WHITE PAPER

Information Security Challenges in the Electric Power Industry

INSIDE

INSIDE

- Growth of information systems
- Electric utility security challenges
- Business needs for security
- NERC cybersecurity standards
- Addressing security challenges

Contents

Executive summary 1

Growth of information systems 1

- Operational systems 1
- Transformation of the traditional network architecture 2

Electric utility security challenges 3

- Operational system security challenges 3
- Corporate IT security challenges 4

Business needs for security 4

- Recent cyberattack events 5

NERC cybersecurity standards 6

Addressing security challenges 8

- Perform regular assessments 8
- Design an effective information security architecture 8
- Deploy a balanced security infrastructure 9

Executive summary

Increasing competition within the electric power industry, combined with increased public demand for power, has resulted in greater reliance by electric utilities on information systems and networks. Already crucial to the control and management of power from generation through to delivery, information systems also allow electric 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 have become increasingly reliant on the use of information networks.

As the information systems of electric utilities have expanded, the risks to them have shown a corresponding increase. Efforts to allow easier access to operational, customer, and supplier information inevitably bring the possibility of compromised access to the network. The expansion of corporate IT boundaries as the result of mergers and acquisitions complicates security strategies. And the budget pressures associated with deregulation have caused some electric utilities to postpone upgrades that would have created a more modern, secure IT infrastructure.

All of those factors vastly increase the vulnerability of power company networks—and today's high volume of Internet threats puts those vulnerabilities at greater risk of being exploited. At stake is no less than a critical component of our nation's infrastructure: the electric power grid. A cyber attack that disrupts normal grid operations could profoundly impact the financial well-being not just of a single power company, but of thousands of other businesses and municipalities that depend on it.

This paper addresses the issues involved in protecting critical infrastructures, and examines the effect recent threats have had on electric utilities. It includes a discussion of the NERC[1] cyber security standards, and of the way in which electric utilities can adhere to those standards. Lastly, it identifies steps electric power companies can take to create a comprehensive information security strategy.

Growth of information systems

The electric power industry is undergoing a fundamental transformation. Companies are restructuring not only the way they conduct business, but also the type of business they conduct. Information technology is both a cause and a means for this restructuring, as power companies are look to the Internet and open systems technologies 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 open information systems.

OPERATIONAL 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 to "move" power from generation facilities to end users. EMS encompass large numbers of transmission and distribution substations, which are often far

[1] North American Electric Reliability Council

apart from each other. In order to provide centralized management and monitoring of those dispersed facilities, 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 that data, SCADA systems can initiate alarms to operations personnel. They can also relay control commands to the field to compensate for systems that have gone offline or for fluctuating power needs in different areas.

Due to the immense size of modern power grids, the use of SCADA systems is considered a necessity for effective energy management. With 30,000 to 50,000 data collection and control points in an average SCADA system, centralized management of network data is indispensible to power system reliability and maximum 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 SCADA systems has led to many of them becoming accessible through non-SCADA networks.

TRANSFORMATION OF THE TRADITIONAL NETWORK ARCHITECTURE

Over the past decade, 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. Internet connectivity enables power companies to operate more cost-effectively, communicate more efficiently, and create innovative business practices.

While the benefits of connectivity initiatives are obvious, many electric utilities are only now beginning to acknowledge the dangers that inevitably result when networks become more accessible—intentionally or otherwise—to a wider range and number of users. Linking corporate systems together to provide access to customers, suppliers, and other third parties significantly increases the threat to the sensitive and proprietary information contained in those systems. Perhaps even more important, such linking also increases the threat to control systems. Linkages between corporate networks and the networks that run an electric utility's operational control system are now increasingly common, yet in many cases, these joined networks are inadequately protected.

An additional complication arises from the fact that certain SCADA networks may have been installed by third-party systems integrators that have exclusive authority to maintain them, introducing yet another potential security exposure.

Electric utility security challenges

All divisions of an electric power company must work together to reduce security risks, or face the prospect of outages that could damage the company's reputation, harm its clients, and lower the price of its shares. Specifically, CIOs and the IT staff who run the corporate network need to work with COOs and the staff who run the operational network to ensure that risks are properly addressed and assets are properly protected throughout the enterprise.

OPERATIONAL SYSTEM SECURITY CHALLENGES

As a result of increased business dependence on the corporate network and widespread use of SCADA systems for energy management, power companies are currently susceptible to both internal and external network attacks. Few (if any) SCADA systems were designed with security in mind and adding security to them after the fact has proven challenging. In fact, the legacy of SCADA security could well be called "security through obscurity"—which is to say, no security at all. The assumption has been that because SCADA systems are complicated and proprietary, few people know enough about them to do much damage. As hackers look for new ways to attack power systems, that assumption is not only false, but dangerous.

