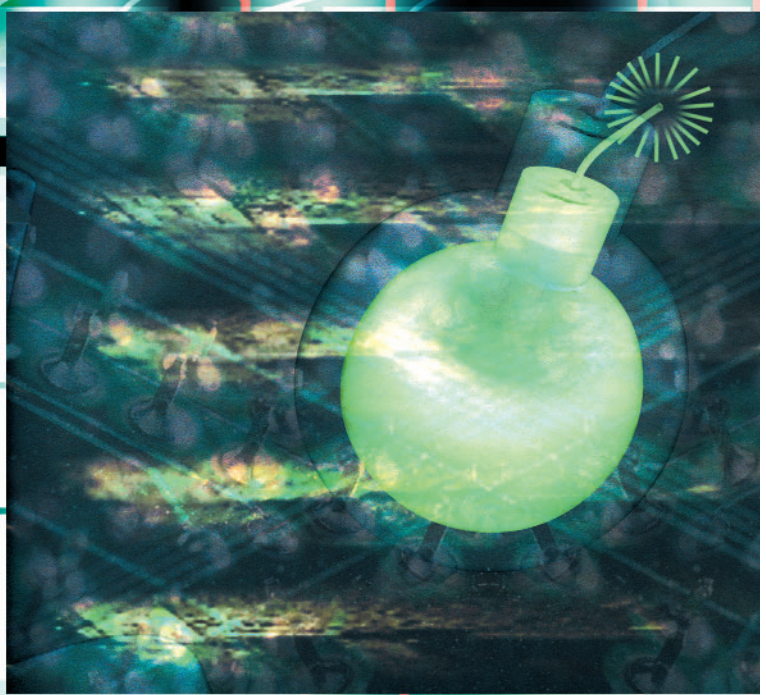
Electric Utility Responses to Grid Security Issues

by Robert Schainker, John Douglas, and Thomas Kropp



1540-7977/06/$20.00©2006 IEEE

Threats to Physical and Cyber Assets Do Exist

THE RISE OF TERRORISM AND MAJOR NATURAL DISASTERS REQUIRES GRID executives, design engineers, and grid operators to analyze and deploy technologies—hardware and software—to address the vulnerability of the power grid to physical and cyberattacks. A wide variety of work has already been performed by utility management, operation, and maintenance personnel in this area. Even so, much-needed work is still required, since threats have increased in both the physical and cyber areas. Because electricity drives virtually all of the nation's critical infrastructures—from lightbulbs to computerized factories—the electric power system presents an inviting target for onshore and offshore terrorists.

A coordinated attack on major power plants or substations could trigger a cascading blackout with major business, social, and national economic impacts. Depending on the extent and success of such an attack, daily life and business could be disrupted for at least several days across a wide area of the country, and a complete return to normalcy could take months to years.

Utility decision makers face a number of challenges in the security area. The broad scope of the security issue has led to the development of multiple and sometimes overlapping requirements from various government and state agencies. At the same time, utility efforts to increase security are often constrained by limited access to useful information produced by these agencies and others, either because of the highly classified nature of the data or because the data are distributed across multiple locations. As a result, utility executives often have been forced to make security-related decisions on the basis of sparse, uncertain, or anecdotal information. A further challenge for electric utilities involves internal communications—how to effectively communicate security weaknesses identified by utility operations, planning, and engineering personnel to higher-level management.

Blessing and Curse

Due to its very large size, the U.S. electric infrastructure (see Figure 1) has both strengths and vulnerabilities with regard to terrorist attacks. Currently, there are over 200,000 miles of transmission lines that are 230 kV or higher (see Figure 2), and there are many more miles of lower-voltage lines. The curse is that it is impossible to secure the whole system, and thus a determined group of terrorists could likely take out any portion of the grid they desire. The blessing is that such a terrorist attack, although disruptive and costly to the local region, would indeed be only a small portion of the overall grid. For example, the destruction of a region's transmission towers would only have temporary impact. Today, utilities are capable of restoring high- and low-voltage equipment damaged by tornadoes, hurricanes, ice storms, and earthquakes in a relatively short period of time. This is because the U.S. grid has been designed for resilience to such natural

events, and personnel are trained to respond quickly, often with neighboring utilities helping out in times of emergency outages and disasters. It would be difficult for even a well-organized large group of terrorists to cause the physical damage of a small- to moderate-scale tornado.

