WHITE PAPER: ENTERPRISE SECURITY SERVICES

Best Practices for Securing SCADA Networks and Systems in the Electric Power Industry

White Paper: Symantec Enterprise Security Services

Best Practices for Securing SCADA Networks and Systems in the Electric Power Industry

Contents

Executive summary

Electric power deregulation and business initiatives demand real-time information, driving more interconnections between control systems and public networks every year. Interconnection delivers important business benefits, but without appropriate security measures, it can compromise control system availability and cause service disruptions.

Proprietary protocols, applications, and private networks have shielded core distributed control systems (DCS), energy management systems (EMS), and supervisory control and data acquisition (SCADA) systems in the past. But interconnections create openings, and hackers know it. At the recent International Electrotechnical Commission (IEC) working group 15 meeting, the Idaho National Engineering and Environmental Laboratory (INEEL) disclosed that the Inter-Control Center Communications Protocol (ICCP) was a growing topic of discussion in the hacker underground. The industry is aware of the risk and is responding with increased awareness, new security initiatives, and cyber security standards like North American Electric Reliability Council (NERC) 1200 and 1300.

Existing security measures are not enough. Firewalls do not stop blended threats, like worms, and desktop antivirus solutions do not protect networks. Nor do such solutions monitor or protect specific SCADA protocols like ICCP. General IT security products, untested in control center environments, can even degrade performance and bring down the systems they're supposed to protect.

To address this gap, Symantec has collaborated with leading SCADA vendors on solutions to secure interconnections with control networks—and validated them with independent parties to assure protection without disruption. This paper summarizes information security needs and targeted solutions for control systems in this industry. In particular, the paper focuses on commonly used EMS and SCADA systems and one of their primary communications protocols: ICCP. Best practices for securing these networks/systems include a range of measures and technologies that can be broadly grouped under the umbrella of the need to Understand, Act, and Control:

- **Understand.** Understanding the problem involves conducting security and risk assessments, creating effective security policies, and implementing early warning systems.

- **Act.** Taking action involves implementing integrated solutions at the gateway, network, and client levels.
- **Control.** Maintaining ongoing control involves measuring and improving security policy compliance, patch management, and managed security services.

Business drivers of cyber security

Changes resulting from electric power industry restructuring have increased the need for heightened information security in this industry. For example, the mandate of open access to transmission systems by the Federal Energy Regulatory Commission (FERC) has led to a dramatic rise in the number and complexity of wholesale power transactions. Coupled with a decrease in construction of new generation facilities and transmission lines and rising electric demand in the last two decades, this mandate has indirectly led to operation of the power delivery system much closer to its limits. This inherently increases the sensitivity of the power system to any sort of cybersecurity threat because the potential impact of equipment failure due to a security breach is magnified. At the same time, the sensitivity of electric loads has increased; microprocessor-based assembly lines and computer equipment are highly sensitive to even momentary interruptions of power. Again, this intensifies the potential impact of a power interruption due to a security breach.

Some aspects of restructuring have also led to the need for more extensive communication and data exchange between various power system operating entities, power generators, and other stakeholders. This growth increases the number of network access points that need to be secured. These changes have also led to the interconnection of corporate networks and power system control networks. The advances in information management that this interconnection affords yield a range of benefits, yet in many cases, these joined networks are inadequately protected.

There are three primary drivers for this interconnection of networks. First, the demand for remote access computing has encouraged many utilities to establish connections that allow engineers to monitor and control the power system from the corporate network. Second, many utilities have added connections between corporate networks and control networks in order to allow corporate decision-makers to obtain instant access to critical data about the status of their operational systems. Third, partner companies, regulators, and financial exchanges often require real-time access to power system data, which is facilitated by linking these two networks.