Because corporate networks and SCADA systems are linked at most electric 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, exposure in both systems is increasing rapidly.

The importance of protecting SCADA networks can hardly be overstressed. Even before the massive power outage of August 2003, the U.S. government was scrutinizing the measures being taken by electric utility providers to prevent disruptions by terrorists. The August blackout focused the attention of Congress, utility shareholders, and the general public on the seeming fragility of the national electric power infrastructure. Yet research by Gartner indicates that many utilities are unwilling to spend the money it would take to implement robust security measures in their SCADA (and business) networks. It's clear that electric power companies must take aggressive proactive steps to secure their networks before shareholders lose confidence and the federal government imposes mandatory security regulations.

"Although Gartner research indicates that many utilities cite improved security as one major driver behind their organizations' technology initiatives for 2003, improved security ranks third behind cost management/cost savings and improved profitability or productivity for electric service utilities. Enterprises must increase the logical security of corporate IT and supervisory control and data acquisition (SCADA) networks as well as address the physical security vulnerabilities of utility generation plants."

Gartner Research, *Critical Infrastructure Protection: Key Issues for Utilities,* February 2003

CORPORATE IT SECURITY CHALLENGES

Already concerned with security vulnerabilities in transmission and delivery systems, electric power companies are now facing additional vulnerabilities as they integrate those systems with their business networks. The opening of billing and accounting systems to online customer and vendor access brings new potential problems. Consolidation through mergers and the integration of new lines of business are forcing power companies to connect diverse legacy systems without full consideration of security issues. Employees are expecting full access to the corporate network no matter where they're working. And customers want to be able to check their accounts and pay their bills online. All of these factors are increasing the number and severity of online security risks.

Business needs for security

Major disruption is the dominant security fear for electric power companies—and it's a well justified fear. The August 2003 blackout in the Northeast and Great Lakes area—the largest blackout in U.S. history—caused over $50 billion in economic losses.

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 to SCADA systems, the rise of Internet access to business networks, 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 similar increase. Some of the business needs for preventing security breaches are illustrated in table 1 below.

Table 1: Business needs for preventing security breaches

Operational continuity	At the core of the electric power industry is the need for reliability and availability of electricity throughout the power grid. Electric utilities must remain vigilant about the protection of their electricity management and SCADA systems to prevent unauthorized access and disruption of service.
TCO/ROI of security investments	Watching the bottom line is always a primary driver in making security investments. The cost of preventing security breaches has a lower potential financial impact than exposing the company to the high risk of unknown and unplanned expenses due to downtime, incident response, and recovery.

Table 1 *(continued)*

Corporate reputation and public confidence	Perhaps the most important result of network security attacks on electric utility information systems is their impact on the reputation of the company. Even a single security breach can have a devastating, irrevocable impact on the reputation and financial health of an organization. Company 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. Competition has brought about an increased focus on customer service; thus, data about customer usage habits, payment, and demographics are crucial to electric utilities' CIS strategies. Disruptions of customer service functions could rupture carefully nurtured customer relationships and have damaging, long-lasting effects on customer confidence. For this reason, electric 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." Any disruption in service caused by the electric utility is also likely to result in a significant loss of shareholder value.

RECENT CYBERATTACK EVENTS

Attacks on electric utilities—whether intentional or the byproduct of a general Internet attack—are not just a theoretical threat. The following incidents have already occurred.

- "A server on the control center LAN running SQL was not patched. The worm did not reach the server via the organization's connection to the Internet. It did apparently migrate through the corporate networks until it finally reached the critical SCADA network via a remote computer through a VPN connection. The worm propagated, blocking SCADA traffic." (NERC, *SQL Slammer Worm Lessons Learned for Consideration by the Electricity Sector,* June 2003.)
- "The control network uses frame relay. The telecommunications frame relay provider utilizes Asynchronous Transfer Mode through the telecommunications network backbone for a variety of services. The ATM bandwidth became overwhelmed by the worm, blocking SCADA traffic." (ibid.)
- "In Queensland, Australia, a former employee used commercially available technology on 46 occasions to remotely take control of the SCADA system used to manage the sewage treatment system. During these intrusions, the utility's managers were unable to determine why the system was behaving abnormally." (Gartner Research, *Prepare for Cyberattacks on the Power Grid*, October 2002.) This attack was accomplished by means of a wireless system in the former employee's vehicle, a "drive-by" attack, if you will. This illustrates the extreme permeability of inadequately protected SCADA nets, which are often connected by wireless links.