Even so, a well-coordinated attack on key high-voltage substations and control centers could disrupt power delivery to a large region, and the impacts of such an attack could be very costly, depending on the number of spare high-voltage transformers available and the utilities' transport and installation capabilities. Because the utilities impacted by such an attack would experience large financial losses, they should do whatever they can to obtain spare equipment and train staff for such emergencies. Although such an attack could be devastating to the utility and region involved, disrupting operations for weeks or even months, the impact on the country as a whole would not be extreme.

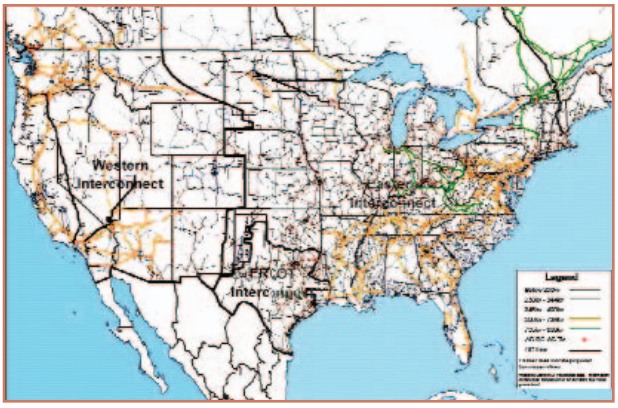


figure 1. The U.S. electric grid infrastructure.

figure 2. Transmission lines gallop across the landscape.

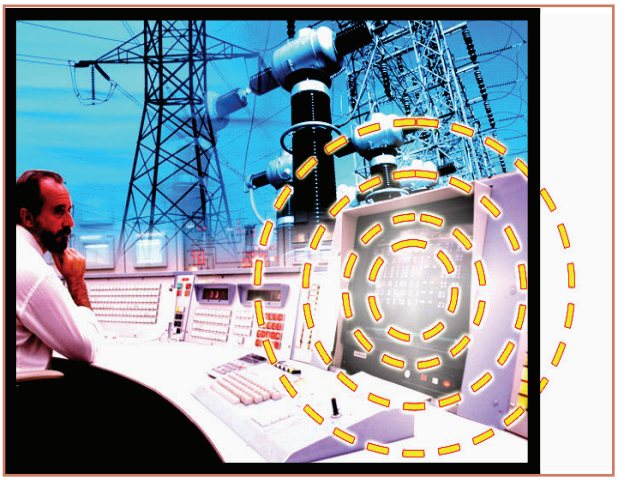


figure 3. A cyberattack could disable an electric grid computer operator control panel.

The Cyberthreat

Especially worrisome in a time of increasing industry dependence on the Internet and computerized monitoring and grid control systems is the fact that a serious attack need not be directly physical. The perpetrators could remain anonymous and remote, achieving their goals by disrupting a utility's computer network or power grid control systems. A successful cyberattack, for example, could potentially allow a terrorist to destroy equipment by sending false control signals or by disabling grid control center computer systems and monitors (see Figure 3) and/or disable protective relays on the electric grid. Every day, a typical large electric utility must fight off hundreds or even thousands of attempted cyberintrusions that appear to originate with hackers trying to disrupt normal business, obtain sensitive data, and/or exert control over parts of the grid. Presented below (see Table 1) are some of the reported cyberattack successes that have occurred for a variety of electric utility and other utility industries.

