Understand the access points and infiltration risks your utility faces as your smart grid evolves.

Discover cost-effective compliance measures, including NERC-CIP reliability standards you must meet.

Identify the security technologies and solutions that enable your systems to respond to unforeseen threats.

Implement the governance and training that will keep your people aware and empowered to thwart cyber attack.

Gain a cybersecurity solution that will scale as you introduce smart-grid technologies and devices.

Do you feel confident you’re ready to identify and manage the breadth of security vulnerability that AMI, grid sensors, automation and two-way communications to customers’ premises present?

Is your security robust enough to expand with the evolution of grid devices and supporting applications software?

Does your utility have IT staff experienced in designing the highest level of security measures for critical infrastructure?

Are your security policy and procedures in line with technology and process changes?

Does your staff even have time to take smart grid security on?

If you’re worried about cybersecurity at your utility, you’re not alone, and you’re not worrying needlessly. Recent research published by McAfee found that 85 percent of utility executives surveyed admitted to large-scale denial-of-service attacks or infiltrations in the past year. Another study found that 76 percent of energy utility IT practitioners had seen breaches during 2010.

The same two-way communications and proliferation of data-gathering points that make the smart grid smart also make it vulnerable. Worse, it’s not just intrusion; you’re open to control and disruption.

When government researchers conducted security assessments on SCADA systems, some 12 percent of vulnerabilities uncovered were on control systems. And, utilities are adding more automation year by year. Right now, automation now helps utilities operate more than 80 percent of transmission substations and some 60 percent of distribution substations.

What’s more cyber risks go all the way down to customer premises via the two-way communications networks used for AMI and the smart meters mounted beside customers’ homes. Many utilities think their SCADA systems remain isolated and therefore secure. Fact is hacking risks have increased with connectivity to the often public and IP-enabled networks that connect utilities with customers. Control threats extend into homes and businesses via the disconnect devices on meters and the household appliances connected to home area networks. These vulnerabilities will only grow in scale. Your security solution must keep pace.

Meanwhile, security standards are fast evolving, so any solution you implement today needs to be able to adapt along with them. And, no single standard covers the entire spectrum of the smart grid. In the near future, grid data will impact almost every enterprise system in your utility, including Internet portals where consumers may log in to see consumption.

Not surprisingly, industry analysts predict utilities worldwide will spend some $14 Billion USD on cybersecurity between 2011 and 2018. Spend wisely. Put the experts of CSC on your team.
CSC: For Cybersecurity as Smart as the Grid it Protects
Cybersecurity for the smart grid must balance risk, cost, and performance. The security experts at CSC stand ready to deliver an end-to-end solution with both operational and financial performance in mind. Services include:

**Strategic consulting:** Build security into your smart grid from the start with a comprehensive risk and threat assessment, business impact analysis and business integration analysis. The CSC team can also support your technology evaluation processes, too.

**Regulatory compliance:** Let CSC perform and document a gap analysis and security plan to assure your standards and regulatory compliance.

**Design and implementation:** As one of the world’s largest business and IT services providers, CSC has the expertise to produce cyber and physical security designs for your utility IT systems, implement the solutions, then deliver the operational support and training your people need to keep safeguards engaged.

**Systems Integration and More:** CSC’s utility IT professionals understand SCADA, as well as the control and business systems that keep your utility operating efficiently. We’re also well-versed in the technologies and lessons learned related to the smart grid and the vendor solutions in this space, leaving our team ready to bring these complex technologies together for maximum compatibility, security, interoperability and effective enterprise-wide information management.

**Managed services:** Putting security measures in place isn’t enough. Hackers keep developing threats, so you need to keep fine-tuning your cybersecurity solution. Let CSC handle the security operations or solution maintenance so that your team can focus on running your business.

**What Sets CSC Apart?**
CSC is a leader in cybersecurity. We manage some of the most mission-critical facilities around the globe, including vital systems for the U.S. Department of Defense and the Central Intelligence Agency. With CSC, you’ll be leveraging:

- More than 1,200 full-time security professionals
- Recognized leadership and innovation in areas such as computer forensic services and biometric engineering services
- Established cybersecurity Centers of Excellence and follow-the-sun support personnel
- Extensive experience with utility processes and systems from trained experts
- Comprehensive security solutions with less time and expense than in-house teams
- Robust security operations expertise from 40+ global secure facilities

Cybersecurity for the smart grid is complicated. You’ll be designing a solution that touches information and operations technology, as well as customers, distributed generation sites and introducing historically closed control systems with open networks, such as the Internet.

CSC’s cybersecurity professionals are already expert at safeguarding the many systems affected by a smart grid initiative. Gain the benefit of our experience and proven delivery methods. To learn more, visit poweryourperformance@csc.com or contact us at 800.272.0081.

“The electric grid is highly dependent on computer-based control systems. These systems are increasingly connected to open networks such as the Internet, exposing them to cyber risks. Any failure of our electric grid, whether intentional or unintentional, would have a significant and potentially devastating impact on our nation.”

Bennie G. Thompson (D-MS), Chair of the US House Committee on Homeland Security, with the introduction of the “Critical Electric Infrastructure Protection Act” (April 30, 2009)