A recent regulatory development that heightens the urgency for cybersecurity measures is the Sarbanes-Oxley Act of 2002 (SOX). Enacted in the wake of various accounting scandals, SOX requires companies to certify the effectiveness of their information technology and financial controls when they file certain financial reports. This means that compliance with this act involves the need for accurate information. Yet, without proper security practices, company officials are unable to confidently sign off on these reports or controls. SOX also requires public disclosure in the event of revenue flow disruption as a result of a cyber incident. Because such disclosure could reduce customer confidence (and investor confidence, in the case of investor-owned utilities), reducing security risks is a high priority.

In a second key regulatory development, on August 13, 2003, NERC voted to adopt the Urgent Action Standard 1200 for Cyber Security.[1] This is the first-ever standard to protect electric utilities' computers, software, and networks from cybersecurity incidents, such as viruses, worms, and attacks. Initially intended as a one-year temporary standard that would be replaced by permanent standard 1300, standard 1200 has been extended to August 13, 2005. Standard 1200 establishes procedures in 16 different areas (e.g., security policy, perimeter, access control, training, incident response, and recovery) that are designed to protect energy companies from malicious attacks. Corporate officers for all electric utilities in North America must sign off on complete adherence to this comprehensive standard by March 2005.

Critical nature of SCADA systems

Utilities and other power system operators, such as independent system operators (ISOs) and regional transmission organizations (RTOs), deploy SCADA systems in order to provide centralized monitoring and control of the often far-flung network of power generation and delivery equipment that is under the purview of a particular energy control center. SCADA systems allow an energy 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 failed 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 indispensable to power system reliability and maximum staff efficiency.

[1] Symantec Corporation, Bill Campbell, *Inside the NERC Cyber Security Standard*, December 2, 2003.

ICCP is the primary protocol used to communicate information between the energy control centers that operate these SCADA systems and between control centers and power generators. In recent years, ICCP also has been used for communication between control centers and remote terminal units (RTUs) and substations. Also known as TASE.2, this application layer protocol is specifically tailored to the needs of electric utilities for the exchange of data. In addition to control centers operated by utilities and utility and non-utility power generators, other entities that use ICCP in the electric power industry include power pools, regional control centers, RTOs, and ISOs. The data exchanged typically consists of real-time power system monitoring and control data, including measured values, scheduling data, energy accounting data, and operator messages. Figure 1 illustrates ICCP traffic on a typical network.

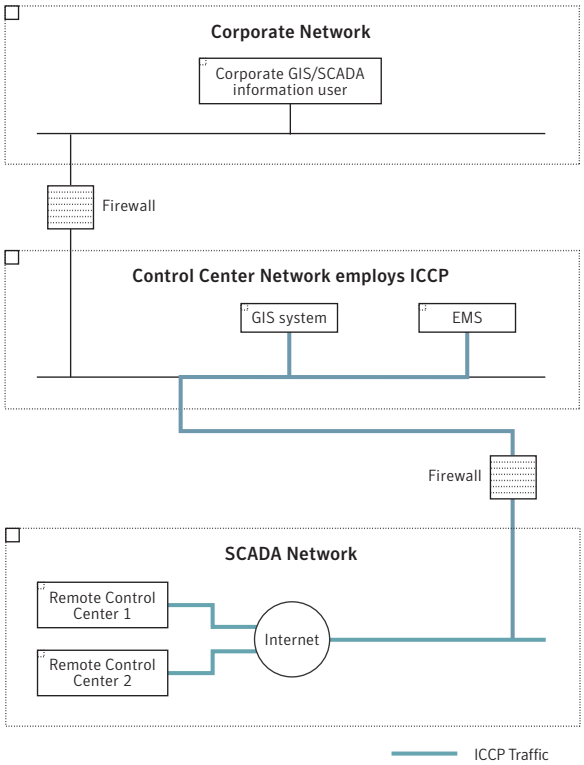

Figure 1. ICCP traffic flows across the control center and SCADA networks, while access to this traffic is often available from a corporate network.

