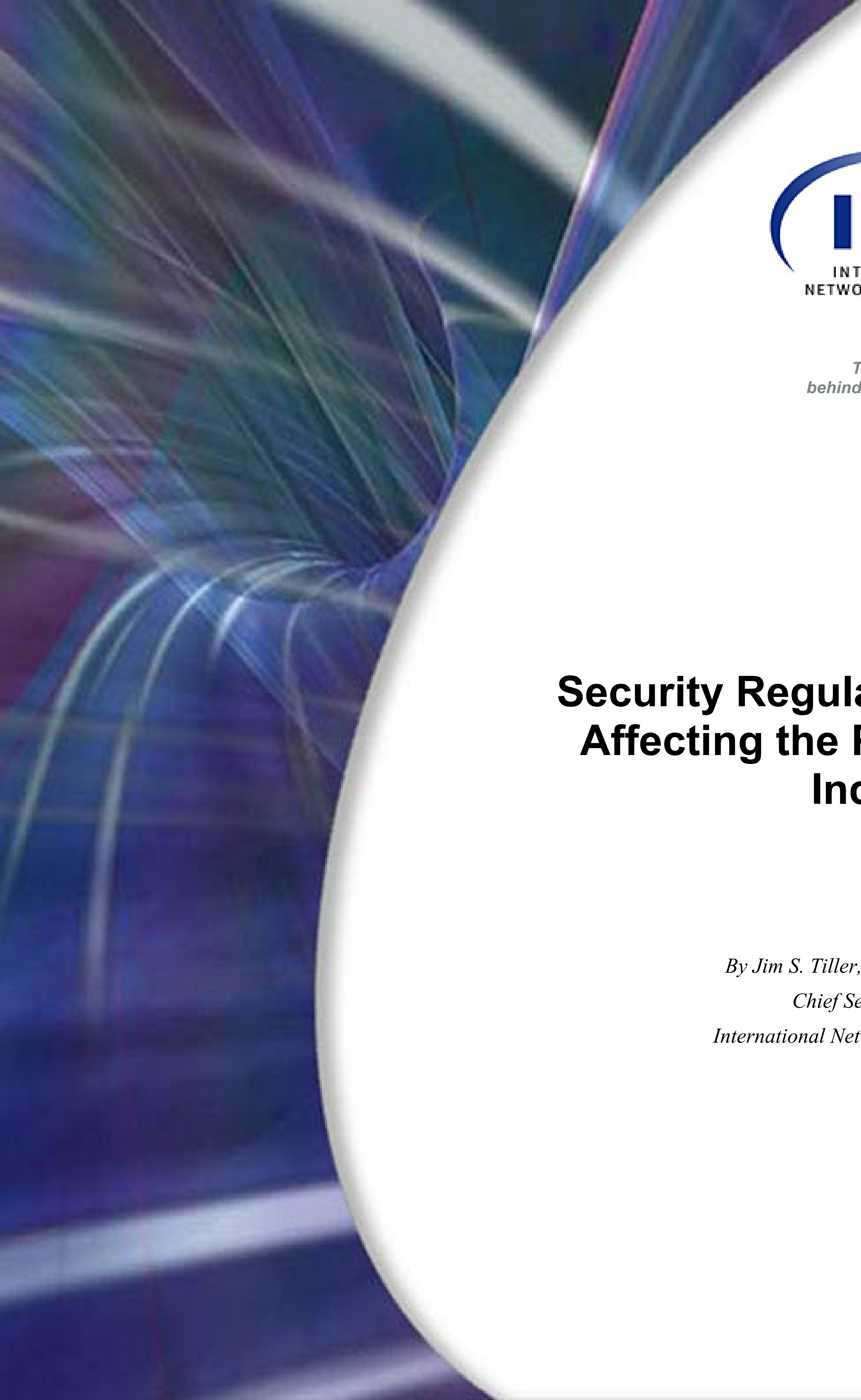


INTERNATIONAL
NETWORK SERVICES

*The knowledge
behind the network.®*

Security Regulations Affecting the Power Industry

By Jim S. Tiller, CISSP, CISA
Chief Security Officer
International Network Services

Security Regulation Affecting the Power Industry

By Jim S. Tiller, CISSP, CISA, Chief Security Officer

Introduction

To simply say the attack on the United States on September the 11th affected how security is perceived and practiced would be an enormous understatement. In reality, it changed our collective perspective on how we do everything from boarding airplanes to buying our favorite NFL jersey on-line. From that moment in time the federal government has taken a number of actions, most notably creating the Department of Homeland Security, which is assigned the task of protecting the U.S. from acts of terrorism.

