WHITE PAPER: ENTERPRISE SECURITY

Effective Practices for Meeting NERC Critical Infrastructure Protection Requirements in the Electric Power Industry

White Paper: Symantec Enterprise Security

Effective Practices for Meeting NERC Critical Infrastructure Protection Requirements in the Electric Power Industry

Contents

Executive Summary

Improving cyber security in the electric power industry is challenging for several reasons. SCADA/EMS and DCS systems were initially designed with efficiency and reliability, rather than security, in mind. These systems are increasingly being integrated with business information systems, introducing new vulnerabilities. At the same time, control system technologies are becoming more standardized, increasing the availability of information on potential vulnerabilities. Lack of 24/7 security expertise in energy control centers compounds the problem.

In recent years, the need to maintain or enhance power system reliability has driven increased security. And today, the need for security is formalized as a regulatory requirement in the form of approved wide-ranging cyber-security requirements known collectively as NERC CIP. This paper outlines effective practices for complying with NERC CIP.

Achieving compliance with NERC CIP requires a range of solutions as part of an ongoing process with a phased rollout. Collaboration between engineering, operations, and IT departments is crucial. Investment in new security products may not be initially needed; instead the recommended compliance process begins with an initial risk assessment, which includes an initial discovery/review of the current security posture through a series of security assessments and penetration tests of the perimeter and internal SCADA/EMS and DCS environments. Based on the results of this first step, security policies are then created, disaster recovery planning is conducted, and protective measures (i.e., both security and disaster recovery measures) are deployed that enable compliance with these policies. Ongoing monitoring and maintenance completes the recommended five-step process. After covering these high-level approaches, this white paper then summarizes effective practices for compliance with each of the eight standards in the NERC CIP.

Challenges to Improving Cyber Security

Because efficiency and reliability were the primary drivers of SCADA/EMS and DCS design, many of these systems lack even basic security mechanisms, especially when compared with today's standard business information systems. In keeping with this focus, system operators have adopted a number of practices to improve operational efficiency, many of which also tend to increase the vulnerability of control systems to cyber attacks.

For instance, most SCADA/EMS and DCS systems are interconnected with existing business information systems. This interconnectivity is required to provide utility corporate decision-makers with access to critical data about the status of their operational systems, as well as to enable onsite access to corporate computing networks by visiting employees and contractors via laptop computers—which are often unsecured. At the same time, company engineers, contractors, and others require remote access to plant/power system control systems via modem or other means to maintain 24x7 operations. Unfortunately, this access introduces additional vulnerability points and could lead to the unleashing of viruses or malicious code within the control systems. At the same time, the nonstop operational requirement of utility control systems complicates security implementation and testing because systems can never be taken offline.

The drive to improve operational efficiency and drive costs down is also leading to increasing standardization of control system technologies and use of off-the-shelf IT technologies. SCADA/EMS and DCSs are increasingly implemented on Microsoft Windows and Linux operating system-based platforms. Similarly, many of these control systems use IP and the Inter-Control Center Communications Protocol (ICCP, which enables communication between control centers, often between different utilities) the protocols of major manufacturers of programmable logic controllers (PLCs) and remote terminal units (RTUs). In parallel with this standardization trend, technical information about these standards is becoming increasingly available in trade journals and from online information sources, enabling would-be attackers to identify vulnerabilities that can be used to attack SCADA/EMS and DCS systems.

Another complexity is the shortage of security resources in key areas of the electric power industry—for example in energy control centers. Most control centers are not staffed 24/7 with IT and security experts, and such staffing would not be economically feasible. This complicates interpretation of security logs and other activities related to maintaining security around the clock.

The Evolution of NERC Standards

While these complexities pose challenges to enhancing security in the electric power industry, the need for security has never been more acute. The need to maintain or enhance power system reliability and availability drives increased security. Stated another way, security is a business enabler for reliability and availability in the new interconnected environment.

