GRIDTALK
POWER UTILITIES COMMUNICATIONS E-ZINE

PROTECTING YOUR INVESTMENT IN TRANSFORMATIONAL RELIABILITY AND EFFICIENCY

A secure smart grid protects its transformational intelligence and delivery efficiency. Back in 2000 we had only the haziest vision of the services and applications that now adorn our internet. The same is true now as we look forward to what smart grids will do for us. A central internet lesson that we can apply to the smart grid is to build in security to protect key network assets and data privacy.

The secure delivery of energy has become critical – even a matter of national security – and that's because we have become more dependent on it than ever before. Just as important, protecting the privacy of the vast amount of usage information generated by the smart grid is an essential part of its value equation and critical to its widespread success.

Energy has become integrated with our cultural values as we become increasingly aware of its impact on our lives. As a result we are transitioning into a culture that wants to be increasingly in control on "how" and "how much" we are consuming, with the assurance that our energy supply will be reliable and our usage patterns kept private. Ultimately, today's energy "consumer" is going to rapidly become tomorrow's energy "customer," along with the intimacy that this transformational technology can bring. As long as you address security on all levels, the smart grid will flourish and blossom, lending unprecedented value and potential to the power generation and delivery landscape. The trick is to be informed and prepared.

These four articles examine the challenges and solutions for smart grid security from the perspectives of four distinguished industry experts – from an academic's insights into the cutting edge of smart grid data privacy and policy, to the unique aspects of securing a major distribution network from those who already have done so, to a distinguished market researcher's views on how smart grid security brings value to the power ecosystem even as it changes the business models of smart grid companies and their partners.

SUBSCRIBE: www.alcatel-lucent.com/blogs/gridtalk/

CONTACT: lynn.hunt@alcatel-lucent.com

VISIT: www.alcatel-lucent.com/smartgrid

SOCIAL VIEW

ENSURING SMART GRID SOCIAL ACCEPTANCE BY SECURING DATA PRIVACY

The game-changing value of the smart grid is driven in large part by entirely new classes of consumption data generated by …

ECONOMIC VIEW

SMART GRID SECURITY: AN IMPERATIVE INVESTMENT FOR SMARTER CONTROL

Security concerns for the smart grid are driving investment, partnerships and government regulation worldwide, leading to …

CUSTOMER VIEW

ALTALINK: IMPLEMENTING AN END-TO-END SMART GRID SECURITY STRATEGY

In 2010 Alberta's largest electricity transmission provider, AltaLink, set out to upgrade the distribution and …

EXPERT VIEW

PROTECTING THE SMART GRID WITH TODAY'S SOLUTIONS

The primary objective of the smart grid is securing the supply of energy and making sure that it will remain viable in the …

ENSURING SMART GRID SOCIAL ACCEPTANCE BY SECURING DATA PRIVACY

WITH: REBECCA HEROLD, NIST SMART GRID INTEROPERABILITY PANEL PRIVACY GROUP LEADER AND INFORMATION PRIVACY, SECURITY AND COMPLIANCE CONSULTANT, AUTHOR AND INSTRUCTOR

HIGHLIGHTS

- **New classes of energy consumption are creating privacy concerns. Securing and managing this data will support customer buy-in and deployment success.**
- **Smart grid companies and government regulators currently are working together to define issues, best practices and technology for securing data privacy.**
- **Complacency is not an option in the face of social adoption of the smart grid. Utilities and partners need to address privacy issues early, and in an open, objective manner.**

The game-changing value of the smart grid is driven in large part by entirely new classes of consumption data generated by smart meters. That raises privacy concerns, since robust tools can now perform deep analysis on much richer data, revealing new levels of intelligence on customers and their personal activities. How smart grid companies and their partners work with customers to secure and control the use of this new data use could profoundly impact customer buy-in, government support and, ultimately, any deployment's success.