Government involvement in information security impacting the private sector, beyond the military or other agencies where strong security measures are expected, was spawned in May 1998. The Clinton administration had recognized that the U.S. maintains the world's largest economy and the strongest military, both of which rely heavily on critical infrastructures. It also recognized that physical and cyber systems have become increasingly interconnected, raising their volatility and exposure to threats. Primary critical public and private infrastructures identified were telecommunications, energy, transportation, banking and finance, water systems, and emergency services. [1.] The result was the publication of Presidential Decision Directive 63 (PDD 63)[2], which states that by May 2003, the U.S. shall achieve and maintain the necessary security measures to swiftly eliminate any vulnerabilities and ensure the continuity of critical systems.

In June 2001, the electric power industry took up the gauntlet and started an effort to secure the U.S. power infrastructure. This white paper will explain the requirements that have been placed on the power industry .

Governmental Agencies and Power Industry Security

The Federal Energy Regulatory Commission (FERC) is an independent regulatory agency within the Department of Energy that was created on October 1, 1977, through the Department of Energy Organization Act. FERC regulates interstate transmission, transportation, or piping and sale of electricity, oil, and natural gas. Additionally, FERC administers accounting and financial reporting regulations and conduct of jurisdictional companies, and approve site choices as well as abandonment of interstate pipeline facilities.

In mid June of 2001, FERC produced a Notice of Proposed Rulemaking (NOPR), a proposed regulation affecting many aspects of power regulation, including information security. Working hand-in-hand with FERC, the Department of Energy (DOE) and National Infrastructure Protection Center (NIPC), the North American Electric Reliability Council (NERC) has operated as a voluntary organization to promote electric system reliability and security. As a not-for-profit corporation, NERC is made up of ten regional councils led by a ten member board of trustees. A working group of NERC is the Critical Infrastructure Protection

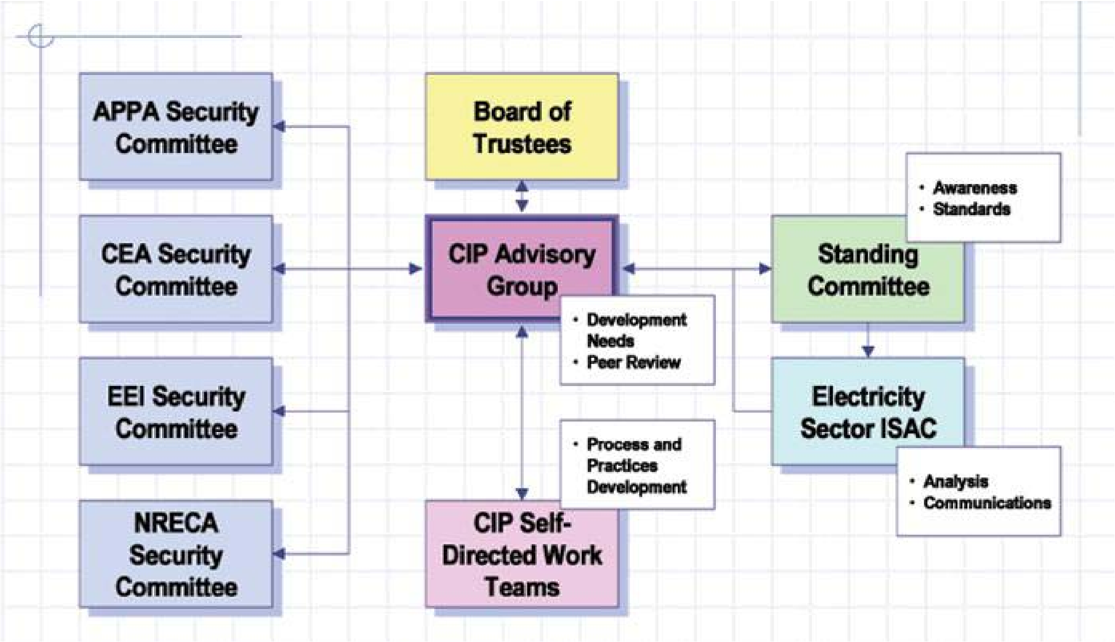
[1] Since its original publication in 1998, several new critical infrastructures have been added to the PDD-63