And today, the need for security is now formalized as a regulatory requirement. NERC has approved wide-ranging cyber-security guidelines ("NERC CIP") to replace narrower, temporary precautions adopted in 2003 as the NERC Cyber Security Standard 1200 (and renamed the NERC Cyber Security Standard 1300 in 2004). NERC CIP is the first set of comprehensive requirements to protect electric utility assets from cyber security attack. Compliance will be enforced by Energy Reliability Organization (ERO). NERC was designated as the ERO in July, 2006. Refer to www.nerc.com for more information.

Most electric power utilities have already achieved compliance with NERC Standard 1200 and are currently planning compliance with NERC CIP. NERC CIP covers the same areas covered by the NERC 1200 Standard, but with some important differences. Major changes from 1200 to CIP include power generation is now being covered; new security areas now covered such as disaster recovery, patch management, and different types of policy compliance, enforcement, and practices.

NERC CIP identifies the minimum requirements to implement and maintain a cyber security program and to protect cyber assets critical to reliable bulk electric system operation. It is divided into the following eight separate reliability standards:

- CIP-002: Critical Cyber Asset Identification
- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeter(s)
- CIP-006: Physical Security
- CIP-007: Systems Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for Critical Cyber Assets

Measurement and accountability are key features of the NERC CIP standards, with each standard requiring an audit to achieve compliance and senior management approval. For NERC CIP, each responsible entity must participate in an annual compliance check and the compliance monitor must keep audit records for three years.

Overview of NERC CIP Compliance Approaches

No single product or service will enable NERC CIP compliance; many different areas must be addressed using a range of solutions. Similarly, NERC CIP compliance cannot be obtained in a short period of time, as a one-time initiative. NERC CIP compliance is best achieved via an ongoing process that involves a phased rollout. Asset owners first identify security gaps, prioritize needs, and gradually implementing measures. In addition to enabling a focus on critical vulnerabilities early in the process, this approach aids budgeting and funding processes.

Collaboration between engineering, operations, and IT departments in a utility is needed to identify gaps and to effectively implement corrective measures and to effectively implement these. The reason is that NERC CIP requires one executive to be designated as responsible for compliance. Assuming this responsibility requires authority across different organizations.

Investment in new products may not be initially needed to enable NERC CIP compliance. Existing firewalls, antivirus software, intrusion detection systems, and other systems that DCS/SCADA vendors have already validated for proper functioning in the existing environment may do the job. Instead of replacing these products, the NERC CIP compliance process can begin with an initial review of architecture and policies, creation of new or revised policies that address critical security vulnerabilities, and identification of additional products needed (if any) to comply with these policies. In any case, close coordination with DCS and SCADA vendors is recommended to ensure that whatever products are deployed in generation plants and transmission SCADA networks are validated and will not disrupt reliable operations.

Hence, the recommended first step in a five-step cyber security process to comply with NERC CIP is to begin with risk assessments and critical asset identification. In this step, critical operational assets are identified and underlying information technology is cataloged. Once completed, a qualitative risk analysis is performed to identify possible threats and vulnerabilities. The risk analysis should also take into account possible threats that could be mitigated or exacerbated by interconnectivity with other parties. Identified threats should include a threat description, the probability of the threat causing a problem, and the impact of that problem.

The first step also includes a security vulnerability assessment. In this step, access levels, protocol security (ICCP, Modbus), patch management, and other aspects of the current state of security are examined. At many utilities, the corporate network is perceived as a trusted network. Yet, after performing security assessments and penetration tests, vulnerabilities in the corporate network are typically identified that may create security gaps into the SCADA environment. Vulnerability assessment and penetration testing methods must be validated in DCS and SCADA environments. Hence, the vendor that performs this assessment and testing should have experience in the DCS and SCADA space.

The second step is to create a security policy that accounts for findings from the security assessment and penetration testing step. The developed policies should take into consideration the specifics of each business, organization, and network. This step also includes disaster recovery planning—assessing backup and restoration procedures, as well as other measures that help ensure uninterrupted operations. The fourth step is to deploy protective measures (i.e., security and disaster recovery measures) that enable compliance with these policies. The fifth step is to monitor and manage on an ongoing basis to ensure compliance with NERC CIP initially and ensure ongoing compliance as the organization evolves.