Most utilities, of course, have already enhanced their efforts to protect both physical facilities and computer networks. The fact that virtually all of the illegal entry attempts so far have failed indicates the effectiveness of current cybersecurity measures. "Utilities throughout North America have made significant strides to implement cyber and physical security," says Luther Tai, senior vice president of central services at Consolidated Edison Co.

Part of the problem is that, with electric power networks so tightly interconnected, a significant security breach anywhere on the system can have an effect on the system as a whole. Since there are many different types of utilities in the United States, each at a different level of cyberpreparedness, there is a compelling incentive to improve the coordination of security precautions taken by all utilities.

Since 2001, a number of individual utilities have pioneered important cybersecurity efforts, each producing valuable results. However, a lack of effective technology transfer and broad industry support has limited the effectiveness of these results for the industry as a whole. Because cybersecurity is only as strong as the "weakest link" in the chain of interconnected information and communication systems that utilities use, increased industry support, participation, and successful implementation of new cybersecurity tools are crucial for effective industry-wide cybersecurity.

In order to help provide the needed coordination and establish a unified response to cyberthreats, government and

industry organizations are continuing to develop and deploy new cybersecurity initiatives and technologies. In addition, important new results are emerging from the industry's own long-standing research and development (R&D) work on electricity infrastructure security.

Industry Efforts to Enhance Grid Security

Before 11 September 2001, the Electric Power Research Institute (EPRI) led an industry-wide effort to reinforce U.S. power infrastructure security. But as with most of the nation's protection and emergency response programs, the 9/11 terrorist attacks sparked a fundamental rethinking, expansion, and refocusing of utility security efforts. While earlier concerns largely centered on the effects of natural disasters, system control anomalies, and small-scale vandalism, the 21st century equation clearly must include protection against calculated assaults designed to disrupt American life and commerce on a large scale. EPRI's Infrastructure Security Initiative (ISI) was launched in response to these challenges and was designed to develop both prevention countermeasures and enhanced recovery capabilities.

As part of the work to provide utilities with immediately useful countermeasures, ISI has documented lessons learned from actual terrorist attacks and other catastrophic events at utilities around the world. One of the highlights of this effort came in 2004 with a report from Israel Electric Corporation (IEC) on the best practices they developed to defend their grid against terrorist attacks. The key conclusions stated in this "countermeasures" IEC report are as follows:

- ✔ There is no simple, single checklist for action that is appropriate to all possible emergencies.
- ✔ Be prepared for *anything*, i.e., any scenario you can think of, based on local/national information and past experience.
- ✔ Successful defense is based on three elements:
  - people-related work efforts
    - — hire qualified people
    - — conduct extensive security (physical and cyber) training after the person is hired and every three months thereafter
    - — make all employees aware of security issues and make them part of the solution development process
    - — conduct frequent security exercises; hold these exercises jointly, across utility departments.
  - procedures-related work efforts
    - — train all staff on what to do for a wide variety of emergency situations
    - — build a comprehensive body of procedures for each department and for each person responsible for decisions and actions during an emergency
    - — audit and update these procedures regularly
    - — issue new procedures where necessary, based on lessons learned from others and experiences staff obtain when they take part in responding to an emergency.
  - technology/spare equipment-related work efforts:
    - — consider a variety of different types of technologies (hardware and software) in pursuing security goals
    - — develop and deploy a crisis management computer system
    - — harden control centers, backup dispatch control centers, and communication systems
    - — develop/deploy an independent, secure emergency communication system
    - — stockpile all necessary spare parts in rapidly deployable, secure, and safe locations
    - — specify key hardware for storage in these locations, including equipment to bypass lines around damaged substations, recovery/mobile transformers, mobile generators, and emergency reconstruction transmission line components
    - — use the best equipment and staff your budget can afford
    - — remember that technology cannot replace well-trained personnel.

The countermeasures project is also providing utilities with information on new ways to protect grid facilities, including an artificial intelligence technology that can automatically analyze the streaming video from large sets of multiple cameras in remote locations to detect, for example,

table 1. Chronology of reported cyberattacks on electric and other utilities.

