



## **ISO 27001: A Powerful Utility Player for the Utilities**

*Information Security Is Becoming an Imperative Priority*

**By**

**Stratton Nicolaidis**

**Chairman and CEO of Numerex (\*)**

When *PricewaterhouseCoopers* and *CIO Magazine* conducted their most recent annual Global State of Information Security® study in the spring of 2008 (2008 GSIS), the result for the utility industry was the classic good news/bad news story. While utilities have made significant strides in improving the state of information security throughout their operations, there still exists a significant gap between the confidence utility executives have as to the effectiveness of their systems and the actual audit or measurement of security policies. And while, in the 2008 GSIS survey, utilities surpassed the cross-industry average for having cellular and wireless security standards in place, the total number showed less than half of all utilities had implemented these key standards.

Utilities face a unique security challenge in that many of the Industrial Control systems in place that include supervisory control and data acquisition (SCADA), remote terminal units (RTU) meters and others were designed and built prior to today's rapidly changing information security environment. And utilities, as part of North America's national critical infrastructure, find themselves at the forefront of the security issue.

For example, in October of 2007, SecureWorks, one of the industry's leading managed security services providers with, at the time, more than 1,800 clients and 100 utilities, reported a 90 percent increase in the number of hackers attempting to attack its utility clients in just one year. In January 2008, a CIA senior analyst reported at a national trade event that hackers had successfully attacked a foreign utility causing power outages that impacted multiple cities, all involving intrusions through the Internet. And closer to home, a Government Accountability Office (GAO) report concluded in May of 2008 that the Tennessee Valley Authority (TVA) was vulnerable to cyber attacks that could have disrupted its power production and transmission system. Incidentally, in its responses to the GAO recommendations (Appendix II of the report) TVA demonstrated through specific actions and processes its "commitment to assuring the security of its critical infrastructures and related information and control systems."

## **Regulations**

Recognizing the potential impact a security breach within a large scale utility operation might cause as well as the increasing overall threat of cyber terrorism, the government has focused its attention on security, the result being a list of cyber security reliability standards for the utility industry. On January 17, 2008, the Federal Energy Regulatory Commission (FERC) achieved a milestone by adopting the first eight mandatory and enforceable

reliability standards that address cyber security concerns on the bulk power system in the United States.

The mandatory reliability standards, which were developed by the North American Energy Reliability Corporation (NERC), require certain users, bulk power system owners and operators to establish policies, plans and procedures to safeguard physical and electronic access to control systems, to train personnel on security matters, to report security incidents, and to have a plan that addresses recovery from a cyber incident. Specifically, the eight standards areas utilities are working to address are:

1. CIP-002: Critical Cyber Asset Identification
2. CIP-003: Security Management Controls
3. CIP-004: Personnel and Training
4. CIP-005: Electronic Security Perimeter(s)
5. CIP-006: Physical Security of Critical Cyber Assets
6. CIP-007: Systems Security Management
7. CIP-008: Incident Reporting and Response Planning
8. CIP-009: Recovery Plans for Critical Cyber Assets

In addition to the above NERC-specific requirements, utilities often find themselves dealing with a wide range of regulatory requirements that touch security of information across their entire operation from power generation and distribution to customer information and employee data, including Sarbanes-Oxley (SOX), Homeland Security Act, Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLBA) among others. And while the requirements and guidelines

generated by these diverse bodies are often vastly different, there are a few common security goals. All of these regulations and laws aim at protecting three key areas that make up the core of information security (the classic “CIA triad” at the center of information assurance):

**CONFIDENTIALITY:** A loss of *confidentiality* is the unauthorized disclosure of information.

**INTEGRITY:** A loss of *integrity* is the unauthorized modification or destruction of information.

**AVAILABILITY:** A loss of *availability* is the disruption of access to or use of information or an information system.

### **The Right Tool for Cyber Security**

As utilities grapple with cyber security regulations and work to ensure the integrity and security of their legacy systems, a new tool has emerged in the form of an international standard that may offer a strong guideline to work toward. In 2005, the Geneva, Switzerland-based International Organization for Standards (ISO) published a new standard, ISO/IEC 27001:2005 (“ISO 27001”) which creates the specification for an Information Security Management System. The objective of the standard itself is to “provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).” ISO 27001 and its associated best practices [ISO 27002] is about Information Technology – Security Techniques – Code of practice for information security management.

Since 2005, the standard has taken hold and is spreading worldwide.

In Japan, ISO 27001 is a basic requirement for public contracts. In the United States, it has been proposed in a testimony presented to Congress in the summer of 2007, that the government “lead the drive toward a common global standard for the public and private sector to secure information systems by accepting ISO 27001 as equal to FISMA [i.e., the Federal Information Security Management Act of 2002].” It is noteworthy that the Consensus Audit Guidelines (CAG) Version 1.0 released on February 23, 2009 by a consortium of federal agencies and private organizations aiming at establishing a baseline standard of due care for cyber security (including 20 top twenty most critical controls) neither duplicated nor replaced guidance for complying with federal IT security requirements (FISMA). The CAG initiative is part of a larger effort housed at the Center for Strategic and International Studies (CSIS) in Washington, DC, to advance key recommendations from the CSIS Commission report on cyber security for the 44<sup>th</sup> Presidency, which was released on December 8, 2008. Of interest, during the comment period running through March 23, 2009, the CAG will be closely compared with the audit guides of some key standards including ISO 27001. As it stands now, the CAG provides precise tactical recommendations, which, altogether, would appear to be a subset of a more all-encompassing strategic information security framework such as ISO 27001.