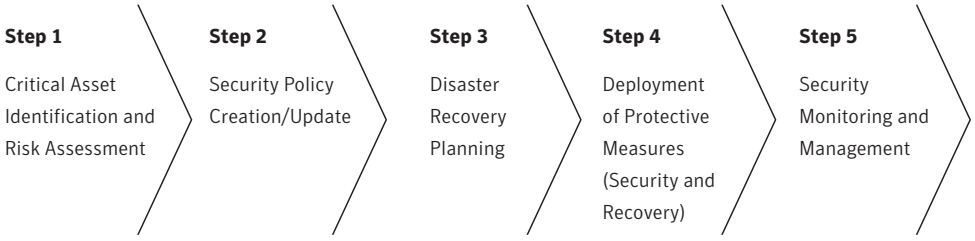

Figure 1. The recommended five steps to NERC CIP compliance

The remainder of this paper summarizes effective practices for compliance with NERC CIP. Developed by Symantec security experts with years of experience in the electric power industry, these practices are organized according to the eight standards in NERC CIP, and within each of these eight, the practices are further organized according to key requirements. Figure 2 shows the areas in NERC CIP that typically require the largest portion of the compliance effort; this illustration also shows typical degrees of compliance in Symantec client engagements.

CIP 002—Critical Cyber Assets Identification

Critical Asset Identification Method. A risk assessment methodology should be used to identify all critical assets. The risk assessment should include the following activities:

- **Operational Risk Assessment.** In this step, critical operational assets are identified and underlying information technology is cataloged. Once completed, a qualitative risk analysis is performed to identify possible threats and vulnerabilities. The risk analysis should also take into account possible threats that could be mitigated or exacerbated by interconnectivity with other parties. Identified threats should include a threat description, the probability of the threat causing a problem, and the impact of that problem.
- **Network Vulnerability Assessment.** A network vulnerability assessment should be performed to accurately depict the current security posture of cyber assets associated with critical infrastructure.
- **Policy Review.** All associated policy documentation should be reviewed to assess its overall effectiveness in policy and practice.
- **Gap Analysis.** Based on information gathered during the network vulnerability assessment and policy review, a gap analysis should be performed to evaluate current practices in accordance with policies and CIP requirements.
- **Security Awareness Review.** A general review of executive and operational security awareness should be performed. General security practices and the strategic importance of security should be evaluated.

Critical Asset Inventory. Critical assets should be defined and catalogued for the entire organization. This catalogue should list the details of every critical asset, including the type of asset, location, date installed, and date of last inspection or maintenance.

Use of asset discovery tools such as network discovery and IT asset management applications can provide a cost effective way to help perform initial asset discovery. These tools identify applications, hosts, and network assets. Many of these tools can also provide patch level and version level information on assets. This information can be used as part of the first step of identifying critical cyber assets.

When evaluating tools, verify that such tools will not affect legacy system stability. If they require a software agent, such tools should be validated in a test environment before production rollout. Finally, since period review is required by the NERC CIP standards, tools should able to perform periodic updates, identifying "adds, moves, and changes."