Challenges to increasing SCADA security

Cybersecurity was not the primary consideration when SCADA networks and systems, as well as ICCP, were developed. Rather, the primary driver was the high level of functionality (and in the case of ICCP, standardization) required to enable the continued reliable operation of the power delivery system. This fact is one of the challenges the electric power industry faces today when seeking to better secure SCADA networks/systems and ICCP. Other challenges include the interconnected nature of corporate networks and control networks such as SCADA, and the division of responsibility for enhanced SCADA security between two separate groups: IT personnel and control system personnel.[2]

To support competition in product choices in the electric power industry, several standards for the interconnection of SCADA systems and RTUs have been published, as have standards for communication between control centers and other entities (i.e., ICCP). This increased availability of information describing the operations of SCADA systems increases the security risk, however. At the same time, the efforts of utility companies to make efficient use of SCADA system information across their companies have led to development of "open standard" SCADA systems. This poses security challenges because protocols such as ICCP now allow for wider access to SCADA systems, meaning that SCADA system security may be only as strong as that of the utility's corporate network.

Another challenge is the lack of awareness among electric power industry personnel of (1) the significant number of actual cyberattacks on control systems that have occurred, (2) the potential vulnerabilities of SCADA networks/systems and ICCP, and (3) the availability of strategies and solutions that can help mitigate these vulnerabilities. Numerous attacks on control systems in the electric power industry have been reported. For example, a March 2004 General Accounting Office (GAO) report on "Challenges and Efforts to Secure Control Systems" summarized such attacks, including a computer system breach at the Salt River Project as early as 1994. More recently, a hacker attack was mounted on a developmental network at an ISO in 2001, and a Microsoft SQL Server worm known as "Slammer" disabled a safety monitoring system for several hours at the Davis-Besse nuclear power plant in Ohio in late 2003.[3] These attacks, though relatively minor in scope and damage, illustrate the potential for malicious cyber activity in the control networks or systems of the electric power industry.

[2] Symantec Corporation, *Information Security Challenges in the Electric Power Industry,* 2003.
[3] United States General Accounting Office, Report to Congressional Requesters, *Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems,* GAO-04-354, March 2004.

SCADA and ICCP vulnerabilities

Recognizing the critical need for increased security of SCADA networks and systems, Symantec is working with SCADA industry leaders to define more specifically the types of vulnerabilities that exist in SCADA systems and, in particular, systems that use ICCP. In one such recent study conducted by Battelle's Pacific Northwest Division and in partnership with Areva, a leading EMS provider, the following key vulnerabilities that are relevant to ICCP were identified:[4]

- Intruders could gain unauthorized access to the control center network (e.g., the ICCP server) via overlooked key access points (e.g., via dial-up remote network access, connections to partner networks that are not secured, or access via unsecured networks in the relatively rare instances in which they are used for ICCP). See figure 2 for more information.
- Disgruntled employees could pose a wide range of threats (e.g., authorization violations, in which an authorized user gains access to the control center and SCADA networks via the corporate network for an unauthorized purpose). See figure 3 for more information.
- An intruder could initiate a denial-of-service attack by sending repeated information requests that "lock up" an ICCP server, preventing the server from performing legitimate operations and serving legitimate users.
- Viruses or worms could infect the ICCP server or other devices, and perform malicious activities such as emailing critical information to another host for retrieval by a hacker.
- Packet sniffing at end points of communication (e.g., the ISP or carrier) could enable packet modification with malicious intent.

While this is not a comprehensive list of vulnerabilities, it serves to illustrate the type of vulnerabilities that could be exploited to a malicious end. A "war game" that Gartner and the U.S. Naval War College conducted in 2002 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.[5] 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."

[4] Battelle Pacific Northwest Division, *Evaluation of Symantec Security Products in an AREVA T&D-Implemented SCADA Environment using ICCP Communication Servers*, S. Katipamula, M.D. Hadley, and T.P. McKenna, prepared for Symantec Corporation, May 2004.
[5] Gartner Research, *Prepare for Cyberattacks on the Power Grid*, October 2002.

