management system (EMS), opening and closing relays, shutting down lines, and causing voltage oscillations and, potentially, cascading outages."

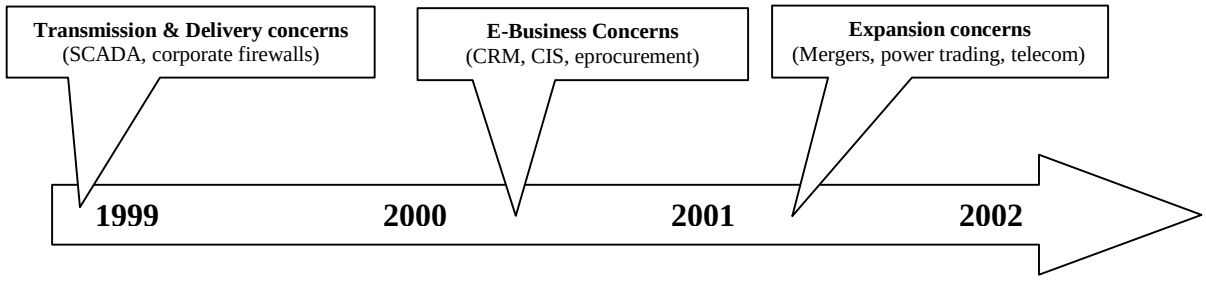
-- National Security Telecommunications Advisory Committee (NSTAC)

Source: "Electric Power Information Assurance Risk Assessment Report." *NSTAC Information Assurance Task Force* (March 1997)

Vulnerabilities extend beyond SCADA systems

As e-business initiatives gain momentum, power companies often integrate, billing and accounting information systems with other corporate information systems. In addition, consolidation through mergers and the integration of new lines of business are forcing power companies to connect diverse legacy systems without considering security risks. All of these factors are increasing the number and severity of security vulnerabilities. As figure 5 demonstrates, the information security concerns in the industry are evolving from operational issues to e-business and Internet concerns in the present and future.

FIGURE 4—Evolution of Network Vulnerabilities at Power Companies



Electric power companies, which are already concerned with security vulnerabilities affecting their ability to protect transmission and delivery systems, are beginning to realize additional potential vulnerabilities. For example, the development of advanced customer information systems (CIS) and e-procurement methods are prime examples of emerging concerns. In addition, expansion into new lines of business that require the integration of legacy systems will introduce completely new information security challenges.

Potential Impact of Security Breaches

The disruption of core business operations is the dominant security fear for electric power companies. Government and consumer pressure to keep electric systems operational have forced the industry to invest in methods to maximize the reliability and availability of power. While network security issues have always posed a threat to electric power system reliability, the expansion of remote access SCADA systems, the rise of e-business, and the rapid integration of legacy systems have significantly increased the number of potential system exploits. At the same time, the potential cost of a security breach has shown a corresponding increase. Some of the ways in which a security breach might negatively impact a power company are illustrated in the following table.

FIGURE 5—IMPACT OF INFORMATION SECURITY BREACHES

Operational Disruptions	At the core of the electric power industry is the need for reliability and availability of electricity throughout the power grid. Utilities must remain vigilant about the protection of their electricity management and SCADA systems to ensure that unauthorized access to these systems does not disrupt service. Although these systems have largely remained isolated from public network access in the past, the use of remote access to manage SCADA makes these systems increasingly more vulnerable to external attacks. Illustrating the monetary cost of service disruptions, a recent 8-hour power outage in Delaware, Maryland, and Virginia cost regional businesses $30.8 million in lost revenue.
Public Confidence	Competition has brought about an increased focus on customer service; thus, data about customer usage habits, payment, and demographics are crucial to utilities' CIS strategies. Disruptions of customer service functions could rupture carefully nurtured customer relationships and have damaging long lasting effects on customer confidence. As such, utilities must ensure that customer information is secured properly and that customer interfaces, such as call centers and web sites, are adequately guarded from denial of service attacks and "cyber-vandalism." An example of the cost of retaining public confidence in the wake of a security breach is illustrated by the recent security breach at the British utility Powergen. Earlier this year, Powergen admitted to a serious leak in network security that inadvertently exposed account information for over 7,000 users. The company issued advisories to all 7,000 users and also offered £50 compensation to each.
Corporate Reputation	Perhaps the most important implication of network security attacks on utility information systems is their impact to the reputation of the company. Just one security breach can have a devastating, irrevocable impact on the reputation and financial health of an organization, especially with increased competition in a deregulated environment. Because many investors are unsure as to which companies 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 power company is managed, including the company's ability to respond to competitive pressures and other market challenges.

Sources: "Power Outage Darkens Delmarva Peninsula," *The News-Times*, May 1996; "Powergen suffers serious security slip-up" *Internet.Works*, July 2000.

Remediation Strategies

With network security vulnerabilities multiplying rapidly, and the cost of security breaches becoming more severe, power companies need to develop top-notch information security practices. An effective approach to network security begins with a thorough assessment of present vulnerabilities and a careful evaluation of network security architectures. Most importantly, electric power company managers must recognize the gaps in their internal capabilities and consult with firms that offer network security expertise when necessary. The following quote illustrates the acute need for network security products and services in the power industry.

The Demand for IT Outsourcing

"To become "clicks and mortar" rather than "bricks and mortar" firms, utilities must do two things at once: restructure their organizations, and realize that their core competencies are in energy—not IT."