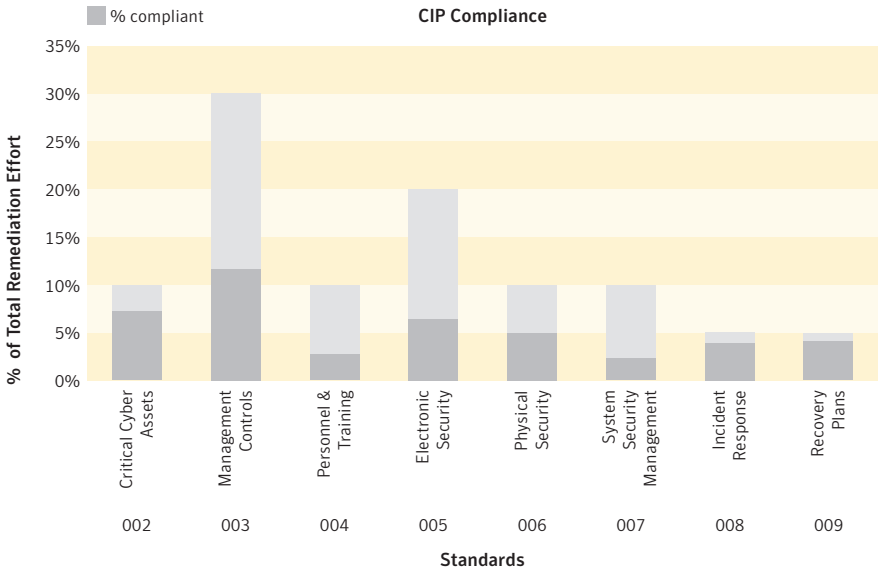

Figure 2. CIP compliance level and focus of remediation efforts in a typical Symantec NERC CIP engagement.

Critical Cyber Asset Inventory. Critical cyber assets should be defined and catalogued for the entire organization. This catalogue should list the details of every critical cyber asset, including the type of asset, location, manufacturer, model number, serial number, version, date installed, and date of last inspection or maintenance. All networks and systems connected directly or indirectly to the outside world should also be identified. Despite likely implementation of some security measures on the corporate network, it should not be considered a trusted network. This should be taken into consideration when cataloguing critical cyber assets.

Review. Asset inventories should be reviewed quarterly to ensure they reflect the current environment.

Governance. A single person should be assigned responsibility for managing and securing the organization's critical assets and critical cyber assets. This person should develop a plan for governance of the assets that outlines change management and access controls.

CIP 003—Security Management Controls

Security Policy. The responsible entity should have a security policy in place, explicitly stating executive management's commitment to security. The security policy should describe the framework for implementing and managing security controls, including the security principals, standards, and regulatory requirements to which the responsible entity is subject. The security policy should describe where in the organization responsibility for security resides.

The security policy should be reviewed on an annual basis. Any modifications to the security policy should be subject to executive management approval. The security policy, as well as any modifications, should be published and communicated to all employees.

Leadership and Exceptions. A single person should be assigned responsibility for managing and securing the organization's critical assets and critical cyber assets. This person should develop a plan for governance of the assets that outlines exceptions, change management, and access controls.

Information Classification. An information classification scheme that is appropriate to the security needs of the responsible entity should be defined and applied to all information related to critical cyber assets. All information related to critical cyber assets should be catalogued, and an appropriate sensitivity level should be applied to it. Appropriate levels of protection should be defined for the information at each of the security levels, including required access controls, encryption, and procedures for disposal, printing, and other tasks.

The information classification scheme should be reviewed on an annual basis to ensure that it remains appropriate to the organization. Modifications to the information classification scheme should be communicated to all employees or contractors with access to classified information.

Effective use of centralized authentication mechanisms can provide the technology base for security management controls. Centralized authentication through "Active Directory" or other LDAP-based authentication mechanisms provides a consolidated view into, roles, data, and their associations.

Additionally, policies involving modifications, additions, and remissions can be enforced through "Active Directory" or other LDAP-based authentication mechanisms.

A separate authentication implementation should be used from the corporate directory. No authentication information should be shared between the corporate authentication mechanism and the one that is used to control access to assets within the electronic security perimeter. Such an integration would violate the concept of "need to know and least privileged access" as outlined in CIP 003.

When evaluating centralized authentication mechanisms, it is important to consider how well IT security policies, such as password strength, password age, and account lockout, can be implemented.

Access Control. An access control model should be in place to manage all access to classified information. The access control model should be based on documented need-to-know information, and should default to no access. The access model should be defined in terms of the information classification scheme (e.g., with greater management sign-off required for access to information of higher sensitivity).

The access control model should be based on roles rather than purely discretionary. The access control model should be reviewed annually or whenever there is any change in the information classification scheme. If a data owner or other employee has discretionary authority to grant access, then the access rights should be reviewed whenever that employees position changes.