Year	Reported Successful Cyberattacks
1994	Salt River Project: A water facility in Arizona was breached by a cyberattack. The hacker trespassed in critical areas that could have caused significant damage.
1997	A teenager remotely disabled part of the public switching network in Massachusetts, which shut down telephone service to 600 customers.
2000	A disgruntled employee of an Australian company used his laptop car computer to remotely hack into the controls of a sewage treatment system, which caused 264,000 gallons of raw sewage to be released into public waterways of Australia over a period of two months. This caused marine life to die and creek water to turn black, producing an unbearable stench to nearby residents, among other impacts.
2001	Hackers attacked the California Independent System Operator which manages the electricity supply of California. The *Los Angeles Times* reported that the cyberhackers "got close" to disrupting power flow during the California rolling blackouts in May 2001.
2003	The SQL Slammer worm infected and disabled internal systems at a nuclear power plant in Ohio. Safety was never compromised, but a safety parameter display system and the plant process control computer were knocked off-line by the cyberworm for several hours.

The U.S. electric infrastructure has both strengths and vulnerabilities with regard to terrorist attacks.

whether an intruder has dropped a suspicious object near important electric grid equipment.

Among potential infrastructure targets attractive to terrorists, high-voltage transformers represent a critical vulnerability. These transformers cost several million dollars each and usually take one to two years to procure, build, and install. In response to this threat, ISI came up with the concept and developed preliminary designs for a new type of transformer that can be easily stored, transported, and installed for emergency use. An important milestone in development of this so-called recovery transformer was achieved in 2004 with the completion of preliminary designs for two units, rated at 500 kV and 345 kV. Both can be transported by truck, rail, or military cargo plane, and once all parts are available on site, they can be installed in about 48 hours.

Emergency communication technologies have also been evaluated by ISI in order to recommend to utilities the best alternatives for use in case of emergency. The aim is to provide utilities with secure ways of communicating with each other and with emergency services after a hypothetical successful, multiregional terrorist attack. This work is being coordinated with related projects going on in government agencies and in other countries. In particular, the use of satellite phones—which support both voice and data communication—is being explored.

Protecting Against Cyberattacks

In this age of wide-scale digitization, physical attacks are far from the only concern. The known successes of cyberattacks on a surprising variety of industries offer chilling testimony to the need for countermeasures against computer-based intrusions.

While physical assaults—facility break-ins, weapon attacks, or bomb explosions—are certainly frightening possibilities, cyberattacks have the potential to be every bit as destructive and carry the insidious added threats of stealth and long-distance control. If a cyberterrorist is able to get through a company's firewall and other protection systems, it doesn't matter if he's on the other side of the world. If he's linked in through the Internet—which is available virtually everywhere—and he penetrates a utility computer's firewalls that protect operational control systems, that attacker may as well be sitting in your control room.

Indeed, the incredible power and flexibility of the Internet has made cyberspace part of the global battlefield, and several nations have incorporated explicit plans for attacking information systems into their military preparations. Russia, for example, has documented successes in cyberattacks against key Chechen Web sites. India and Pakistan have pursued competing preparations for electronic warfare. China has formulated an official cyberwarfare doctrine, and North Korea has experimented with offensive cybertechnologies. Terrorist organizations in the Middle East have shown increasing sophistication in the use of information technologies and have made no secret of their intent to attack critical American infrastructures.

The U.S. government has long been concerned over the wide-ranging effects that computer-based attacks could have on the nation's key infrastructures. After the Morris computer worm brought 10% of the country's Internet systems to a standstill in 1988, the Defense Advanced Research Projects Agency (DARPA) set up the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University to monitor cyberthreats and respond to serious security incidents. According to CERT, keeping ahead of the trouble is no easy task. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty in detecting an attack, and increased difficulty in catching the attackers.