[2] http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

Advisory Group (CIPAG), which reports to the board of trustees and coordinates all of NERC's activities regarding security initiatives and is responsible for the security portion of the NOPR

Therefore, at the end of this alphabet soup, CIPAG is the group within NERC responsible for the creation and management of security regulations to support FERC's NOPR security objectives based on PDD 63. Figure 1 portrays the internal structure centered on the CIPAG.

Figure 1: CIPAG Internal Structure



Recent Changes

Originally, FERC requested NERC to develop security standards, noted as Appendix "G", for inclusion in the NOPR. However, as the new FERC regulation started to take shape – in the form of 600 plus pages – the development and adoption of the entire NOPR began to slow considerably. The time-consuming legal process threatened the likelihood that the security regulation would see the light of day, or be ratified in a meaningful timeframe.

Early in 2003, NERC initiated an "Urgent Action SAR (Standard Authorization Request)" to establish a NERC Cyber Security Standard (CSS) to preclude Appendix "G" of the FERC's NOPR. This SAR promoted the CSS for quick adoption in an effort to promote implementing security best practices as soon as possible.

Based on the NERC Reliability Standards Process Manual, Version 2.1, approved by Board of Trustees March 11, 2003, the CSS must survive a two-phased voting process. First, each electric market member has the opportunity to vote on the adoption of the standard and provide comments. A second vote – not completed at the time of this writing – will be executed to determine if the standard is to be accepted. If the CSS is passed, the standard will be in effect for one year starting first quarter of 2004. The hopes are the CSS will become Appendix "G" in the approved NOPR once it is passed as a federal regulation or become an ANSI (American National Standards Institute) standard.

So, that leaves us with the FERC regulation and its Appendix "G" lying in wait as NERC attempts to ratify a security standard to help the power community become more secure. In essence, the CSS stipulates good, sound security practices. It's as simple as that.

Many in the power industry have already met a large number of the requirements by exercising security best practices. While these companies have implemented sound security measures, there remain elements of the standard, particularly logs, reports, and management, that will have to be addressed in order to pass the audit process. Nevertheless, the CSS may represent a challenge to some. The need for basic security in our most critical infrastructure, however, is well worth the effort.

Why Security, Why Now

The simple fact is that the power industry as a whole has generally neglected security, as do many organizations. There are pockets of excellence and pockets of poor security that can be identified in nearly any vertical market. But the major difference between the power industry and other institutions, such as retail, entertainment, and manufacturing, is that power companies are one of the “seven” original terrorism targets identified by the government. Why? Because there is ample evidence that terrorists are targeting the electrical infrastructure.

Throughout the late 1990’s, the National Security Agency (NSA), Federal Bureau of Investigation (FBI) and Department of Defense (DoD) performed several penetration tests against the power grid and the controlling elements. During the multi-year investigation, they found that the system was wide open, allowing unrestricted access to control systems, accounting systems, management devices. Furthermore, they obtained control of nearly all of them.

While the report from the NSA, FBI, and DoD consortium raised awareness, little was done on a national scale to support greater security measures. Nevertheless, awareness was raised. During that same time period, the consortium also discovered that “unwanted influences” were “browsing” the networks of many power companies. In the fall of 2001, FBI found hackers (terrorists, possibly) from Pakistan, Indonesia, and Saudi Arabia collecting logistical data on emergency telephone systems, electric generation and transmission, water storage and distribution, nuclear power plants, and gas facilities. Later that same year, Vitek Boden released one million liters of sewage into the coastal waters of Queensland, Australia by changing PCL code in pump controllers using the Internet to access critical systems.

In January 2003, SLAMMER, the fastest spreading worm in the history of the Internet, consumed resources all over the globe in eight minutes, bringing down countries, not just networks. Korea went off-line, 300 ATMs stop functioning in North America, and two power companies lost control of their power grids for nearly eight hours.