"The smart grid has great possibilities, but anyone making decisions about deployments must address the security and privacy issues that come along with it," says Rebecca Herold, a privacy expert who leads the Smart Grid Interoperability Panel Privacy subgroup of the U.S. National Institute of Standards and Technology (NIST). "Privacy involves much more than just confidentiality. It also includes giving individuals control over who their data is shared with, how it is used, and how long it is retained."

NEW TYPES OF DATA RAISING THORNY PRIVACY ISSUES

Herold notes that the smart grid's ultimate social acceptance and success depends upon utilities securing four increasingly sensitive categories of privacy:

- **Privacy of Personal Information:** The traditional focus of customer data privacy, this involves protecting such information items as names, addresses, credit cards and bank accounts from identity theft and other types of inappropriate use.
- **Privacy of the Person:** As smart meters become more sophisticated in the future, they increasingly could reveal a greater fingerprint of energy usage, and more information about an individual's medical or physical issues that previously weren't visible. "One example would be someone who has to be hooked to some sort of electric device to get medications in order to continue life functions," says Herold. "What if this information was shared with the energy customer's health insurance company? How could that impact health insurance rates and coverage?"
- **Privacy of Personal Behavior:** "Smart grid data can reveal when someone is cooking in the kitchen or in their hot tub and what time they were there and so on," Herold notes. "This provides a virtual peak inside of a person's home, and not only presents a safety risk if it should get into the hands of burglars and vandals, but could also be misused by many other types of entities, such as target marketers, investigators and even employers."
- **Privacy of Personal Communications.** "Communications devices and smart appliances within the home may share too much information about your activities," says Herold. This goes beyond tapping a phone line. Smart appliances have already been rigged to send emails, and even post messages to Facebook and Twitter whenever certain activities occur. These in-home energy activities triggering automatic communications are new with the smart grid.

Herold says that consumers are concerned that their smart grid data might be shared not only with third-party marketers, but with other business and government entities. "They are asking 'will the government use smart meter data to see if I am using too much energy on a particular day and tax me higher as a penalty for doing that?'" Herold notes. "They also are worried that insurance companies may use this energy data to, for example, void fire coverage in a case where a house burns down as the result of a kitchen appliance being overused or misused."

PLUGGING SECURITY HOLES

Ensuring smart grid data privacy is a collaboration of policy, partners and technology. A smart grid company should first comprehensively identify the privacy risks involved, then establish the policies and procedures to address them. That should be followed by implementation of security technologies and best practices that can support the solution, including systems that limit access to the data to only those who truly need it in the performance of their business responsibilities and functions.

Herold believes that utility companies need to expand and clarify their privacy policies, stating whether they share customer data or will share only with certain entities, and under what circumstances they would do so. "If a utility has subcontracted with a third party to do any type of data collection for them, they need to consider what type of controls that entity has with regard to sharing the data, unless they've obtained consumer consent to do so," she notes. "They may want to take actions to make sure that the third party is not using the data in ways beyond that for which they were contracted to do the work."

Good policies and procedures within the utility itself are also important. "I'm finding a lot of people come to me and say, 'My utility company can't answer my questions about how my data that's collected in the smart meter is going to be used, or even what type of data is kept in the smart meter,'" Herold says. "Utilities should make sure that their own personnel receive training so that they are informed – that they know and understand what is actually going on in these smart meters and the data that's involved and how it is shared."

DEFINING AND REGULATING PRIVACY

In the absence of (or sometimes despite) regulations, rules or contractual restrictions, third parties in a range of industries have taken the data they've obtained through their business partner relationships and have used it for questionable, and in some cases even illegal, purposes, leading to a wide spectrum of privacy breaches, from spamming to disclosing data to others who have used it for criminal activity.

"Currently in the U.S. there are no Federal laws or regulations that clearly define the protections required for anybody who has energy data, regardless of where it came from," Herold says, though she points out that efforts to address the issue exist at all levels of government, as well as among privacy groups such as the Electronic Privacy Information Center and the Electronic Frontier Foundation and energy industry groups, such as the North American Energy Standards Board (NAESB) and others.