- "The W32.Blaster worm may have contributed to the cascading effect of the Aug. 14 blackout.... On the day of the blackout, Blaster degraded the performance of several communications lines linking key data centers used by utility companies to manage the power grid...." (Computerworld, *Blaster worm linked to severity of blackout,* August 29, 2003.)

In the paper cited above, Gartner Research states the obvious lesson: "Power companies should conclude that they are vulnerable to cyber attack. They have a real and growing exposure that many in the industry have been slow to understand. They have deployed only the most rudimentary security services and devices to protect the command and control elements."

"To assess the vulnerability of the electric power grid to cyberbased attacks and what the result would be on the other infrastructures and the economy in general, Gartner and the U.S. Naval War College sponsored, designed and carried out a war game in July 2002....

"The exercise showed that cyberattacks alone are unlikely to bring down major segments of the electrical system, but could cause major and prolonged interruptions of electrical supplies within regional power grids. The war game also revealed that no single attack on the control systems of the nation's power grid is likely to do more than cause an isolated outage. However, a coordinated assault—using a physical attack on key electrical transmission and generation facilities, coupled with cyberattack—would allow perpetrators to amplify and prolong the effects over a larger area."

Gartner Research, *Prepare for Cyberattacks on the Power Grid*, October 2002

NERC cybersecurity standards

In response to the need for protecting our national grid, NERC approved Urgent Action Standard 1200—Cyber Security. Coincidentally, NERC's Board of Governors adopted the standard just one day before the August 14, 2003, blackout once again focused the country's attention on the reliability of that grid.

Drawing long-term lessons from the outage, NERC President and CEO Michehl R. Gent said, "I cannot address this event without underscoring yet again the need to establish mandatory, enforceable reliability standards. NERC has developed a world-class set of planning and operating standards, and I expect we will find areas of those standards that need improvement based on the events of August 14. However, as long as compliance with these standards remains voluntary, we will fall short of providing the greatest possible assurance of reliability that could be achieved through mandatory verification of compliance and the ability to impose penalties and sanctions for non-compliance."

The adoption of Standard 1200 recognizes that voluntary adherence to industry standards and other demonstrations of a proactive commitment to cybersecurity are vital to avoiding the imposition of mandatory measures by the FERC[2].

[2]Federal Energy Regulatory Commission

Table 2: NERC urgent action standard 1200—Cyber Security

Standard	Title and description
1201	**Cyber Security Policy.** Requires companies to create and maintain a cyber security policy for implementing the measures outlined in this standard.
1202	**Critical Cyber Assets.** Requires companies to identify their critical cyber assets.
1203	**Electronic Security Perimeter.** Requires companies to identify their electronic security perimeter(s).
1204	**Electronic Access Controls.** Requires companies to identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter.
1205	**Physical Security Perimeter.** Requires companies to identify their physical security perimeter(s) for protecting critical cyber assets.
1206	**Physical Access Controls.** Requires companies to identify and implement physical access controls for access to critical cyber assets within the electronic security perimeter.
1207	**Personnel.** Requires companies to identify all personnel who are granted electronic or physical access to critical cyber assets.
1208	**Monitoring Physical Access.** Requires companies to monitor physical access to critical cyber assets 24 hours a day, 7 days a week.
1209	**Monitoring Electronic Access.** Requires companies to monitor electronic access to critical cyber assets 24 hours a day, 7 days a week.
1210	**Information Protection.** Requires companies to protect information associated with critical cyber assets and the policies and practices used to keep those assets secure.
1211	**Training.** Requires companies to train personnel as appropriate for their level of access to critical cyber assets.
1212	**Systems Management.** Requires companies to establish systems management policies and procedures for configuring and securing critical cyber assets.
1213	**Test Procedures.** Requires companies to establish test procedures and acceptance criteria to ensure that new or modified critical cyber assets comply with this standard.

Table 2 ***(continued)***

Standard	Title and description
1214	**Electronic Incident Response Actions.** Requires companies to define electronic incident response actions, including roles and responsibilities assigned by individual or job function.
1215	**Physical Incident Response Actions.** Requires companies to define physical incident response actions, including roles and responsibilities assigned by individual or job function.
1216	**Recovery Plans.** Requires companies to create action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.

Source: *NERC Urgent Action Cyber Security Standard*, August 13, 2003, www.nerc.com.

Addressing security challenges

With network security threats multiplying rapidly, and the financial consequences of security breaches becoming ever greater, every power company must develop information security practices that address today's challenges. Effective network security begins with a thorough assessment of each network and its security architecture, followed by a carefully developed plan for improving security. The following pages highlight the major steps that every electric power company can take to minimize the number and impact of security breaches.

