2012 Utility Cyber Security Survey

Sponsored By

ViaSat

January 2013
Executive Summary

A hacker wearing a fake beard and dark sunglasses took the stage at a computer security conference in Miami, Florida this month and showed a group of about 60 security researchers how to intercept smart grid radio communications.¹

“If you can understand the way these systems speak to one another, the potential to hack them is very real.”

- Atlas, January 17, 2013

Building the utility of the future is expected to yield numerous benefits such as lower power losses, cleaner power, lower electricity bills, and a healthier environment. In fact, Smart Grid investments to date have been largely in technologies that can yield these benefits. However, the consequences of not securing a digital grid connecting billions of devices such as smart meters, electric vehicles, sensors, intelligent electronic devices, transformers, smart phones, and home energy monitoring systems are just now being seriously discussed. Simply put, Smart Grid rollouts across the globe provide more “entry ways” for potential hackers or cyberattacks to cause electrical disturbances.

Utilities, global utility conglomerates, niche solution providers, government stakeholders, and security experts across the globe are working tirelessly to develop standards, protocols, and system architectures that address Smart Grid cybersecurity. To assist in this effort, Zpryme’s Smart Grid Insights and ViaSat have set out to address several issues around utility cybersecurity, and identify vulnerable parts of electrical systems and networks.

Overall, the major findings in this report show that utilities are becoming increasingly cognizant of credible threats to their electrical systems and networks. More importantly, utilities are now prepared to install cybersecurity systems that can identify, isolate, and mitigate attacks to prevent catastrophic system disturbances.

About This Report

The purpose of this report is to assess the overall cybersecurity threat faced by utilities, and identify the key benefits of cybersecurity investments. Additionally, this report identifies key budgeting considerations for cybersecurity, and where these funds are most likely to be spent. And finally, this report outlines system architectures or approaches that will best provide grid security.

Methodology

Zpryme surveyed 213 Smart Grid and utility professionals in November of 2012. Respondents were asked 21 questions. The survey was conducted over the internet.

Major Findings

- Nearly half (47%) of the respondents believed automation security belonged in the top 10% of all priorities for utilities.

¹ http://bits.blogs.nytimes.com/2013/01/17/a-hacker-says-smart-grid-can-be-penetrated/
• The least secure of an electricity grid’s components were the end user segment and the distribution system; and only 4% of the sample said that U.S. electricity grids were very secure.

• Over half (52%) believed that IT-based solutions alone were insufficient for securing the electrical grid.

• The most important role that standards play in implementing security automation technologies was to ensure interoperability among components.

• Seventy-seven percent of the respondents reported that cyberattacks on U.S. utilities would increase in 2013 with power outages and damage to electricity control systems being the major impacts.

• The top-rated benefit of secure automation technology was reliable service.

• Nearly two-thirds of the sample (65%) said investments in cybersecurity in 2013 would increase, with private industry software companies and system integrators providing the best systems to thwart cyberattacks.

• This sample said the average organization amount being budgeted for cybersecurity was $1,450,000 annually.

• Almost three-fourths (73%) felt that the Cybersecurity Act of 2012 should have been passed.
Cybersecurity Survey Implications and Recommendations

The survey results (presented in figures 1 – 21) in this report offer key insights about how utilities will proceed with cybersecurity projects in the near future. In this section we present the major implications of the data, and recommendations that can assist in advancing cybersecurity deployments.

Market Implications

Several implications of the survey supplement evidence from published articles about cybersecurity. Survey respondents noted that security issues involve the IT sector as well as operations technology. And there is some evidence that security spending over the next three years could be heaviest on equipment protection and management.²

Although survey data reflected that the end user was less secure than the distribution system, requiring more security automation, other evidence suggests that the distribution system will reap more benefits from security spending than from an advanced metering system.³ Both, in fact, require substantial “shoring up” to reduce cyberattack risks. Further, Pike Research forecasts more investment in smart grid control systems transmission upgrades, substation automation, distribution automation than in smart metering.⁴

Hackers, terrorists, industrial spies, criminals, and disgruntled employees are all potential threats to the electrical grid. There are two major pathways to the electrical grid: the internet and wireless networks.⁵ The NIST published report in 2010 identified 137 interfaces points of data exchange within or between smart grid systems and subsystems where opportunity exists for security breaches.⁶ A full-spectrum of security measures is needed to best protect the electrical grid. Tight security for industrial controls, physical security such as cameras, badge access, and perimeter security are all crucial to limit unwanted access.⁷

Politics are a consideration for creating and enforcing cybersecurity standards. Survey respondents supported the recent Senate-rejected Cybersecurity Act of 2012. However, some experts are concerned that the division of responsibility between state and federal regulations requires clarification.⁸ Further, evidence implies that utilities are more concerned about regulatory compliance than achieving effective cybersecurity.⁹ Political uncertainty also impacts utilities’ willingness to follow guidelines until they are enforceable.¹⁰ And the lack of enforceability creates a reluctance to invest until laws have been enacted.