Change Management and Change Controls. A change management process should be in place for all changes to critical cyber assets (software and hardware). The change management process should require formal change requests that describe the reason for the change, the cost of the change (both immediate and over the lifecycle of the asset), and the impact of the change. All changes to critical cyber assets must undergo functional testing prior to being deployed in production. Production data should not be used for testing. Back out procedures are defined prior to making a change to a critical cyber asset. All proposed changes must be certified by management prior to being deployed in production.

Policy Creation and Management Tools. In many companies, the existing corporate IT policy can be extended to cover new areas, such as SCADA and DCS networks. However, the customized policy for NERC CIP compliance should recognize the important differences in security requirements between corporate and process control networks. Various policy management tools can be used to automate the process of creation, management, and enforcement of the security policy.

CIP 004—Personnel and Training

Awareness. A security awareness program that describes and communicates the security policy and all relevant procedures and standards should be provided for all employees. The security awareness program should have visible and explicit senior management support. The security awareness program should employ multiple media to reinforce the message, such as posters, intranets, memos, give-aways, and other rewards. All employees should acknowledge in writing that they have read and understood the security policy.

Web-based security awareness programs can be an effective way of increasing employees familiarity with security and their responsibly as an employee. These programs can be easily deployed and usage can be tracked.

When evaluating Web-based security awareness programs, place special attention on the applicability of the contents to the unique security needs of the operations environment or process control network. The Web-based security awareness program should be able to be modified with specific information unique to each environment and have reporting functionality that will document compliance to CIP 004.

Training. All employees whose role has a security component, including users with access rights to classified information or system administrators responsible for the management of critical cyber assets, should receive security training. The training should cover the responsible entities' security policy and the specific procedures and standards relevant to that role. Training should be provided on a quarterly basis or more frequently, depending on need. Records of all training should be maintained, including the lists of all attendees.

Personnel Risk Assessment. Background checks should be conducted on all candidates for roles with access to classified information or access to critical cyber assets. The background checks may include criminal background, credit checks, and reference checks as appropriate for the level of security access.

Background check records should be maintained, and employees should be re-assessed after five years or whenever there is a change in role that carries an increase in access rights.

Access. The responsible entity should maintain records of all access rights for all employees or contractors with access to classified information or to critical cyber assets.

Access rights should be reviewed on a quarterly basis. An individual's access rights should also be reviewed upon any change in position or responsibility (including promotions within the department). Access rights should be retained on a need-to-know basis, and should default to no access. All access rights should be terminated immediately when the employee or contractor leaves the position (for whatever cause.)

As stated as part of CIP 003, use of centralized authentication mechanisms such as "Active Directory" can provide much of the information that is required as part of this requirement. Access rights can be exported as part of any enterprise level authentication mechanism and should be used for that purpose to adhere to this policy requirement.

CIP 005—Electronic Security Perimeter

Defined Electronic Security Perimeter. The electronic security perimeter should be well delineated and thoroughly documented. Any access through the perimeter should go through a limited number of well-controlled points that only allow the minimum number of ports and services, and are configured for default deny.

Network firewalls and network asset discovery are good tools to help define the electronic security perimeter. Because of the importance of assets with the electronic security perimeter, special attention should be placed on network firewalls. These firewalls should include the

capability to block network traffic based on traditional network filtering and the capability to inspect network traffic for malicious code and vulnerabilities. Additionally, firewalls should be able to understand and inspect industry specific protocols such as ICCP and Modbus.

Firewalls across the electronic security perimeter should have the capability of being centrally managed and monitored. Logs should be centrally viewable and exported for review and archival.

Because of the sensitivity of process control network hosts to performance degradation, which is often caused by host security measures, selection of a perimeter security device that contains antivirus and intrusion detection capabilities is recommended. SCADA and DCS vendors should test and validate this device.

Finally, firewalls should contain virtual private network (VPN) capability to allow automated user access to the inside of the electronic security perimeter and allow data to leave the inside of this environment. This VPN capability should be integrated utilizing two-factor authentication and a centralized authentication mechanism that is not associated with the corporate environment, as outlined above.