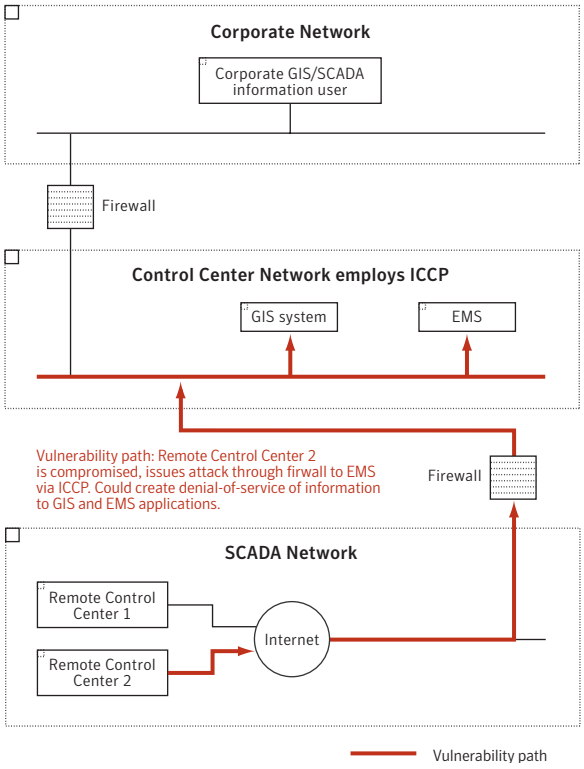

Figure 2. One vulnerability path involves remote access to the SCADA and control center networks.

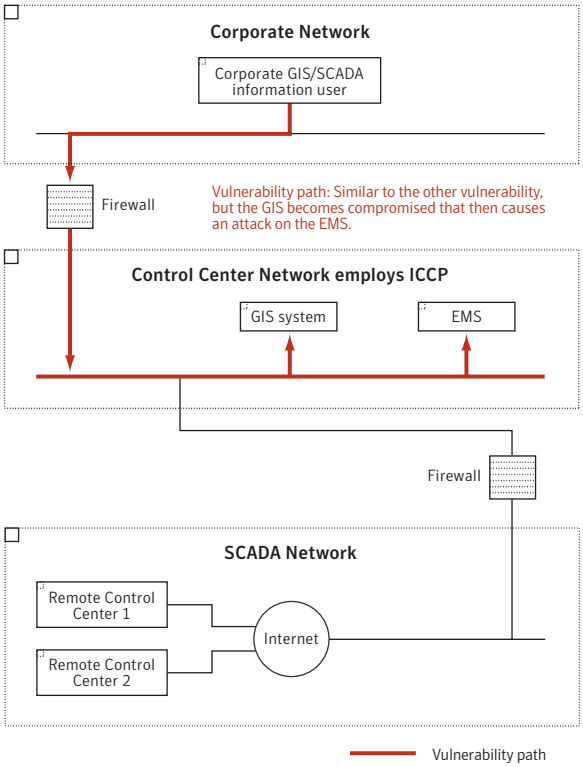

Figure 3. A second vulnerability path involves access to the SCADA and control center networks via the corporate network.

Firewalls are not enough

Taking action to respond to vulnerabilities and proactively securing networks and systems requires much more than implementing firewalls. Many utilities deploy perimeter firewalls to control the traffic entering and leaving their networks, thereby providing a first line of defense against external attacks. Another common measure is the deployment of firewalls between the corporate and control networks. Some security administrators believe that these firewalls provide sufficient protection across the utility. However, firewalls can offer a false sense of security: Many firewalls simply allow or disallow certain types of traffic at each port. In order to secure these ports, companies need more than a firewall—they need security measures that recognize anomalies in IP traffic caused by abnormal ICCP traffic or other protocol traffic. These measures would ideally have vulnerability signatures for these specific protocols, which would trigger alarms if these vulnerabilities are exploited.[6]

[6] Symantec Corporation, *Symantec Internet Security Threat Report*, Trends for July 1, 2003–December 31, 2003, Volume V, published March 2004.