PERFORM REGULAR ASSESSMENTS

Power companies should conduct regular risk assessments of information systems and networks that support critical business processes—and then take appropriate post-assessment actions to mitigate any risks discovered during the assessment.

While many electric utilities conduct regular risk assessments of their EMS and SCADA systems, the majority do not. In addition to regular, scheduled assessments of operational systems, power companies should strongly consider conducting additional assessments of corporate networks, Web servers, and customer management systems. A thorough review of this kind can reveal unintended gaps in security, unknown linkages between public and private networks, and firewall configuration problems.

DESIGN AN EFFECTIVE INFORMATION SECURITY ARCHITECTURE

An overwhelming number of security technologies, networking devices, and configuration options are available to power companies. While firewalls, intrusion detection systems, and virtual private networks can all help protect networks and data from malicious attacks, improper configuration and/or product selection can seriously reduce security. Often, companies greatly reduce the value of their investment in information security by failing to install and configure products correctly, or by not properly defining "zones of trust" (information separation areas) within the internal network. In order to minimize risks associated with poor network architecture, electric utilities should consider working with information security professionals to ensure that evolving network architectures do not compromise information security capabilities.

DEPLOY A BALANCED SECURITY INFRASTRUCTURE

In order to be well protected, corporate and control networks need to be surrounded by several different robust technologies. Products offering those technologies must be selected carefully to ensure that they will work properly together to create a comprehensive security environment.

Table 3: Recommended security deployment and Symantec offerings

Assessments and early warning	In a real-time industry like electric power, finding out about a virus, worm, or hacker attack after the damage has been done could be disastrous. Early warning is key to maintaining business continuity, allowing the company to take proactive measures to keep the power flowing. The **Symantec DeepSight™ Threat Management System** sends warnings before attacks hit critical systems. It delivers customized and timely warnings on imminent threats, enabling power companies to focus resources on preventing attacks rather than recovering from them. **Symantec DeepSight Alert Services** help secure an IT environment faster and more effectively by supplying vulnerability and malicious code alerts customized to each company's exact network infrastructure.
Protection technologies	Protection is critical, whether it be developing effective zones of trust that cut between the corporate and the operational networks, implementing security policies, or better defending the network against complex threats. **Symantec ManHunt™** offers high-speed network intrusion detection, real-time analysis, and proactive measures against intrusions and denial-of-service attacks. **Symantec™ Gateway Security** is a next-generation firewall appliance that integrates seven different security technologies for maximum effectiveness against a wide range of cyberthreats.

Table 3 *(continued)*

Monitoring and managing	As power companies add network security technologies the management and monitoring of security devices is becoming increasingly complex. Hiring experienced IT security experts to manage and monitor security devices can be prohibitively costly, so many organizations are outsourcing the management and monitoring of their security devices to highly specialized, managed security companies. Such partnerships enable 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. **Symantec Enterprise Security Manager™** provides comprehensive, policy-based security assessment and management. It now includes policy templates designed especially to ensure compliance with the NERC cybersecurity standards. **Symantec Managed Security Services** deliver industry-leading security monitoring, management, and response. These 24x7 real-time services are designed to enhance an organization's information security posture through continuous monitoring and management of security devices, expert analysis of log data, and immediate response to potential security threats as they're detected. A crucial component of security management is incident response. **Symantec™ Incident Manager** turns security data into prioritized, actionable information. By uniting cyber security events from both Symantec and third-party security products, it offers a unified view of a company's information security issues and response activities.

"Power companies depend on SCADA to control their operations. Therefore, they should provide security in proportion to the threat. Measures for SCADA systems should include physical security, intrusion detection and strong authentication measures, as well as business continuity and disaster recovery plans for the operation centers and SCADA systems."

Gartner Research, *Prepare for Cyberattacks on the Power Grid,* October 2002

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

For more information, please visit http://enterprisesecurity.symantec.com.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product Information in the U.S., call toll-free 800.745.6054

Symantec has worldwide operations in 36 countries. For specific country offices and contact numbers please visit our Web site.

Symantec and the Symantec logo and DeepSight are U.S. registered trademarks of Symantec Corporation. Symantec Enterprise Security Manager, Symantec Gateway Security, Symantec Incident Manager, Symantec ManHunt, Symantec Managed Security Services, and are trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. All product information is subject to change. Copyright © 2003 Symantec Corporation. All rights reserved. Printed in the U.S.A. RM101003draft