In 2004, the Department of Homeland Security (DHS) set up the Process Control Systems Forum (PCSF) to focus specifically on threats to the computerized automated control systems that underlie operation of most of the country's critical infrastructures, including the electric power grid. The PCSF is leveraging security knowledge currently dispersed among different infrastructures and stimulating cross-functional discussions between those responsible for information technology and operations. EPRI and the North American Electric Reliability Council (NERC) are coordinating with the PCSF to ensure that the utility industry's security concerns and solutions are shared (on a confidential basis).

Technologically, utility industry restructuring has created several unforeseen effects that increase the vulnerability to cyberattacks. Power companies are now much more interconnected than previously, which not only provides more points of entry for an attacker but also means that potential damage may be more widespread. Open (as opposed to proprietary) operating systems and communications protocols have been successfully designed and deployed to improve ease of use, but they may have made the task of a cyberintruder easier as well. And remote access systems, such as those used to monitor field data and revise set points for relays, may have opened new portals for cyberintrusion.

Changing business practices may also inadvertently open new opportunities for cyberintrusion. For example, an increasing number of businesses—including utility companies—are turning to third-party vendors to provide day-to-day administrative or service functions such as payroll, accounting, and maintenance. As a result, a power plant's operating control system may have direct communication links to a vendor-managed purchase/selling function, such as procurement or billing. But the vendor's computer system may not be as strongly protected from the outside world as the utility's heavily firewalled control room, providing an easier point of entry for hackers or computer viruses. After gaining access to the utility through this "back door," the intruder may be able to move to more critical areas of the plant, unbeknownst to the utility company.

These and other emerging concerns prompted EPRI to add computer-based threats to its portfolio of security R&D. This focus on cybersecurity had its beginnings in the development of the first utility open-systems architecture—the utility communications architecture (UCA), used to share data between various computer systems in a company—and was strengthened after the highly successful program to prepare utility computer systems and equipment for the Y2K transition. Growing concern over the possibility of computer-based

Glossary of Cyberattack Terms

Bot-network operators: Cyberhackers who, instead of breaking into systems for the challenge or bragging rights, take over multiple systems in order to coordinate attacks and distribute phishing schemes, spam, and spyware/malware attacks.

Criminal groups: Cyberattackers that seek to attack a system or digital network for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud.

Foreign intelligence services: Offshore cyberattackers who use cybertools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.

Hackers: Cyberattackers who break into computer communication networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption that can cause serious damage.

Insiders: Disgruntled individuals within an organization who manipulate computer systems for revenge or personal gain. Insiders may not need a great deal of knowledge about computer intrusion because their knowledge of a target system often allows them to gain unrestricted access to cause damage or steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.

Phishing: A cyberattack method that uses e-mails and Web sites that are designed to look like those of well-known legitimate businesses or government agencies in order to deceive internet users into disclosing their personal data for criminal purposes, such as identity theft and fraud.

Phishers: Individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.

Spammers: Individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).

Spyware/malware: Software designed with malicious intent. Authors, individuals, or organizations can carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

Terrorists: Individuals or organizations that seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, or damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Even so, a well-coordinated attack on key high-voltage substations and control centers could disrupt power delivery to a large region.

security breaches led to development of EPRI's Energy Information Security (EIS) program in 2000. EIS was designed to provide tools that individual utilities could use to enhance their own security programs, including cybersecurity awareness training, information sharing, approaches to assessing control system vulnerability, and risk management protocols.

The EIS program has already produced valuable results. When vulnerabilities were discovered in standard communications protocols, such as those specified in UCA, EIS researchers developed enhancements designed to increase cybersecurity. Early exploratory work has also been conducted on fast encryption and instruction detection technologies to protect data and control systems and provided basic procedures for enhancing network security.