Electronic Access Controls. Two-factor authentication should be used for any access through the electronic security perimeter. Authentication should be centralized for all access points. Where two-factor authentication is not feasible, access through the perimeter should also be limited to known hosts.

Wireless Security. All wireless traffic should be encrypted using 128-bit or better encryption. Systems using 802.11 wireless should be tuned to the minimum strength required, not broadcast SSID, and use WPA2 encryption with AES.

Protocol Security. All traffic traversing the electronic security perimeter should be encrypted using 128-bit or better encryption. However, encrypted traffic is not necessarily secure. If a hacker tampers with the traffic at the point of its origination, the attack will be encrypted and difficult to detect with network-based security measures. Hence, protection of the originating server of the traffic is recommended, if possible. Alternatively, the traffic should be scanned prior to encryption.

Vulnerability Assessment. A vulnerability assessment should be performed quarterly on the electronic security perimeter. These assessments should identify all devices on the perimeter, the ports and services allowed through the devices, and any devices that are visible through the perimeter. The assessment should then attempt to find exploitable weaknesses in the configuration of the security perimeter, and attempt to gain access to critical cyber assets and critical assets by exploiting those vulnerabilities. However, whether conducted by company IT personnel or outside consultants, the assessment must not interfere with continued operation of the SCADA or DCS servers, which can be extremely sensitive to automated vulnerability assessment tools.

Monitoring Electronic Access. All traffic traversing the electronic security perimeter should be logged. All logging performed by devices on the electronic security perimeter should be stored on a centralized log server. These logs should be reviewed monthly and retained for at least 90 days. An intrusion detection system should be used in conjunction with the centralized logging in order to detect attacks and to notify administrators of anomalous behavior.

Since different perimeter security measures from different vendors produce a huge number of security logs, many times about the same events, yet using different syntax, it is increasingly difficult to manually monitor logs, identify attacks and respond in time. Adding to the ever increasing number of vulnerabilities discovered on a daily basis, the manual process of monitoring becomes almost impossible.

There are two efficient ways to address this challenge. One ways is via usage of Security Information Management software or appliances. These measures automate the process of aggregation, correlation and reduction of security logs, so that monitoring personnel can identify and quickly respond to the attacks.

This approach may work well for highly centralized utilities that do not have many distributed assets and where IT controls SCADA networks as well. However, the majority of Electric Power companies have different organizations controlling generation plant DCS and transmission SCADA networks. Also, the need for security in the operational environment is physically 24x7, where severer security events need to be immediately discovered and addressed before they can cause reliability issues.

Usually it is not effective for the centralized IT organization to monitor dozens of distributed operational assets, because these require different security approach and, unlike control centers with operators physically present, usually IT does not operate physically 24x7. It is also not considered a good practice to overburden system operators with an additional task of security log management. Finally, it is not cost-effective to hire dozens of new employees for this task.

For these environments, using Managed Security Services may be a very efficient and cost-effective practice. These services deliver real-time threat analysis, helping organizations establish compliance, minimize business impact, and reduce overall security risk at acceptable cost in the face of today's emerging threats. These services offload the burden of real-time network monitoring, advanced security analysis, and global intelligence correlation, while allowing businesses to maintain complete insight into critical business information.

Documentation Review and Maintenance. All systems in the electronic security perimeter should be thoroughly documented, and the relationships between systems should also be documented. All changes should be thoroughly reviewed and implemented according to a documented procedure, and those changes should be immediately reflected in the documentation. All documentation should be reviewed quarterly to ensure accuracy.

As stated above, network discovery tools should be employed to document the physical topology of the electronic security perimeter.

CIP 006—Physical Security

Physical Security Plan. The physical security plan should outline the physical perimeter and controls around all critical assets and critical cyber assets. It should address potential vulnerabilities and contain plans to respond to or mitigate potential risks.

Documentation Review. Physical security documentation should be reviewed quarterly to ensure that it reflects the current environment and controls that are in place in the environment.

Physical Access Controls. Electronic locks with a centralized authentication system supporting two-factor authentication should be used wherever possible. If this is not possible, strong key control procedures should be used to prevent loss, theft, or unauthorized duplication of keys. All critical cyber assets should be located in secure facilities, with restricted access.