Area of Concern

The power grid is made up of cables, transformers, breakers, power lines, meters, and a seeming endless collection of devices used to exert control and the flow of power. As with any large, complex network, there are nodes or devices that are used to manage the network. Think of the control systems as routers and switches managed by a distant system, such as HP OpenView.

The power grid is managed by an Energy Management System (EMS), which collects data from the grid and makes decisions on various ebbs and flows of electricity. These decisions are driven by requirements to support heavy loads, transfer power, sell or buy power, and other characteristics. When a change is required, the remote element or device in the field is sent commands or triggers to implement the change.

The EMS interfaces with the Supervisory Control and Data Acquisition (SCADA) network, a very large, complex, integrated, shared network used by computers to collect and send information to remote systems. These remote systems are simplistic computers, such as a Programmable Logic Controllers (PLCs), that use latter logic (a simple program of “if this, do this”) to obtain data and make changes to the physical equipment. Physical equipment can be as obvious as a switch and complicated as a capacitor or regulator.

To use a very simple example, EMS collects information from a field system, which warns of a possible overload on grid section 343a. To rectify this, a backup circuit must be closed to send more electricity into the grid. Since this is not a typical situation, the PLC controlling the switch does not have the installed logic to make the determination to close the switch based on the information it is aware of. It may only know the state of the switch (open or closed) and the temperature of the line. Based on the information collected from other systems, EMS sends a command into the SCADA network. This command may have to survive several types of technologies, for example an IP data network, a digital-to-analog converter (DAC), a leased line, or a tone managed interface on a box sitting in the middle of nowhere in Wyoming. The command is implemented; the PLC closes the switch and power is transferred to the grid. The PLC responds with "Switch Closed" and "Temperature 145 degrees".

So, what is the issue? Simply stated, the exposure of the control network to various threats due to complexities, deregulation, and poor security practices has opened the power grid to unauthorized changes that could have enormous impacts felt on a national scale.

SCADA is used by many other types of industries – gas, oil, water, sewage – to manage similar "networks" that control valves, pressure sensors, pumps, and wells.

SCADA 101

We talked about SCADA a little bit and the role it plays in the management of power grids. But what does it look like and how is it used in the industry?

All companies have corporate back office systems and networks to manage day-to-day business. SCADA integrates with these systems and networks at various levels. As more systems are integrated, security becomes more difficult.

There are basically three SCADA architectures:

- Segregated – Some organizations have maintained a manageable delineation between their operational networks and systems and SCADA cyber systems. For example, in some remote area or in various departments there are actually rooms – sometimes cages – that house systems used to manage the power grid. Unfortunately, this segregation is often breached, such as running ethernet from one system to another so the employee in the cage working on SCADA all day can surf the web. Once a physical and logical connection is made, Internet vulnerabilities and threats are transferred to the SCADA network and systems.
- Decentralized - When SCADA activities are located in distant, controlled facilities, many organizations use solutions such as Citrix and other similar protocols like X-Windows, to export the remote system's desktop to a host on the corporate network. The security implications of this remote connection are broad. The security of the protocol between the systems, physical access to the remote host is just like sitting in front of the SCADA host, and authentication controls are fragmented. However, one of the aspects of the CSS is to define a perimeter – a control point – between the SCADA systems and other "grid-critical" systems. Therefore, decentralized management of the remote SCADA systems adds a great deal of complexity to establishing a perimeter and what that will impact.
- Integrated – The natural assumption that integrated EMS and SCADA is better. Unfortunately, the NERC security requirements specifically require segmenting these systems. Power companies with integrated SCADA networks face the biggest challenge in meeting the regulation.

The reality is that most power companies' SCADA architectures don't fall into just one of these categories. Typically, some pieces of the SCADA network might be segregated, while others are decentralized or integrated. This complicates the job of meeting the standard.

CSS Requirements and Considerations

The elements of the CSS are straightforward, although not always easy to meet. The following provides a brief description of each element[3] and issues that must be considered to achieve compliance.