Another major reason that firewalls alone do not offer sufficient protection is that the network perimeter is no longer easily discernible. Companies once clearly defined "insiders" from "outsiders"; now utility control centers must enable collaboration and open communication with other control centers, power generators, contractors, and remote employees. Thus, attacks can be either unknowingly or maliciously perpetrated by those with legitimate network access. In fact, according to a recent CSI/FBI Computer Crime and Security Survey, one-third of network attacks are perpetrated by individuals inside the traditional firewall. Attacks could include integrity violations (i.e., unauthorized information creation or modification), authorization violations (in which an authorized user gains access for an unauthorized purpose),intercept/alter (in which a packet is intercepted, modified, and forwarded), eavesdropping (i.e., data confidentiality is compromised via monitoring), and others.

Traditional firewalls also cannot protect against blended threats (i.e., threats that combine characteristics of hacking, denial-of-service attacks, and worm propagation). According to the Symantec Internet Security Threat Report issued in March 2004, blended threats represented 54 percent of the top ten submissions during the second half of 2003.8 Traditional firewalls can even become the launch point for an attack.

Best practices for securing SCADA networks and systems

Best practices for protecting SCADA and ICCP against these vulnerabilities can be grouped according to the measures of "Understand, Act, and Control."[7]

Understand means gathering knowledge about the information environment, both inside and outside of the organization. This includes awareness of electronic threats emerging anywhere in the world before they reach the organization, identifying possible regulatory compliance issues, assessing the effectiveness of security and administration tools, and constantly monitoring the status of network and system assets.

Act is about deploying security measures and responding successfully to vulnerabilities; securing devices, applications, and networks against threats before they happen; and taking steps to ensure that information is up-to-date, compliant, and restorable. It also involves recovery procedures and tools in the event that an attack eludes other security measures.

Control is about managing information resources to prevent disruptions and minimize downtime. That means provisioning new applications, managing software patches, and taking other steps to keep networks up, running, and growing. Table 1 summarizes various

[7] Symantec Corporation, *Understanding SCADA System Security Vulnerabilities,* 2004.

recommended best practices and corresponding Symantec solutions. Figure 4 illustrates potential locations for implementation of various Symantec solutions on utility corporate, control center, and SCADA networks.

Table 1. Summary of Recommended Best Practices to Secure SCADA Networks and Systems

Best Practice	Description	Symantec Products
Understand		
Security/risk assessment	Periodic security and risk assessment services, corporate network vulnerability assessments, incident forensics, and penetration testing	SCADA Security Assessment Services
Policy creation	Security policies that address who is authorized to gain access to what information, who is authorized to perform what functions, and procedures that authorized parties must follow to ensure effective security	Symantec Professional Services
Policy enforcement	Means to measure the current state of security, compare it with the state needed to comply with regulations and security standards, and recommend measures to accomplish such compliance	Symantec Enterprise Security Manager™ software
Early warning	The ability to gain early insights into upcoming threats that could affect corporate networks and may spread to SCADA systems	Symantec DeepSight™ TMS and Alert Services
Act		
Beyond firewalls: Integrated Gateway Security	Network gateway solution that employs firewall, intrusion prevention and detection, virus protection, content filtering, antispam, and virtual private network technology	Symantec™ Gateway Security
Network security	Network-based intrusion detection technology that uses protocol anomaly detection	Symantec™ Network Security
Client security	Client-based protection against worms, viruses, Trojan horses, and blended threats for all clients, including remote and mobile employees, contractors and partners, and others	Symantec™ Client Security software

Table 1. Summary of Recommended Best Practices to Secure SCADA Networks and Systems (cont.)

