Utility cybersecurity in the 21st century

Trends shaping the future of utility cybersecurity

There are many common characteristics of utilities in need of enhanced cybersecurity capabilities. A combination of regulators, consumers, and technology are increasing the pressure on utility companies to effectively adapt to current and emerging security threats.

Legacy security systems, founded on discrete point solutions, hamper this effort. This approach to cybersecurity is simply not capable of combating sophisticated antagonists along with the vulnerabilities that come with a multitude of digital endpoints, smart grid monitoring and control devices, mobility applications, and customer-facing web portals.

Utilities require a cybersecurity defense-in-depth approach based on an enterprise-wide architecture.

"Pike Research, a clean-tech market research firm, expects the global smart grid cybersecurity market to grow to $4.1 billion in 2013 at a compound annual growth rate of 35%."[1]

In practice that means folding all security operations (distribution automation, generation operations, field operations, transmission, IT, market operations, marketing, and portals, etc.) into a comprehensive utility security framework. This is already happening in the industry and is one of the trends we discuss in greater detail in a viewpoint paper available here.

The types and sheer numbers of smart grid devices connecting to utility grids are growing rapidly – from smart meters and in-home devices at the customers' premises to phasor measurement units and capacitor banks, which monitor and control power flow on the grid. As these numbers swell, so too does the security risk. To prevent being overwhelmed, utility executives must utilize operational and strategic business intelligence solutions that sift through the real-time data to deliver actionable intelligence and dig deep into historical data for trends. Not only is this approach the only viable way to process the massive data volumes, it is also the most cost-effective method.

Another trend rippling through the industry has been a dramatic increase in mobile applications and web portal access methods. This is driven primarily by the consumerization of utility business models. As enterprises shift toward more customer-friendly relationships, they are tasked to incorporate new web, text, email, mobile-app, smart home, and anytime-anywhere service capabilities. Each of these channels, along with their attendant devices, exposes a host of new vulnerabilities.

Understanding these issues, along with HP's proven strategies to combat them, can help guide utilities to creating a robust cyber-security system while satisfying stringent regulatory requirements.

HP utility industry offerings deliver defense-in-depth cybersecurity solutions.

Our enterprise security offerings are based on an end-to-end enterprise-wide security

[1] http://blogs.wsj.com/source/2010/02/25/power-up-on-smart-grid-cyber-security/

framework discussed here. For a more detailed discussion read our viewpoint paper: The secured utility of the 21st century.

A comprehensive strategic framework lowers risk.

Our governance services help utilities integrate all of their security policies and processes into a cohesive whole. We ensure that they align with the utility's business goals, legal and regulatory requirements, and threat profile.

An enterprise-wide architecture gives utilities granular visibility into their operations and security.

Among our operational-level offerings is the HP ArcSight solution. It collects data from across the utility enterprise to help monitor, detect, and act upon advanced and insider threats. ArcSight's data-aggregation feature also simplifies the utility's compliance reporting activities.

"No utility wants to be the weak link in the chain. The concern over grid vulnerability is driving utility technologists to work closely with systems integrators, infrastructure suppliers, and standards bodies to develop a robust framework for smart-grid cybersecurity across multiple domains."[2]

- Clint Wheelock, Managing Director for Pike Research

Accounting for rapid growth in endpoints promotes a more secure environment.

HP's comprehensive service suite addresses the dramatic growth in endpoints. Our specialists have expertise in DLP-at rest, enterprise mobile security, endpoint protection, and encryption services.

Although a majority of utility executives want to bolster their cybersecurity, many believe

---

[2] "Utilities to Invest $21 Billion in Smart Grid Cyber Security by 2015," February 4, 2010 Pike Research Press Release, http://www.pikeresearch.com/newsroom/utilities-to-invest-21-billion-in-smart-grid-cyber-security-by-2015

Five things utility executives should consider when evaluating their IT security

1. Create a comprehensive, enterprise-wide security architecture that implements a defense-in-depth cybersecurity model.

2. Include operational systems (such as distribution automation) in their comprehensive architecture. Bringing formerly siloed distribution automation operations into a holistic framework strengthens not only the security of those systems, but also every system integrated with them.

3. Leverage business intelligence solutions to cost-effectively increase the effectiveness of cybersecurity initiatives. Sorting through the data to develop targeted, actionable intelligence requires a utility draw on all the information at its disposal.

4. Account for information across its lifecycle to effectively implement data privacy and security.

5. Position cybersecurity to evolve. A comprehensive cybersecurity architecture, complete with granular visibility into utility operations, is a flexible ecosystem capable of adapting to current and emerging threats.

that budgetary constraints and evolving threats are significant barriers. However, just as threats have evolved, so have cost-effective strategies and technologies to combat the most innovative cyber criminals. Why put your utility at risk?

To learn how HP Enterprise Security Services can help utilities, visit us at www.hpenterprisesecurity.com/services.