Identification. All employees and visitors should be required to wear photo identification badges that are clearly visible above the waist at all times.

Logging Physical Access. All attempted and successful access to areas containing critical assets or critical cyber assets should be logged electronically to a centralized logging server.

Monitoring Physical Access. All potential entry points to the physical security perimeter should be monitored electronically. Dedicated staff should monitor video in real-time.

Access Log Retention. Access logs should be reviewed monthly for unauthorized access and retained for at least 90 days. Video should be retained for at least 90 days.

Maintenance and Testing. All physical security controls should be tested quarterly to ensure effectiveness.

CIP 007—System Security Management

Non-critical Cyber Asset Inventory. All devices within the electronic security perimeter should be defined and cataloged. This catalogue should list the details of every asset, including the type of asset, location, manufacturer, model number, serial number, version, date installed, network address, hardware address, and date of last inspection or maintenance.

In addition to the asset discovery tools as discussed as part of CIP 002, policy compliance and auditing technologies can provide excellent visibility into the configuration of critical and non-critical assets. When evaluating policy compliance and auditing technologies, these technologies should be validated within a test environment so that they do not negatively affect the performance or stability of critical application and cyber assets.

These technologies should be customizable to map documented policies to technical implementation and actual system checks. Policy compliance tools should be able to map "trending and report percentage of compliance over time. Finally, these tools should be able to provide segmented information for specific regions and operational areas.

Test Procedures. Any changes to the production environment must be documented, approved by authorized authority, tested in a non-production simulation of the running environment, and then applied to the production network during a scheduled window, with a rollback procedure.

Ports and Services. A best practice is to ensure that only those ports and services necessary to provide essential functionality should be enabled on all cyber assets.

Security Patch Management. When patches are released by device manufacturers, they should first be evaluated for criticality based on the severity of the potential exploits they address. Patches with a high criticality should be tested on non-production systems before being deployed within one week. Patches with lower levels of criticality should be tested and deployed on a quarterly basis. If patches are not applied, this decision should be documented and approved by an executive, and mitigating steps should be taken to address the vulnerability.

Malicious Software Prevention. All systems that support anti-virus software should have anti-virus software installed. The client software should be configured to update definitions at least every 24 hours from a secure, centralized server controlled by the covered entity. The entity should test all definition updates in a non-production environment before deployment to the production network.

Anti-virus technologies should be evaluated based on their acceptance by software vendors, providing support for critical cyber assets such as EMS, PI, and DCS systems. This will ensure that such software will not affect the stability, performance, or supportability of the specific applications.

Additionally, antivirus technologies should have the capability to pull down signatures from a source within a DMZ on the electronic security perimeter. Directly connecting antivirus software on DCS and SCADA servers to the Internet is not recommended, because this approach opens another security threat vector.

Account Management. All systems should authenticate to a centralized host, and local accounts should be disabled. Shared passwords and accounts should not be used.

Security Status Monitoring. All systems should log to a centralized log host, and those logs should be reviewed monthly and retained for at least 90 days. In addition, an intrusion detection system should be used on hosts to detect attempted exploits and alert administrators. Intrusion detection should have the capability to not only provide information on traditional attacks but also attacks and vulnerabilities inherent within industry specific protocols such as Modbus, OPC, and ICCP.

All information should be centrally collected in a repository capable of providing automated and applicable security alerts based on actively collected intelligence and log information. Systems should be evaluated primarily on their ability to detect industry specific attacks and minimization of false positives.

Disposal and Redeployment. All decommissioned systems should be destroyed and not re-used. If systems must be re-purposed, all hard drives should be overwritten with random data seven times, and all BIOS settings should be reset to the default before being released.

Cyber Vulnerability Assessment. A vulnerability assessment should be performed quarterly against all devices within the electronic security perimeter. These assessments should identify all devices on the network, the ports and services running on the devices, and any applications running on the devices. The assessment should then attempt to find exploitable weaknesses in the configuration of the devices, and define an action plan with a prioritized list of mitigating steps.

