VISION STRATEGY REALITY

Industry in transition

+ COLLABORATION AND STANDARDIZATION KEY FOR CYBERSECURITY

By Darren Highfill

SO "CHANGE" IS THE NEW BUZZWORD, EH? MAYBE THE ELECTRIC POWER industry will emerge from the back of the room after all. Our industry is coming closer to the forefront of many current social issues, infrastructure investment is getting more talk time and we have been working hard on the whole change thing for a couple of years now.

Before we get too full of ourselves, however, we need to make sure we are doing the right thing. This industry is not used to rapid change and we can quickly find that we are out of our element—caught up in the moment—and before we know it we could be committed to decisions we wish were easier to undo.

COMMUNICATION NETWORKS

In this article, Darren Highfill takes a broad look at cybersecurity as well as utilities' specific efforts to deal with cybersecurity challenges. In the next issue, Jill Lyon will discuss strategies for dealing with the spectrum crisis and Curt Harler will study PNM Resources work with cellular networks for meters.

While transition is required for us to achieve our goals, it is also when we are the most vulnerable. We must focus carefully on the task at hand and make certain that we are not only building in security today, but also we are doing our best to allow for the inevitable changes in technology, environment and adversaries for tomorrow.

Rapid development and pressured deployment are ripe for making mistakes. And in the world of security, today's mistakes are tomorrow's vulnerabilities. Collaborative community efforts and standardization are the best methods we have to learn from each other's mistakes and maximize our collective engineering prowess. Nowhere does this maxim hold more true than in cybersecurity.

DISTRIBUTION TRANSFORMATION

We are witnessing an unprecedented transformation of how the grid operates at the distribution level. Utilities are proving they too can be innovators as they create new models of interaction and operation tailored to their individual environments and business constraints. Fortunately, in the midst of this emerging market, many leading utilities from North America and around the world are collaborating through the Utility Communications Architecture International Users Group (UCAIug) to develop system requirements.

Within the UCAIug family of activities, the AMI Security Task Force (AMI-SEC) has been producing a set of recommendations and best practices for securing advanced metering infrastructure (AMI). The first set of deliverables for this effort was completed at the end of 2008, including a landmark document, "AMI System Security Requirements," that provides guidance for utilities procuring and deploying AMI systems and equipment.

INDUSTRY COLLABORATION

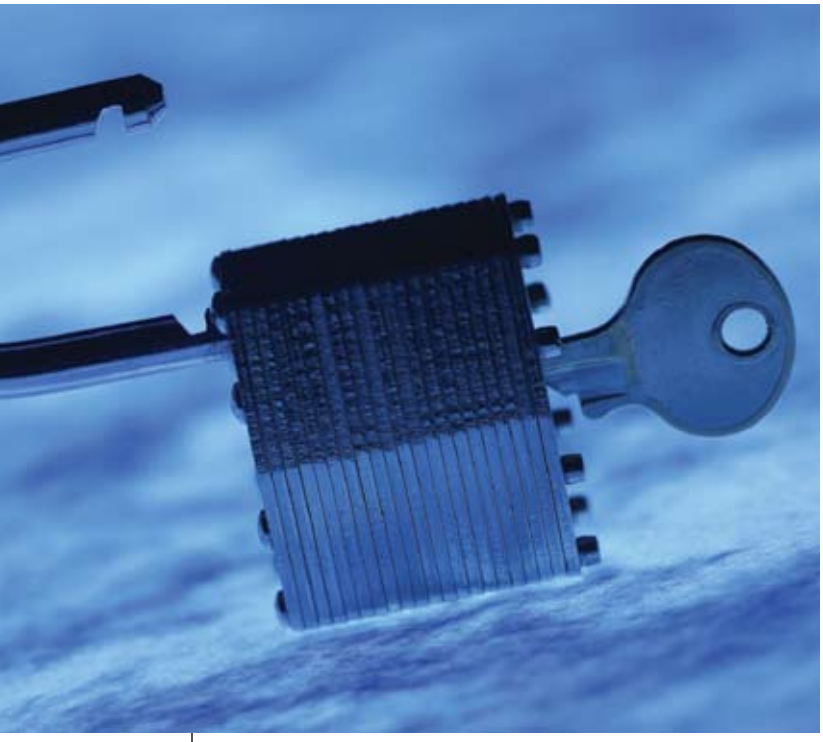
Utilities faced a challenge in 2008 with the human resource demands of developing guidance for AMI security. With so many high-priority projects vying for attention, they were hard-pressed to donate engineering resources to a volunteer-based activity like AMI-SEC. Yet the community recognized the importance of developing specifications and figured out a way to still get the job done by forming a public-private collaborative called the AMI Security Acceleration Project (ASAP).