The U.S. Department of Energy recognizes the importance of having rules in place to address the unique data privacy issues of the smart grid, and is actively creating guidelines for legislation and regulations that will be coming down the line. "The DoE, Department of Commerce and other agencies and state lawmakers have taken the recommendations that we provided in NISTIR 7628, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid", (http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf) and have put together reports that are circulating right now throughout Washington," Herold states, "Such as the DoE's report "Data Access and Privacy Issues Related to Smart Grid Technologies" (http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf)

Some states such as California, Oklahoma and Colorado already have laws that specifically address the smart grid, while state public utilities commissions (PUC's) are looking at creating their guidelines and their rules for their own state utilities. "We have several members of our privacy group who are from the state PUCs in places such as California, Ohio and New Hampshire who are participating because they want to hear some of the best ways to address the privacy issue and also get the perspectives of the utilities and the privacy advocates at the same time," says Herold.

SOCIAL IMPACT

The bottom line in all of this is making sure that energy consumers are comfortable in having a smart meter and participating in a demand response program – knowing that their personal energy data is secure and is being used and shared appropriately.

Herold warns against complacency in the face of social adoption of the smart grid. "If you take the attitude that there's nothing to worry about, and if you only consider privacy in its more conventional sense – that it is simply about name, address, credit card number – then you're not going to be able to really address the new issues that the smart grid brings with it. It's important for utilities and any other involved entity to have someone assigned to address these privacy issues in a very open, objective way, and also be ready to answer consumer questions about them."

SMART GRID SECURITY: AN IMPERATIVE INVESTMENT FOR SMARTER CONTROL

WITH: ROBERTA BIGLIANI, HEAD - EUROPE, MIDDLE EAST & AFRICA, IDC ENERGY INSIGHTS

HIGHLIGHTS

- **Smart grid security is increasingly recognized as an investment imperative – one that leads to greater reliability, efficiency, customer acceptance and profitability.**
- **Regulation can serve as an important engine for change, driving partnerships that will add value to the ecosystem.**
- **The global smart grid security ecosystem is evolving and consolidating, creating an end-to-end value proposition that makes security both stronger and more cost effective.**

Security concerns for the smart grid are driving investment, partnerships and government regulation worldwide, leading to substantive changes in the business models for power suppliers.

Smart grid security is a cost that is increasingly recognized as an investment imperative – one that leads to greater reliability, efficiency, customer acceptance and profitability. "When the smart grid was first starting to be debated, the concern about cyber security was obviously there, but it was not one of the priorities," says Roberta Bigliani, Head – Europe, Middle East & Africa, IDC Energy Insights. "Over the last years, however, things have radically changed because of new threats such as viruses designed to attack operational control systems like SCADA. So while it previously thought that cyber security was for enterprise IT systems, these types of attacks have broadened the perspective."

This new priority is reflected in IDC Energy Insights' latest security compliance and governance survey, conducted among 600 security professionals across Asia/Pacific, Europe, Middle East and Africa (EMEA) and Latin America. Consider these findings for the EMEA region:

- About 71.4 percent of utilities have a documented and approved IS strategy in place, as compared to the 59 percent cross-industry average.
- Driven in large part by security concerns, a significantly smaller percentage of utilities (8.2 percent) are prepared to accept some area-specific vulnerability as a cost-saving measure compared with other industries (20.3 percent).
- The utility sector's spending in security software will grow with a compound annual growth rate of 9.4 percent from 2010 to 2014, higher than the growth of the utilities spending on total software (6.6 percent).
- "The more the vision developed around the smart grid, the more people talked about interoperability, the need for standard platforms and protocols – all of these things have been raising the bar of interest in cyber security," Bigliani notes.

REGULATION CREATING INCENTIVES FOR SECURITY INVESTMENT

Wherever power providers are located, from Asia to Europe and North America, regulation serves as both a barrier and incentive for smart grid security investment. Regulatory agencies tend to move slowly and cautiously, which often can restrict smart grid development, yet these same bodies also serve as an important engine for change, driving partnerships that will add value to the ecosystem.