Overall, ISO 27001 consists of 11 security domains, 33 Control Objectives and 133 Security Controls. All of the elements that are used to manage and control the information security risks comprise the information security management system (ISMS). Every ISMS process follows the Plan-Do-Check-Act (PDCA) model. The 11 security domains are:

1. Security Policy
2. Organization of information security
3. Asset management

4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

As of February 2009, there are over 5,200 ISO 27001 certified organizations throughout the world with about 85, including premier institutions and companies, based in the United States. The good news, especially for utilities, is that all the NERC CIP Cyber-Security Requirements are covered under “the umbrella” of the ISO 27001 standard. Using the standard as a guideline to adopt cyber security best practices and procedures can help utilities not only meet NERC requirements but can help with SOX and other federal security requirements. Because the certification requires a process-centric approach to security, it can itself become a long-term blueprint for system and operational change. Therefore, beyond its security focus, ISO 27001 can be a powerful vehicle to help instill a systemic discipline in change management. It provides overall organizational efficiencies.

### **The Human Factor**

Time and again, when it comes to security, human threats score much higher than those posed by technology itself in the many information security surveys conducted around the world. In the words of the GISS survey for the utility sector, people are the “weakest link”. The sixth annual Deloitte Touche Tohmatsu (DTT) Global Financial Services Industry (GFSI) Practice information security survey published on February 4, 2009 effectively summarizes

the related issues: **“A major focal point, people continue to be an organization’s greatest asset as well as its greatest worry. . . Those of us in the security industry know that an organization’s best defense against internal and external breaches is not technology alone. It is a culture of security within an organization – a mindset on the part of every individual so that actions in support of information security become automatic and intuitive.”** Security vigilance that fights human distraction is even more important in light of the growing “social engineering” (e.g. manipulating people into performing actions or divulging confidential information). In the words of Bruce Schneier, a renown security expert and currently Chief Security Technology Officer with BT **“Amateurs hack systems, professionals hack people.”** (Source: Cisco 2007 Annual Security Report).

Also, across the board, there is a rising concern for the threat posed by outsourced processes. In 2007, the GSIS study remarked that outsourcing processes to third parties doesn’t transfer risk—it often increases it. What is especially troubling is that in this environment of increased security risk from outsourced process is that 73 percent of the utilities don’t conduct due diligence of third parties handling private consumer information, and 49 percent have yet to establish security baselines for partners and suppliers (Source: 2008 GSIS). As Scott Beritano, Senior Editor of CSO Magazine puts it: **“An organization's security is only as strong as its users and partners. Without third party security parameters, an organization's partners can inadvertently become its biggest threat.”** (Source: PricewaterhouseCoopers Press Release of September 10, 2007).

Imposing compliance with ISO 27001 among third-party suppliers and partners will ensure that they adhere to best practices that match the inside organization’s in terms of data protection. There are several popular standards such as the Control Objectives for

Information and Related Technology (Cobit), the IT Infrastructure Library (ITIL) and Statement of Auditing Standards (SAS) No. 70, which address in part information security. However, ISO 27001 is the only auditable international standard focused on information security management systems. Therefore, it provides in the area of information security an effective and controllable bridge between companies.

While there is yet no single silver bullet when it comes to information security, ISO 27001 is gaining acceptance across markets and industries, and provides a common frame of reference throughout the world. It also aligns very well with many other standards, making it the potential cornerstone of an overall security plan.

#### **Numerex and ISO 27001**

Numerex is the first machine-to-machine (M2M) service provider in North America awarded the ISO/IEC 27001:2005 certification. Complying with this standard ensures that our M2M network services and solutions meet the highest level of data security. We follow an ISO-sanctioned systematic approach to enterprise management of sensitive company information, which encompasses people, processes, and IT systems. ISO certification means the M2M data that we process and transport on behalf of third-party organizations maintains the strictest levels of confidentiality, integrity and availability.

In much the same way that ISO 9001 says, "quality is our priority," ISO 27001 indicates that information security is of paramount importance to the organization.

From our people, to our processes, to our technology, Numerex is proactive in regard with data protection, and ensures that threats are mitigated with efficiency. Through the ISO 27001 rigorous certification process, Numerex has elevated M2M information security capabilities and practices, enabling us to provide our customers with reliable and secure services and solutions.

Numerex Corp. (NASDAQ: NMRX) is the machine-to-machine (M2M) provider of choice to some of the world's largest organizations delivering secure, all-around solutions through a single source. The Company's M2M expertise enables its customers to efficiently, reliably, and securely monitor and manage assets remotely whenever and wherever needed, while simplifying and speeding up development and deployment. Numerex is the first M2M service provider in North America to carry the ISO 27001 information security certification. Numerex DNA™ offerings include hardware *Devices*, *Network* services, and software *Applications* offered as individual components or as bundled services. At Numerex, "Machines Trust Us™". For additional information, please visit [www.numerex.com](http://www.numerex.com).

*(\*) This White Paper is adapted from a presentation given at the Remote 2008 Conference & Expo - SCADA, Device Networking, M2M, Wireless Technology, Onsite Power and Security for Remote Sites - held in Atlanta, GA, November 5-6, 2008 - Atlanta, GA, February 27, 2009.*