ASAP brought together eleven of the largest and most progressive utilities in the United States, the U.S. Department of Energy and the Electric Power Research Institute to directly fund industry security expert resources and assist AMI-SEC in getting the work done. The work included developing drafts for all AMI-SEC deliverables, a vendor landscape analysis, procurement language guidelines, penetration testing techniques and methodologies and establishing an independent third-party testing pipeline.

LOOKING AHEAD

While the activities of AMI-SEC and ASAP have produced some first-round guidance for securing AMI, all parties involved recognize the need to start thinking more broadly than just AMI. Deploying a smarter grid will require us to think about security not just holistically, but also from the perspective of complex systems engineering. On tap for 2009 are issues such as new or changing enterprise applications, home area networks, certificate authorities and plug-in vehicles.

Fortunately, ASAP did its home-



work and, in developing best practices for procuring and deploying AMI, intentionally laid the foundation for securing the smart grid. Much of the guidance in the AMI documents can be transformed into a smart grid security specification, which is precisely what the team intends to do in the coming months. Look for another industry-government collaboration associated with the UCAIug under the banner of the UtiliSec Working Group.

ENGAGE

As most utilities are aware of, a smarter grid can take many different shapes and forms. It all depends on a specific set of business needs for the utility implementing it. At the same time, utilities have learned the value of buying commercial off-the-shelf products and not being the lone, special customer for a vendor. The industry is also in need of security guidance. The products of these collaborative efforts will quickly be adopted as de-facto standards for the industry.

In order to prevent winding up on a different track than the rest of the world and ensure your needs are met, there is only one way to play: get involved. Engage in these collaborative activities and make sure your voice is heard. If not, you may suddenly find that change has indeed arrived. Change is happening all around you and the time to move with the future is now.

Darren Highfill is the utility security practice lead for EnerNex Corporation.

SECURITY UNDERCURRENTS

Regulatory transformation. Much has been said in the past year about our new federally mandated electric reliability operator, the North American Electric Reliability Corporation (NERC), especially in regard to cybersecurity and the protection of critical infrastructure. While it is easy to stand on the sidelines and throw criticism, even a casual glance inside reveals a significant and mature standards machine. NERC is handling substantial external pressure through proactive management and process discipline. Regardless, NERC faces some challenges and unclear issues in both the immediate and not-too-distant future.

NERC and FERC. The NERC Critical Infrastructure Protection (CIP) standards received considerable discussion last year, including a long list of explicit comments from the Federal Energy Regulatory Commission (FERC) and associated debate on Capitol Hill. Some of the issues are organizational in nature, as FERC is responsible for all electric system assets in the United States while NERC's charter focuses on protecting bulk power assets in North America.

Other issues have historical or cultural aspects. NERC started out as an attempt by the industry to self-regulate and thus is more comfortable with concepts like requirements stemming from a utility-selected risk management process. On the other hand, FERC, being a governmental entity, likes to see clear and prescriptive guidance to minimize ambiguities for auditing.

Cybersecurity and national security. Recent reports, memos and recommendations are starting to show a shift from cybersecurity being a homeland security issue to a national security issue. Accordingly, responsibility is shifting from the U.S. Department of Homeland Security to the White House and directly appointed positions. The implications of this shift are not yet clear, although it is safe to assume cybersecurity will be receiving more attention and higher priority.

States' rights. While a uniform cybersecurity vision and strategy across the system may make sense from a technical standpoint, we also face a hurdle in the way that our government is fundamentally structured. States still hold the trump card when it comes to legislation, and from a regulatory standpoint we operate more like 50 separate markets—each with its own rules and procedures. As long as state regulatory commissions determine how rates are figured, this issue is not likely to go away.

Smart grid security. With regulatory guidance for cybersecurity aimed at the bulk power system level, the security of many smart grid applications is being left up to utilities. This allows the industry to be aggressive in its pursuit of solutions, but carries the potential downside of individual utilities falling out of line with the industry and not committing the resources necessary to solve the problem.