- **Vulnerability and Risk Assessment** - Helps identify those facilities that may be critical to overall operations, as well as their vulnerabilities. Consideration should be given to closely safeguarding such information and restricting it to only a few individuals with a job specific requirements.
- **Threat Response Capability** - Ensures that company personnel at critical operating facilities understand how to respond to a spectrum of threats, both physical and cyber. Consideration should be given to NERC's "Threat Alert Levels and Response Guidelines."
- **Emergency Management** - Ensures that companies are prepared to respond to a spectrum of threats, both physical and cyber. Consideration should be given to reviewing, revising, and testing emergency plans on a regular basis. Plans should include training provisions for key responders to ensure they have the skills and knowledge to effectively carry out those plans. Maintaining comprehensive mutual assistance agreements at the local, state and regional levels also supports response, repair, and restoration activities in the event a critical facility is disrupted. Liaison relationships with local FBI offices as well as with other local law enforcement agencies are also effective.
- **Continuity of Business Processes** - Reduces the likelihood of prolonged interruptions and enhances prompt resumption of operations when interruptions occur. Consider flexible plans that address key areas such as telecommunications, information technology, customer service centers, facilities security, operations, generation, power delivery, customer remittance and payroll processes. It is useful to revise and test plans on a regular basis. It also is advisable to train personnel so they fully understand their roles with respect to the plans.
- **Communications** - Ensures the effectiveness of threat response, emergency management, and business continuity plans. Consideration should be given to establishing liaison relationships with federal, state, county, and local law enforcement agencies in the area. Building the relationship might include providing tours of critical facilities for law enforcement agencies having jurisdiction in areas where those facilities are located, and planning to identify possible response needs. Such liaisons may need to be periodically updated and tested. Consideration also should be given to planning how personnel will respond to alarms, outages, or other issues at critical operating facilities. Robust communications systems such as radio, cellular phone, or similar communications devices are effective.
- **Physical Security** - Mitigates the threat from inside and outside the organization. A physical security program should include deterrence and prevention strategies. A systems approach is advisable, where detection, assessment, communication, and response are planned and supported by adequate policies, procedures, and resources.
- **Cyber Security** - Mitigates the threat from inside and outside the organization. Consideration should be given to computer network monitoring and intrusion detection, placing particular attention on EMS, SCADA, and other key operating systems. It is advisable that only authorized persons have access to those critical systems, and only for valid purposes. Consideration also should be given to adequate firewall protection and periodic audits of the network and existing security protocols. Third-party penetration testing would be useful.
    - ***Risk Management*** - A risk management program is critical for any IT organization to successfully implement and maintain an acceptable level of security.

[3] Security Guidelines for the Electricity Sector, version 1, June 14, 2002. NERC publication

    - ***Access Control*** - Provides for a minimum baseline for secure cyber access control across the electricity sector. This guideline identifies some of the key elements associated with managing access to information systems and services vital to maintaining the reliability of the electric infrastructure. Such access includes logical access to computers and networks, as well as access to the physical environments where computer and network equipment is located, e.g., computer rooms.
    - ***Firewalls*** - An understanding of firewalls and firewall technology is critical to successfully implement and maintain an acceptable level of security. The CSS identifies some resources that are available for an IT organization to develop an understanding of firewalls and firewall policies that will help mitigate cyber risks to its computing systems.
    - ***Intrusion Detection*** - An understanding of cyber intrusion detection technology and methods is critical to successfully implement and maintain an acceptable level of security. The CSS identifies some resources that are available for an IT organization to develop an understanding of intrusion detection systems that will help mitigate cyber risks to its computing infrastructure.
- **Employment Screening** - Mitigates the threat from inside the organization. Hiring standards and pre-employment background investigations may help ensure the trustworthiness and reliability of personnel who have unescorted access to critical facilities, including contractors and vendors.
- **Protecting Potentially Sensitive Information** - Reduces the likelihood that information could be used by those intending to damage critical facilities, disrupt operations, or harm individuals. Consider creating a hierarchical confidentiality classification framework (e.g., Public, Market Participant Confidential, Company Confidential, Highly Confidential) and the authorization requirements and conditions to permit disclosure.

Four Fundamentals

The most prevalent characteristics of the CSS are based on security best practices that are the foundation of traditional security applied to the technical architecture common in the utilities sector.