PowerSec: A Coordinated Approach

Much progress has been made through the ISI and EIS programs. But considering the complexity of the nation's power infrastructure, the ever-increasing capability of cyberattackers, and the diverse nature of current security efforts, a more comprehensive, highly coordinated effort is clearly required. The response—developed in cooperation with several industry organizations—was a proposal for an industry-wide cybersecurity program, which was based on existing security work at various utility industry and government organizations and feedback from more than 60 utilities, representing private and public segments of the electric power industry. As a result, an alliance has been formed to create the PowerSec Initiative, which will bring together EPRI staff, a variety of industry organizations, and several industry experts to address the cyberthreat issue as it could impact electric utility operational and control equipment.

By examining threats, vulnerabilities, and potential consequences, the PowerSec Initiative will evaluate the industry's current cyberattack readiness, identify gaps in this readiness, and specify existing best practices for filling these gaps. For some types of cyberattacks, current utility cyberattack readiness is quite good, whereas for other types of cyberattacks, even current best practices will not be sufficient. Therefore, the work in this area will also identify vulnerabilities that require new solutions and specify what R&D work is needed to develop and test potential solutions.

One important goal of PowerSec is to consolidate and leverage ongoing and completed cybersecurity work from utilities, government, regulatory agencies, and others. Appropriate information on best practices will be disseminated to the industry using methods consistent with safeguarding confidential or classified information. In addition to integrating and sharing disparate information, the PowerSec Initiative will serve as a model of how the utility industry, regulators, and government can work together to solve complex security problems.

The PowerSec Initiative will focus first on electric utility supervisory control and data acquisition (SCADA) systems and energy management systems (EMS), both of which have been identified by experts as critical cybersystems to secure. Identifying and filling existing security gaps in communication and control systems will make it more difficult for potential intruders to gain access and cause damage. Improvements in these systems will also tend to increase overall levels of power system reliability, providing a more secure business environment for wholesale power markets and enabling utilities to offer better service to their customers.

One of the objectives for the PowerSec Initiative is to develop an overview of the electric power industry's current cybersecurity posture. From this, the initiative will provide utilities with a list of vulnerabilities for each major type of SCADA and EMS control system commonly deployed across North America and will tailor this information to reflect the particular combinations of systems in use. A comprehensive, prioritized list of viable cyberthreats will also be developed, along with the compendium of best practices with recommendations on how to maximize cybersecurity using currently available tools and methods. A compendium of current cybersecurity projects being pursued by both government and private industry will also be developed to clarify which areas are being adequately studied and which need more attention.

Together, these results will be used to identify gaps between viable threats and defenses, both current and planned. Results from this work will then lead to an action plan for developing technologies to eliminate any gaps, identified or perceived.

Clearly the first order of business for PowerSec will be to assess the vulnerability of information and control systems currently used by utilities and system operators. This work will begin with on-site interviews and inspections and will be supplemented by the evaluation of past or ongoing security analyses by individual utilities, industry organizations, and government. Researchers will also examine existing information systems to determine their cybervulnerability. Particular emphasis will be placed on examining SCADA and EMS systems to help prevent hackers from using them to take over control of critical utility equipment.

Information gleaned from the PowerSec cybervulnerability assessment process is also intended to complement ongoing

security standards development by NERC and the Federal Energy Regulatory Commission (FERC). The Urgent Action Cyber Security Standard 1200 adopted by NERC in 2003 already specifies actions to be taken to protect utility systems in 16 areas, such as access control, information protection, personnel training, incident response, and recovery planning, among others. This standard, which was originally adopted as a temporary measure, has been extended and modified for development into a set of permanent cybersecurity standards: CIP-002 through CIP-009.

PowerSec's assessment phase—expected to take about a year—will provide an objective assessment of the industry's cybersecurity. If significant security gaps are identified, approaches to resolve/mitigate these vulnerabilities will be proposed.