⁹ Ibid.
The entire system, IT and operational technology, has to become the focus for cybersecurity implementation. When separate system components are secure, this does not mean that the entire system is safe. A cybersecurity architecture is needed for a system-level approach.

**Recommendations**

1. Utilities should strive for real-time situational intelligence visualization of the security posture of their operational technology (OT) systems. Attacks on utility OT systems can easily cause millions of dollars in damages, and reduce customer confidence in their electricity provider. Real-time situational awareness of OT systems gives utilities actionable data so they can significantly mitigate any potential threats in a timely manner.

2. Utilities should recognize that threats can originate both inside and outside the utility’s systems. For example, compromised supply chains where malware is embedded in new equipment or anyone with access to a utility’s system can use a simple USB thumb drive to execute an internal attack.

3. The multiple networks (and silos) across a utility system make both IT and OT systems vulnerable to cyberattacks. Multiple networks often have varying degrees of security and often do not integrate with one common system, leaving ‘security gaps’ that hackers can easily identify. Thus, utility cybersecurity systems should enable integration of OT and IT networks and scale across multiple service territories and systems.

4. Utilities should work closely together with vendors that use standards based architecture that will enable them to implement scalable security systems that work in a multi-vendor environment.

5. Defense in depth is strongly advocated for cybersecurity by implementing multiple levels of security to achieve:
   - Prevention
   - Detection
   - Identification
   - Mitigation

   Threats will continue to evolve, but a multi-layered approach to security is a critical defensive strategy.

6. As new technologies drive OT and IT network convergence, utilities should establish a specialized representative or office where security accountability for all networks is priority one.

**Conclusions**

Electric utilities are recognized as perhaps the most fundamental critical infrastructure sector, and thus need to be protected from the cascading effect of both physical events and cyberattacks. The drive towards pervasive automation calls specific attention to the need for integrated cyber-physical security systems that will enable the advances in technology to truly deliver on the promise of improved efficiency, resiliency and reliability.
The Stuxnet cyberattack using a highly sophisticated computer worm during the summer of 2010 demonstrated that control networks (i.e., Siemens industrial software-SCADA) are no longer secure simply because they are isolated from the electrical network. The attack has led to a critical need to upgrade electrical grid security.

The utility industry will be spending significant money on cybersecurity (some reports as much as $21 billion by 2015 around the globe). Therefore, the security investments need to be coordinated among all stakeholders to promote effectiveness across the utility industry.

The aging infrastructure combined with unique regional needs means each utility provider will have to examine its own specific security needs to customize a response to counter potential threats.

---

Survey Respondent Characteristics

Organization Size

More respondents (45%) were located in organizations with less than 100 employees than in any other size range. Other organization size responses were: 101 – 500 (12%), 501 – 1000 (6%), 1001 – 5000 (14%), 5001 – 10,000 (6%), and those with over 10,000 employees (18%). A sample average was 2878.

How many employees are in your organization?

(figure 1, source: Zpryme)

Title Within Organization

The sample was composed of: 36% professional/staff, 31% executives, 19% management personnel, 2% operations, and 11% “other.”

What is your title within your organization?

(figure 2, source: Zpryme)
Industry Type

Respondents classified themselves as: a consultant (business, technical, engineering) (25%); a vendor (integrator, technology, electrical equipment, etc.) (32%); a utility employee (24%); a nonprofit organization employee (4%); a power generation organization employee (4%); a state/federal government employee (2%); or from other industries (9%).

Utility Type

The types of utilities where respondents were employed were: investor-owned utility (41%), municipal (27%), federal/state owned (15%), and cooperative (11%). Another 6% said other (than one of these four types).
Cybersecurity Survey Detailed Findings

Priority of Automation Security Real-time systems for Utilities

The respondents believed that automation security was important for utilities' real-time systems and should be placed in the top 50% of all priorities, with 25% saying top 5%, 22% saying top 10%, 23% saying top 25%, and 29% saying top 50% of all priorities. In fact, nearly half (47%) said automation security belonged in the top 10% of all priorities.

Least Secure Segment of the Electrical Grid

The largest group of respondents (43%) said that the end user segment was the least secure component of the electricity grid. The distribution system was next less secure (38%), with the transmission system (14%) and the generation system (5%) both lowest security risks. The end user and distribution system appear most vulnerable to security threats.
Overall Security of Electrical Networks in the U.S.