Risk

Any effort to secure an IT infrastructure is founded on risk. To attempt the application of security measures in the absence of awareness of risk would be a futile effort. One can argue that policy is core, but even defining a policy stating the required security practices of an organization must be based on a risk analysis.

A risk analysis identifies and assigns a value to assets, and calculates their exposure to threats and the likelihood of those threats being exploited. In terms of cyber security, the focus is on digital risks and assets. There are also physical considerations, of course, but those are outside the scope of this paper.

Many government regulations, e.g., HIPAA, GLBA, Patriot Act, 21CFR11, AB-700, stipulate the execution of a risk analysis on at least an annual basis. There is a clear reason for this requirement: you have to know your company's exposure better than the hacker does to secure yourself against the threat. Moreover, every company has unique characteristics that introduce varying degrees of risk. Differences appear because people's impression of security and business goals will never be quite the same. Internal skills, demands, customer profiles, partnership structure, corporate growth plans, you name it, will come into play when evaluating risk.

There are several goals you'll need to fulfill when performing a risk analysis with regards to the CSS..

- **Identification of assets** – First and foremost, identify critical assets that fall within the parameters of the CSS. These include control systems, administrative terminals, EMS interface systems, ICCP gateways, and traditional network interfaces to other parts of the organization, including other offices. Include in the process a determination of whether or not each is a critical asset, which will play a significant role in future compliancy efforts. Most organizations will include marginal assets within the definition of critical asset to support existing infrastructure and simplify the overall effort. For example, it may take much more investment, monetarily and timewise, to move parts of a system outside the scope as opposed to simply lumping it in with the other identified systems.

- **Threat identification** – For critical systems and physical and internetworking elements it is necessary to determine the types of threats they're expose to. For example, company A may have no interaction between the critical systems and the Internet, therefore simplifying the process. Company B, much larger and more dispersed, may have several exposure points to the Internet. This is a simplified example, nevertheless, exposure to threats must be weighed to determine an action plan for proportionally implementing the necessary controls for compliance.
- **Risk matrix** – Once critical systems and potential threats are identified, a matrix should be created that states acceptable risks, risks that will be transferred, and risks that will be mitigated. For the risks that will be mitigated, the matrix will help prioritize efforts and assist in finding opportunities to eliminate several threats with one compliant process or technology implementation.

What makes the process interesting and, arguably, easier is the valuation of system and assets is not necessary for CSS compliance. Once the critical assets are identified and located within the perimeter, the security controls for them will be equally applied across the solution. This is a very important concept and will greatly affect how you determine if an asset is critical or not.

Perimeter

The perimeter is essentially a boundary between critical assets and the rest of the world. The perimeter comes in two forms: physical and logical. Of course, defining the perimeter can't be done until critical assets, elements that play a significant role in the management of the power grid, are identified.

The perimeter serves to isolate systems, therefore, the logical perimeter can not stretch beyond the physical perimeter. Thus, if you have several locations, the perimeter must be a unique entity at each location. Moreover, the interface(s) with the SCADA network is a delineation point separating security controls of the critical assets from the mechanics of the SCADA and back-office systems.

This implies that SCADA itself is not included in the regulation. Although SCADA should have some security standards applied, the reality is the high percentage of proprietary systems, diverse implementations, and specialized protocols (e.g., ICCP) limit the ability – either financially or technologically – to implement effective security on a broad scale. Therefore, in an effort to implement some form of security, the CSS covers only systems that control and manage SCADA rather than SCADA itself.

The perimeter is the point where many security considerations materialize, including physical and logical access controls. Additionally, access to areas defined within the perimeter have to be monitored and logged. Think of the perimeter a logically and physically protected area with controls for *everything* that must enter inside this space, including people, programs, protocols, networks, data, and wires..

Technology solutions are standard, best practices for security. Firewalls, intrusion detection systems (IDS), router security, application controls, and system hardening will all play a part in security. Procedurally, background checks employees have to be conducted, user names and passwords have to be maintained, and change controls for people (e.g., passwords, ID badges) and systems (e.g., upgrades, configuration changes, access management) have to be executed and recorded. Moreover, user access must happen in a defined time period and logged for later auditing and compliance proof.