The effectiveness of PowerSec results will be evaluated using independent test-bed exercises at the Idaho National Laboratory and Sandia National Laboratory, as appropriate. These facilities are capable of testing new tools on a variety of SCADA and other cybersystems provided by manufacturers. Evaluations will also be conducted at individual utilities. The PowerSec team will use the confidential results of these evaluations, together with feedback from the deployment process, to revise vulnerability assessments and enhance the alert system by adding new attack mitigation actions.

The Future

Feedback from utility executives during the formulation of the PowerSec Initiative revealed that utilities believe they have made considerable progress toward protecting their own cybersystems but recognize that key vulnerabilities remain across the industry as a whole. The executives generally believe that cyberattacks are likely, from domestic and/or international terrorists, and that disgruntled past or present employees also represent a potentially dangerous threat. They also say that PowerSec should ultimately address a combination/hybrid response to cyber and physical threats and vulnerabilities, because successful physical attacks may involve very long recovery times. An area of particular concern is how to ensure the availability of spare parts for long-lead-time equipment.

The PowerSec Initiative will help participants move quickly up the learning curve about cybersecurity risks and vulnerabilities and will give them enhanced capabilities to assess cyber-related threats on their own systems. Access to government and regulatory thinking on security issues should also help participants better prepare for potential changes in cyberregulations that impact utilities. The biggest issue today is the incomplete and anecdotal aspects of the situational data available. Such uncertainties prevent utilities from positioning themselves effectively for dealing with cybersecurity issues. A more comprehensive understanding of the situation will allow PowerSec participants to better allocate financial and personnel resources to security preparedness. Ultimately, it is hoped that PowerSec will help focus future government cybersecurity regulations, spur the development of innovative mitigation tools and methods, and promote enhanced cybersecurity preparedness by the industry at large.

But if continued attacks on the grid are inevitable, as many industry leaders believe, prevention will only be part of the answer to grid security concerns. A lot of smart people are working on this problem, but the field of opportunity for intrusions is very broad. Electric utilities should thus assume that sooner or later an intruder will succeed in breaching their cyberdefenses. This is why a long-term program for increasing overall system resiliency becomes crucial. If a hacker or terrorist does manage to compromise a transformer or power line, the grid must be able to withstand the loss without the danger of wide-area cascading outages. EPRI's IntelliGrid Consortium—another industry-wide initiative—is working on adaptive, self-healing technologies that can be built into the nation's power delivery system to provide just such resiliency.

The industry is clearly entering a new phase of security consciousness. Some individual utilities have already done a lot to protect their own cyber and physical systems against terrorist attacks, and now the time has come to expand this work through coordinated, industry-wide efforts. If successful, the payoff will be large indeed. With PowerSec reducing the probable success of attacks and IntelliGrid features limiting the scope of their effects, tomorrow's power grid will have every potential to meet the challenges of the post-9/11 world.

For Further Reading

"Security vulnerability self-assessment guidelines for the electric utility industry," EPRI, Palo Alto, CA, Rep. 1001639, Dec. 2002.

"Guidelines for detecting and mitigating cyber attacks on electric power companies," EPRI, Palo Alto, CA, Rep. 1008396, Mar. 2004.

A.M. Sauter and J.J. Carafano, *Homeland Security*. New York: McGraw-Hill, 2005.

Biographies

Robert Schainker is a technical executive and manager of the Security Program Department at the Electric Power Research Institute. He received his D.Sc. in applied mathematics and control systems, his M.S. in electrical engineering, and his B.S. in mechanical engineering at Washington University in St. Louis, Missouri.

John Douglas is a consultant to the Electric Power Research Institute and other leading electric power organizations. He received a B.S. in physics from Vanderbilt University, Nashville, Tennessee, and an M.S. in physics from Cornell University, Ithaca, New York. Also, he holds an M.J. degree in science writing from the University of California at Berkeley, California.

Thomas Kropp is a security infrastructure project manager within the Security Program Area at the Electric Power Research Institute. He received a B.S. in mathematics at Santa Clara University and an M.A. in mathematics at the University of California at Davis.