Best Practice	Description	Symantec Products
Control		
Policy compliance	Measure compliance, subsequently implement ways to improve compliance in problem areas, and comply with legislative requirements imposed by Sarbanes-Oxley and the NERC Cyber Security standard 1200 (and upcoming standard 1300)	Symantec Enterprise Security Manager software
Patch management	Alleviate intrusions that result from vulnerabilities for which patches exist and that have been tested and validated by an EMS vendor and the utility's laboratory via an automated patch management process	Symantec ON *i*Patch™, Symantec *i*Command™, Symantec Professional Services
Backup and disaster recovery	To ensure business continuity, perform non-intrusive, real-time backups and perform truly rapid disaster recovery when needed. Whether equipment failure forces you to do a bare-metal restoration, or you need to recover from a virus attack, or if the problem is just the accidental loss of an important file, disaster recovery solutions will significantly reduce the pain point of getting back up and running.	Symantec LiveState™, Symantec Professional Services
Managed services	24x7 centralized management and monitoring of protection technologies along with early warnings, incident response, and decision support to ensure that all security devices are configured properly and fully patched, monitor actual activity on each device, and detect malicious activity in real time	Symantec Managed Security Services

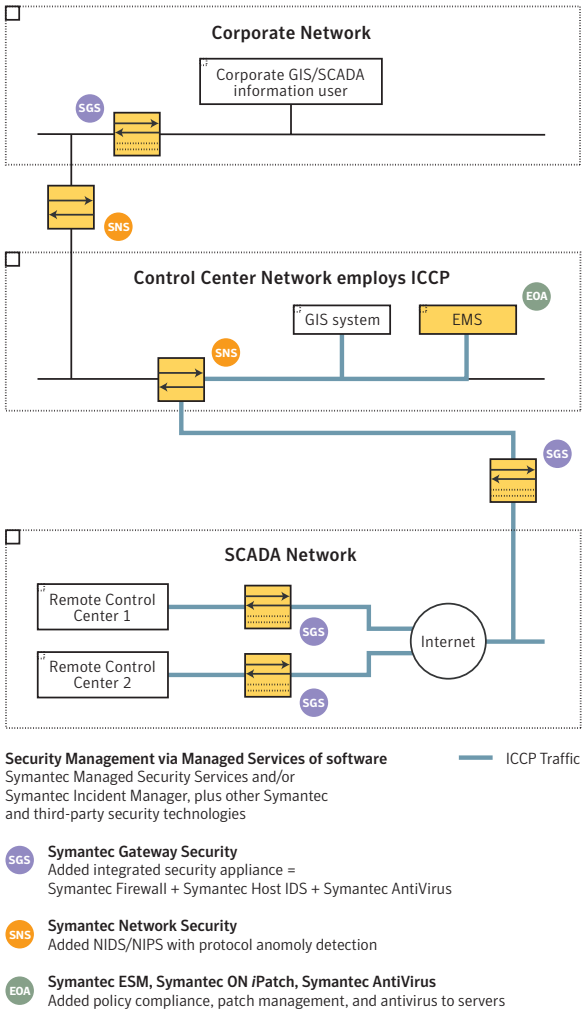

Figure 4. Symantec solutions enable utilities and other stakeholders in the electric power industry to implement recommended best practices to secure SCADA networks and systems.

Understand: Security/risk assessment

Understanding the information environment begins with the assessment of the vulnerabilities of SCADA networks and systems on a recurring basis. Such security and risk assessment is complicated by the large number of applications installed on these networks. Another complexity involves the interconnection of corporate networks and control networks; each type of network exposes a unique set of vulnerabilities, all of which must be assessed. Hence, corporate networks, Web

servers, and customer management systems should also be assessed to reveal unintended gaps in security, including unknown links between public and private networks, and firewall configuration problems.