Documentation Review and Maintenance. All non-critical cyber assets should be documented, and the relationships between systems should also be documented. All changes should be reviewed and implemented according to a documented procedure, and those changes should be immediately reflected in the documentation. All documentation should be reviewed quarterly to ensure accuracy.

CIP 008—Incident Response

Incident Response Plan. The responsible entity should implement an incident response plan that explicitly states the authority under which the plan operates, the constituency for the plan, and the services that the plan will offer that constituency. Also, the jurisdiction of the incident response team should be defined together with any dependencies on other internal or external organizations.

Service levels for each of the services defined in the incident response plan should be defined. Personnel should be available for incident response 24x7. Contact and organizational information should be updated on a monthly basis.

Incident Response Documentation. The incident response team should maintain records of all incidents or suspicious events, including original evidence such as system or host logs, video, or physical access records. Also, all records of investigation of, or response to, an incident or event should be maintained. Report all incidents to ES ISAC. For more information, refer to http://www.esisac.com.

As stated above, information correlation systems should be evaluated primarily on their ability to detect industry specific attacks and minimization of false positives.

In addition, these systems should be able to gather information from multiple sources and across multiple vendors in order to better validate an attack and effected systems. Finally, incident response systems should be able to provide pinpointed actionable intelligence to the internal incident response team so that immediate and appropriate action can be taken.

CIP 009—Disaster Recovery

Recovery Plans. Recovery plan must define action triggers, acceptable downtime service level, and acceptable data loss. The recovery plan should include critical vendors as part of the planning process and a risk assessment. Applications, host hardware, and networks should be prioritized, and an inventory of assets should be kept current with regular review. Finally, verification criteria and procedures must be included to validate the recovery plan.

Exercises. Define, perform exercises, and evaluate results based on probable disaster scenarios.

Change Control. Document changes to critical assets, recovery plans, and test procedures. Changes must be must be kept current with regular updates.

Backup and Restore. Recovery of critical assets must be ensured with applications to acceptable patch level, data to acceptable interval, and network/operating system configurations to the last known state. Additionally, authentication mechanisms must have the capability of being restored to the last known state.

Testing of Backup Media. Backup media must be verified to a level that ensures that the data catalog is not corrupt and that can be restored to an acceptable level. Media must be available within an acceptable time period and re-usable media must be within its life cycle.

For More Information

CIP Section	Security Technology or Service	Symantec Product or Service
CIP 002—Critical Cyber Asset Identification	Risk assessment service	Professional Services
		Veritas Provisioning Manager
	Network, server and application discovery	Veritas Configuration Manager
		LiveState Client Management Suite
CIP 003—Security Management Controls	Security policy development service	Professional Services
		Bindview Policy Manager
		Control Compliance Suite
	LDAP authentication	Enterprise Security Manager
CIP 004—Personnel and Training	Web-based security awareness	Security Learning Services
CIP 005—Electronic Security Perimeter	Network security appliances	Professional Services
	Network intrusion detection / prevention appliances	Symantec Gateway Security 1600 and 5600 series
	Network asset discovery	Symantec Network Security appliance 7100
	Virtual Private Network	Veritas Provisioning Manager
	Two-factor authentication	Veritas Configuration Manager
	Secure wireless access points	LiveState Client Management Suite
	Network architecture assessment	
CIP 006—Physical Security		Professional Services
CIP 007—System Security Management	Policy compliance	Professional Services
	Host-based antivirus	Bindview Policy Manager
		Control Compliance Suite
		Enterprise Security Manager
	Network vulnerability assessment	Security Information Manager 9500
	Network host assessment service	
		Managed Security Services
CIP 008—Incident Response	Security information management	Professional Services
	Security incident correlation	Security Information Manager 9500
	Managed security service	Managed Security Services
	Incident response	
	Process/procedure development	
CIP 009—Disaster Recovery	Backup and recovery	Professional Services
		LiveState Recovery Advanced
	Disaster and risk assessment service	Server Suit
		Backup Exec

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

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

08/06 10431282