When considering electrical networks in the U.S. as a whole, only 4% of the sample believed they were very secure. Forty-three percent said the networks were somewhat secure, 39% said somewhat insecure, and 15% said very insecure.

Expected Cyberattacks on U.S. Utilities in 2013

Respondents were asked to predict how cyberattacks on U.S. utilities would change in 2013. While 23% believed attacks would stay the same, 77% said they would increase (20% would be focused on information technology (IT) systems, 57% on both IT and operations technology).
Concern for Potential Cyber and Network Attacks

Nearly two-thirds (63%) said utilities should be very concerned about the potential for cyber and network attacks, with 33% saying moderately concerned, and the remainder (5%) saying slightly concerned.

Major Risks Associated with Cyberattacks

The major risks associated with cyberattacks on a utility distribution system were reported as (in descending order of frequency): power outages (44%), damage to electricity control systems (22%), financial losses and fines (9%), denial of service (8%), damage to operations equipment (7%), and safety equipment failure (5%). Another 5% said risks (other than those in this list) would occur.
Benefits of Secure Automation Technology

The sample was next asked to rate the benefits of secure automation technology by using a scale where 1 = lowest benefit and 6 = greatest benefit. Benefit ratings were: reliable service (4.58), accurate network information (4.36), positive control of safety systems (4.33), low/no fraudulent activities (4.06), and low/no power losses (4.02).

Expected Cybersecurity Investments in 2013

Expectations about how utilities would change their investments in cybersecurity in 2013 were pulsed. Sixty-five percent of the sample said investments would increase; 34% said investments would remain stable; but only 1% said investments would decrease.
Roles Standards Play in Security Automation

The most important role that standards play in implementing security automation technologies was to ensure interoperability among components for 41% of these respondents. Another 23% reported that providing acceptable protection levels was most important, with 17% saying to enable communications across utilities, and 16% saying to provide metrics to measure security status.

Security Automation Demand by Technology

The technology that will see the strongest demand for security automation and applications (in descending order of frequency) was: smart meters/AMI (32%), distribution automation (26%), upgrade of existing transmission and distribution equipment (18%), advanced transmission monitoring systems (15%), and substation automation (10%).
Technologies Most Vulnerable to Cyberattacks

The technology that is most vulnerable to cyberattacks is: operations and information technologies equally (47%), information technology (35%), and operations technology (18%). Clearly, information technology has the highest risk.

Annual Utility Cybersecurity Budget

Their organizations were budgeting differing amounts for cybersecurity on an annual basis: less than $100,000 (25%), $100,001 to $500,000 (30%), $500,001 to $1,000,000 (5%), $1,000,001 to $2,500,000 (20%), $2,500,001 to $5,000,000 (10%), and over $5,000,000 (10%). Although around half (55%) spent $500,000 or less, the average amount for the entire sample was $1,450,000 annually for cybersecurity, which is substantial.
Decision Making about Cybersecurity

The organizational level where decisions are made about cybersecurity was: executive (CEO, VP) (37%), management (47%), or professional/staff (16%).

Real-Time Overlay for Visualization of Security Status

Having a real-time overlay for visualization of their organization’s security status was important (28% said very important, 72% said moderately important) to these respondents.

At what organization level are decisions made about cybersecurity?
(figure 15, source: Zpryme)

How important to your organization would a real-time overlay for visualization of security status be?
(figure 16, source: Zpryme)
Scalable Security “Dashboard” for Monitoring Security Status

And having a scalable security “dashboard” to monitor their organization’s security status was felt to be useful for them: 22% said very useful, 56% said moderately useful, and 22% said slightly useful.

Cyber Security Importance to Ensure Reliability and Resilience

A strong majority (82%) said that cybersecurity was very important to ensuring the electricity grid reliability and resiliency. Fewer said cybersecurity was moderately (16%) or slightly (2%) important.
Providers of Cyberattacks Solutions

When asked who will provide the best solutions to thwart cyberattacks on utilities, respondents said: private industry software companies (42%), system integrators (27%), utility companies themselves (14%), or private hardware companies (9%). An “other” category (than these four choices) was chosen by an additional 9% of respondents.

IT-based Security Solutions – Securing the Electrical Grid

Two final statements were provided and respondents were asked for their level of agreement. The first statement was: “IT-based security solutions are sufficient for securing the electrical grid.” About half (48%) agreed with this statement (7% strongly, 41% somewhat) with slightly more (52% disagreeing (28% somewhat, 24% strongly). Slightly more than half of the sample believed more than just IT is involved in securing the electrical grid.