One key part of security assessment is penetration testing. The "always on" nature of control networks complicates such testing. This effectively rules out use of traditional IT security assessment companies with little or no experience conducting penetration testing in SCADA environments.

An overwhelming number of security technologies, networking devices, and configuration options are available to utility companies. While firewalls, intrusion detection systems (IDSs), virtual private networks (VPNs), and other technologies can all help protect control networks from malicious attacks, improper configuration and/or product selection can seriously hamper the effectiveness of any security posture. Due to this complexity, and the often overtaxed nature of system operators and other utility IT personnel, many utilities are likely to benefit from the services of independent consultants in this area. Such independent assessments can help ensure that evolving SCADA and corporate network architectures do not compromise network security, while addressing vulnerabilities such as hacker attempts to bypass controls, attempted denial-of-service attacks, and many others.

Based on years of experience in this sector, Symantec Security Professional Services offers SCADA security and risk assessment services, corporate network vulnerability assessments, incident forensics, and penetration testing to help customers in the electric power sector develop more robust information security infrastructures, processes, and programs. Symantec professionals work with operations, engineering, and IT personnel to understand everyday operations, procedures, processes, policies, workflows, systems, and applications before conducting penetration testing. Based on the knowledge gained during this research, as well as the experience gained from working with many customers in the electric power industry, Symantec's service ensures optimal security assessment without disrupting control systems and networks.

Understand: Policy creation and enforcement

The foundation of effective security best practices is a comprehensive, well-conceived security policy. For the control systems used by electric utilities and other power system operators, security policies must address issues of who is authorized to gain access to what information, and who is authorized to perform what functions, as well as procedures that authorized parties must follow to ensure effective security. Such policies are particularly important for

the control of access by parties outside of the control center (e.g., other control centers, power generators, remote employees, contractors, and others). Hence, electric utilities need a policy compliance tool that measures the current state of security, compares it with the state needed to comply with regulations and security standards, and recommends measures to accomplish such compliance. At Symantec, this function is provided by the Symantec Enterprise Security Manager solution.

Understanding: Early warning

The "understand" component also involves early warning—the ability to gain early insights into upcoming threats that could affect corporate networks and spread to SCADA systems. Early warning is key to maintaining business continuity. Receiving early, detailed alerts of potential attacks allows utilities to efficiently prioritize tasks and deploy internal resources to keep the power flowing. The Symantec DeepSight Threat Management System tracks security on a global basis, providing early warning of active attacks specific to customers' systems and applications. With personalized notification triggers, expert analyses, and industry-specific reporting capabilities, it enables utilities to prioritize IT resources in order to better protect critical information assets against a potential attack.

Act: Firewalls are not enough

Utilities need a solution at the network gateway that employs more than firewall technology. The Symantec Gateway Security solution, for example, offers full-inspection firewall technology, protocol anomaly–based intrusion prevention and intrusion detection engines, award-winning virus protection, URL-based content filtering, antispam technology, and IPsec-compliant virtual private networking technology with hardware-assisted high-speed encryption. This appliance provides strong security at the gateway between the Internet and the corporate network or control network, or between network segments.

Act: Network security

As a complement to the gateway security described above, utilities also need network security. Because an intrusion detection system is a vital element of effective network security for utilities, the President's Critical Infrastructure Protection Board has recommended it as a component of electric utilities' overall security strategies. Intrusion detection systems offer real-time analysis and correlation of traffic flowing across a network. Due the highly repetitive

pattern of traffic flowing over networks using protocols such as ICCP, protocol anomaly detection is feasible in utility control centers. One example of a solution in this area is Symantec ManHunt™, which provides high-speed network intrusion detection, real-time analysis and correlation, and proactive prevention and response to defend against internal and external intrusions and denial-of-service attacks.