Source: "Pressures to Outsource Intensify." *Energy IT*, August 2000.

The most effective information security strategies for electric power companies blend regular, periodic security assessments with an ongoing attention to security architecture and monitoring. The following pages highlight the major steps that every electric power company should undertake to minimize the number and impact of security breaches.

STEP 1: Regular Vulnerability Assessments

Power companies must conduct regular vulnerability assessments of information systems and networks that support critical business processes. While many utilities try to regularly assess the vulnerabilities of their SCADA and EMS systems, the majority of firms fail to schedule assessments on a regular, re-occurring basis. In addition to assessing operational systems, power companies should strongly consider conducting additional assessments of corporate networks, web servers, and customer management systems. A thorough assessment of this kind can reveal unintended gaps in security, unknown linkages between public and private networks, and firewall configuration problems.

STEP 2: Expert Information Security Architecture Design

An overwhelming number of security technologies, networking devices, and configuration options are available to power companies. While firewalls, Intrusion Detection Systems (IDS), and Virtual Private Networks (VPN) can all help protect networks and data from malicious attacks, improper configuration and/or product selection can seriously hamper the effectiveness of a security posture. Often, companies severely compromise the value of their information security investments by failing to install and configure products correctly. In order to minimize risks associated with poor network architecture, utilities should work with information security professionals to ensure that evolving network architectures do not compromise information security capabilities.

STEP 3: Managed Security

As power companies add network security technologies to solidify their security posture, the need to properly manage and monitor these devices is becoming increasingly complex. The quotations below illustrate the failure of most large companies to adequately manage and monitor security devices throughout the organization.

Many Organizations Struggling to Manage Security Devices

"You'd be surprised at how many blue chip companies and dot-com sensations do not have someone in their organization who is competent to answer even simple questions."

– Richard Power, Editorial Director, Computer Security Institute

"Intrusion detection is becoming a full-time job—detecting it and then cleaning up after it."

– Kevin Baradet, Network Services Director, MIT

Source: "Hack Attacks Drive Outsourced Security." *PC Week.* (August 1999); "Expert Alarmed by Lack of Cybercrime Defenses." *The Indianapolis Star.* (May 2000).

Unfortunately, the implementation of "technology-only" solutions without close monitoring and management provides system administrators with limited security (often lessening the effect of the security devices). Because hiring experienced IT security experts to manage and monitor security devices is cost prohibitive, many organizations are outsourcing the management and monitoring of their security devices to highly specialized, managed security companies. Managed security offerings ensure that all security devices are configured properly and fully patched, while monitoring the actual activity on each device using intelligent software solutions and security analyst expertise. This enables corporations to maintain a real-time security monitoring capability at a relatively low cost, and can actually increase the value of existing information security devices by enhancing their performance and capabilities. Several of the advantages of managed security services are listed on the following page.

ADVANTAGES OF MANAGED SECURITY SOLUTIONS

Cost-effective security management
Managed security products eliminate the need for organizations to recruit and retain qualified IT security staff – a task that has occupied a rapidly increasing portion of the IT budget in recent years.

Centralized Device Monitoring
Many large and mid-sized organizations operate a variety of security devices spread over several geographic locations. Continuous monitoring and maintenance of these devices from a single location is difficult, if not impossible, for most organizations. Managed security products allow organizations to feed data from all security devices to a central (outsourced) location for real-time, continuous monitoring and analysis.

Upgrade and Patch Management
Many organizations overlook frequent patches and system upgrades released by product vendors (e.g., operating system patches, firewall upgrades, etc.) rendering protective mechanisms more vulnerable to new hacker techniques. Managed security products ensure that all patches and upgrades are added to all security devices immediately upon release.

Incident response and forensics
Most organizations experience difficulty sifting through millions of lines of log data and IDS alerts even after malicious activity has been detected. By standardizing the data produced by all security devices, managed security products are able to retrieve data that identifies the type and source of malicious activity, which can then be used by law enforcement to identify and prosecute those responsible.

Intelligent decision support
Managed security products feed security device logs, activity reports, and alerts into a proprietary analysis engine that searches for patterns of malicious activity that would otherwise be overlooked (if not ignored) by untrained or even expert security staff. The decision support function enables organizations to react in real-time to prevent potential security threats, rather than simply investigating the problem after malicious activity has already occurred.

About Riptech

Riptech [SM], the premier information security services provider, delivers Real-Time Information Protection [SM] through a comprehensive suite of Real-Time Managed Security Services and Security Professional Services. Riptech secures clients through around-the-clock security management, monitoring, analysis and response delivered by security experts in world-class Security Operations Centers using a proprietary, next generation intelligent technology platform. This platform is capable of processing large volumes of network security data to separate actual security threats from false positives in real-time, with nearly limitless scalability. Additionally, Riptech's Security Professional Services group provides security policy development, assessment and auditing, penetration testing, incident forensics, and response. Riptech has secured hundreds of organizations including Fortune 500 companies, emerging e-Businesses, and federal agencies. Founded in 1998 by former U.S. Department of Defense security professionals and market experts, Riptech is headquartered in Alexandria, Virginia. If you have questions about this white paper or Riptech's consulting and managed security solutions, please feel free to contact the following individuals:

Joe Pendry
Director, Utility Strategies
703-373-5100
jpendry@riptech.com