Who will provide the best solutions to thwart cyber
attacks on utilities?
(figure 19, source: Zpryme)

How much do you agree with this statement: “IT-based
security solutions are sufficient for securing the
electrical grid.”
(figure 20, source: Zpryme)
Need for Cybersecurity Legislation

The second statement was: "The recent Senate-rejected Cybersecurity Act of 2012 was an important piece of legislation and greatly needed by the electricity industry." A large majority (73%) agreed with this statement (19% strongly, 54% somewhat), while fewer (28%) disagreed (22% somewhat, 6% strongly). Nearly three-fourths of this sample believed the Cybersecurity Act should have been passed.

The recent Senate-rejected Cybersecurity Act of 2012 was an important piece of legislation and greatly needed by the electricity industry. How much do you agree with this statement? (figure 21, source: Zpryme)
Zpryme Outlook

Utilities are becoming increasingly cognizant of the fact that their electrical systems and networks face many credible threats. Smart Grid rollouts across the globe further provide more 'entry ways' for potential threats to cause electrical disturbances. In the short-term, utilities will focus on preparing a plan of action to secure the most vulnerable part of the grid. Thus, field proven systems and technologies that can increase the security for end-users and the distribution system will be in high demand among utilities. The focus on Smart Grid cybersecurity will also demand higher budget allocation to technologies that enhance grid security.

Although many utilities will hold-off on large scale cybersecurity investments until well defined standards are in place, forward looking utilities will be the first to install the best of breed cybersecurity, irrespective of costs and standards.

The high demand for grid security products will bring multiple key and niche players in the market. However, niche players will face an uphill battle with utilities if they do not have previous experience working with the electrical sector.

Creating a 'hacker-proof' electrical grid is going to take five to ten years, but utilities with a long-term vision and plan to secure their grid will be best able to mitigate the losses associated with cyberattacks.
About Zpryme Smart Grid Insights:

Zpryme-powered Smart Grid Insights Publication, Practice and Advisory Board help organizations understand their business environment, engage consumers, inspire innovation, and take action. Zpryme Smart Grid Insights represents an evolution beyond traditional market research and consulting; combining sound fundamentals, innovative tools and methodologies, industry experience, and creative marketing savvy to supercharge clients’ success. At Zpryme, we don’t produce tables and charts; we deliver opportunity-focused, actionable insight that is both engaging and easy-to-digest. For more information regarding our custom research, visit: www.zpryme.com.

Zpryme Smart Grid Insights Contact:

smart.grid@zpryme.com | +1 888.ZPRYME.1 (+1 888.977.9631)
www.smartgridresearch.org (Zpryme Smart Grid Insights)

About ViaSat

ViaSat delivers fast, secure communications, Internet, and network access to virtually any location for consumers, governments, enterprise, and the military. The company offers fixed and mobile satellite network services including Exede® by ViaSat, which features ViaSat-1, the world’s highest capacity satellite; service to more than 1,750 mobile platforms, including Yonder® Ku-band mobile Internet; satellite broadband networking systems; and network-centric military communication systems and cybersecurity products for the U.S. and allied governments. ViaSat also offers communication system design and a number of complementary products and technologies. Based in Carlsbad, California, ViaSat has established a number of locations worldwide for customer service, network operations, and technology development. For more information about ViaSat, please visit: www.viasat.com/critical-infrastructure-security

White Paper Credits:

Zpryme:
Managing Editor
Megan Dean
Sr. Research Analysts
Roger Alford, PhD
Paula Smith
Research Lead
Stefan Trifonov
Nivedita Wantamutte

ViaSat (Expert Contributor):
Brett Luedde (brett.luedde@viasat.com)
Director, Critical Infrastructure Security Secure Network Systems

Disclaimer:

These materials and the information contained herein are provided by Zpryme Research & Consulting, LLC and are intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. These materials and the information herein is provided as is, and Zpryme Research & Consulting, LLC makes no express or implied representations or warranties regarding these materials and the information herein. Without limiting the foregoing, Zpryme Research & Consulting, LLC does not warrant that the materials or information contained herein will be error-free or will meet any particular criteria of performance or quality. Zpryme Research & Consulting, LLC expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, fitness for a particular purpose, noninfringement, compatibility, security, and accuracy. Prediction of future events is inherently subject to both known and unknown risks, uncertainties and other factors that may cause actual results to vary materially. Your use of these and the information contained herein is at your own risk and you assume full responsibility and risk of loss resulting from the use thereof. Zpryme Research & Consulting, LLC will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials and the information contained herein.
INTELLIGENT RESEARCH FOR AN INTELLIGENT MARKET