Act: Client security

In the client security area, inadequately protected networked, mobile, and remote users are at risk of infection by worms, viruses, Trojan horses, and in particular, today's blended threats, which are highly sophisticated combinations of single threats. Remote and mobile employees, contractors, and partners, for example, may unknowingly introduce these threats to the corporate network and, as a result, to the interconnected control network. These users can also serve as a potential conduit for hackers and unauthorized users to gain access to the corporate and control network. As a result, the desktop and laptop computers of system operators, local personnel accessing the corporate network, and remote users need comprehensive protection. Symantec Client Security, for example, provides threat protection through integrated antivirus, firewall, and intrusion detection for remote, mobile, and networked client systems.

Control: Policy compliance

In addition to security policy definition as part of the "understand" component, policy compliance during the "control" phase is equally important. Utilities need to measure compliance, subsequently implement ways to improve compliance in problem areas, and comply with legislative requirements imposed by Sarbanes-Oxley and the NERC Cyber Security standard 1200 (and upcoming standard 1300). Symantec Enterprise Security Manager provides comprehensive, policy-based security assessment and management. Using templates based on the NERC Cyber Security standard and Sarbanes-Oxley, it provides a solid foundation for electric utilities to begin implementing the NERC standard and measuring their ability to adhere to it.

Control: Patch management

Software vulnerabilities resulting in security weaknesses can leave utility corporate and control networks and systems unprotected and open to misuse by unauthorized parties, such as computer hackers. A report by the CERT Coordination Center at Carnegie Mellon estimates that

almost all reported intrusions result from vulnerabilities for which patches exist. Although these patches are available on software developers' Web sites, the task of applying patches is often perceived as time-consuming, expensive, and complex, or as a low priority. Yet, with the number of threats on the increase, and security and software fixes being released more frequently than ever before, the implementation of a reliable patch management solution has become a critical component of a utility's overall lifecycle management plan.

On utility control networks and systems, such as SCADA systems, patch management is complicated by the inability to remove critical systems from service, without taking careful measures to avoid any impact on power system reliability. In contrast to corporate networks that are typically unused for some portion of each day, SCADA systems operate 24 hours a day, 7 days a week. There are two complementary approaches to solving this problem: (1) focusing on hardening perimeter, network, and host security; and (2) implementing a centralized patch management solution.

While earlier sections address the first approach, solutions such as Symantec ON *i*Command and Symantec ON *i*Patch provide utilities with the tools to help automate the otherwise tedious patch management process. Symantec ON *i*Patch, for example, can determine the patch status of a SCADA system, identify missing security patches, and automatically install them on individual computers or groups of computers, or across the entire organization simultaneously.

Control: Managed services

As utilities deploy network security technologies throughout their networks, the challenge of properly managing and monitoring these resources is becoming increasingly complex. Unfortunately, the implementation of "technology-only" solutions without close monitoring and management significantly weakens the effectiveness of security devices. Hiring experienced IT security professionals to monitor network security devices can help to mitigate risk; however, this option is cost-prohibitive for most, if not all, utility companies. Additionally, most IT teams do not work 7 days per week, 24 hours per day, which is a requirement in the utilities space. At the same time, control center personnel must focus on their system operation duties and are typically not trained in the nuances of effective security monitoring and management. As a result, many organizations are using third parties that have experience in providing 24x7 management and monitoring of security devices to highly specialized, managed security companies in the utilities environment.

Via its Managed Security Services, Symantec currently manages the security infrastructures of several leading U.S. electric utilities. This service provides 24x7 centralized management and monitoring of protection technologies along with early warnings, incident response, and decision support. The services ensure that all security devices are configured properly and fully patched, and monitor the actual activity on each device to detect malicious activity in real time. For power system operators that seek an enhanced level of control over their security operations, Symantec's solution provides control center operators with a view of the same data that Symantec views, enabling in-house analyses as well. For utilities with established policies that preclude the use of managed services but that have significant in-house resources, Symantec™ Security Management Systems offer an alternative solution.

About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com

01/05 10354494