Monitoring and Logging

One of the major elements of the CSS is the ability to monitor and log all events within and at the perimeter. This includes physical as well as logical access to critical assets. On the surface this can appear to be a daunting task. However, access control and management solutions should include monitoring and archiving of activities.

The teeth in the CSS come into play when the auditing occurs, especially with the logging elements. If you cannot demonstrate the ability of previous logical or physical events (logging) then 1) you do not meet the requirement and 2) it insinuates your monitoring is faulty and not meeting the standard.

Monitoring requirements can include things as diverse as IDS firewalls, security cameras, and visitor sign-out sheets. Logging is inherently part of the process, and the ability to produce the "results" of your monitoring practices and technology will materialize in your logs.

Another element of the logging and monitoring concept is the ability to detect unwanted activity – a major portion of the CSS and detailed further in the next section. Collecting logs is one thing, reviewing them regularly in search of insecure behavior is another. Many people are turning to SIM (Security Information Management) products, which collect logs and provide activity reports. Another strategy is to transfer risk to Managed Security Service Providers (MSSPs) or Managed Security Monitoring (MSM) companies.

Incident Management

Finally, the ability to detect, identify, isolate, eradicate, recover and report on adverse events is a major CSS requirement. There is a great deal of information to assist organizations on detecting and reporting incidents (www.nipc.gov & www.esisac.com).Much detection will be provided by good security practices and the implementation of security measures such as IDS, firewall log review, and security awareness as discussed previously.

Reporting incidents is not new to the power industry. However, in the realm of digital security, it is. To facilitate the process, NERC has built an Incident Sharing and Analysis Center (ISAC) to support the reporting and communal activity for targets of an attack. NERC has also created the NIPC-EP/ISAC Indications, Analysis & Warning Program Standard Operating Procedure (SOP), or IAW-SOP, which details the process. Included in the IAW-SOP is a refined incident report form provided by the NIPC (National Infrastructure Protection Center). The reporting process is divided into two types of events, physical and threat (also know as digital), each with three stages. Each event also has an Event Criterion and an Event Threshold.

A physical event is typically associated with the interruption of power generation or distribution. For example, if the ability to control or managed the power grid is lost, that can be considered a valid criterion for a reportable event. The threshold for such an event would be a grid outage for more than 30 minutes or affecting more than 100,000 customers, or the loss of High Voltage (HV) greater than 500MW for more than 30 minutes due to adverse conditions. Another physical criterion is the loss of HV substations (> 230kV) or on HV transmission or tie lines (> 230kV).

Threat or digital events are based on the primary criterion "Announced and credible threats that, in the judgment of the reporting organization, potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission." as stated in the IAW-SOP. Other criteria include hacker activities such as social engineering, investigative actions (e.g., port scanning), worms and Trojans, and, of course, security breaches.

The stages defined in the IAW-SOP represent the number of reports, the amount of information and the timeframe. Therefore, stage 1 is reporting within 60 minutes, stage 2 is in 4-6 hours, assuming more information, and stage 3 is within 60 days detailing the event. Fairly straightforward, but resource intensive to say the least.

Conclusion

With the growth in standards providing a method for measuring security it was only a matter of time before government became involved to promote (i.e., enforce) better security, especially given the events of 9/11 and PDD-63. The CSS, frankly, is relatively lenient with its focus on the most basic of security measure. In fact, most utilities affected are believed to be near compliancy today. Larger, more complex organizations will feel the full force of the CSS. Nevertheless, it is founded on technology and best practices that have been around for years. Most of all, these standards will ensure that critical infrastructures are secure from attack.

About INS

International Network Services Inc. (INS) provides network consulting services and business solutions to help companies build, secure, and manage business-critical network infrastructures. Our end-to-end network consulting solutions address customers' needs in Next Generation Networking, Security, and Network & Systems Management, helping them optimize their business to better face competitive challenges and meet future demands. We are one of the world's largest independent network consulting and security services providers with a track record of thousands of successful engagements. INS is headquartered in Santa Clara, Calif., and has offices across the U.S. and Europe. For additional information, please contact INS at 1-888-767-2788 in the U.S., 44 (0) 1628 503000 in Europe, or 1-408-330-2700 worldwide, or visit www.ins.com.