A case in point is the Dutch distribution power company, Alliander, which between 2009 and 2011 spent €2 million to certify the data privacy of its meters. The initiative started after the Dutch Minister of Economic Affairs, concerned about data privacy, repealed a proposed mandate for smart metering deployment. Alliander very quickly realized that it had to look for new approaches to address consumers' concerns about data privacy, and undertook the project to become "certified compliant" in its deployment of smart meters. Working with diverse business partners, Alliander identified over 300 detailed criteria that needed to be brought into compliance, addressing technological, procedural, organizational and policy controls.

Regulation is essential to fully enable cross-industry partnerships like these that will bring additional value to smart grid services, for example allowing power suppliers to fully leverage such advantages as telecom cellular infrastructures and services for IP network extension, smart metering, backhaul communications and enriched customer experience.

Bigliani notes that even in a complex regulatory environment, algorithms can be used to identify tariffs to offset different

pieces of investments that can be used in different ways. A report published by industry group Eurelectric found that Europe's distribution system operators, which are regulated businesses, lack adequate incentives to invest in smart grid technology, and urges national regulators to establish a more intelligent approach to grid tariff regulation models, taking the needs of an energy-efficient power system and a low-carbon economy into account.

"If the business case of investment is good enough, you are in reality making the entire system cost lower because you can avoid other operational costs – and if that's the case, of course society and the economy will benefit," Bigliani says.

FUKUSHIMA'S IMPACT ON SECURITY AND IT SPENDING

Bigliani believes that the disaster at Japan's Fukushima nuclear generating facility will ultimately impact positively on the worldwide industry's safety and environmental applications, as well as on its economics. "If you want to increase safety and security, you need to have more information, better organization, better analytics, better procedures – all things that are supported by IT and the businesses that support it. Collaboration technologies will also be positively impacted, as we have learned from this and other tragedies that it is difficult and dangerous to have a company working in isolation from others."

Security in this case means that all of the transactions and information needs to be in the hands of regulators, partners and other agencies and bodies that are responsible, and they need to be shared in a secure way. This will help prevent accidents and a quicker response when they do happen. At the same time, Bigliani says that utilities will be seeing a corresponding increase in cost, which could slow the reaction a little somewhat, so they will have to identify spending priorities.

VALUING SECURITY CONCERNS IN THE SMART GRID ECONOMY

As illustrated by Alliander's meter certification project, the global smart grid security ecosystem is evolving and consolidating, with numerous acquisitions, coalitions and alliances. The effect is to create an end-to-end value proposition that makes security both stronger and more cost effective. Bigliani says that it is important for power providers to share experiences, seeking public and private projects and experience that can be replicated everywhere. She sees the new smart grid economy as encompassing a holistic relationship among all of its stakeholders, with security a top priority.

- **Consumers:** Data privacy and protection is an important aspect of the value consumers assign to smart grid investment, and how it impacts their own budgets.
- **Businesses:** Utilities and their ecosystem partners must treat cyber security as a number-one priority – as an integrated part of smart grid rollouts and associated products.
- **Government/National:** Standards issued by working groups of industry participants and experts will help the different operators to have security in place. Cyber security and data privacy are on top of the agenda and are the focus of specialized task forces.

Ultimately, the investment priority for the smart grid cyber security is clear to Bigliani. "The perimeter of risk for utilities is expanding," she states. "This is not the time to reduce the budget for security and compliance. Accepting vulnerabilities as a cost-saving measure is unacceptable."

ALTALINK: IMPLEMENTING AN END-TO-END SMART GRID SECURITY STRATEGY

WITH: CLINT STRUTH, PRINCIPAL ENGINEER IN TELECOMMUNICATIONS NETWORKING AND WITH CORY STRUTH, NETWORK ARCHITECT, ALTALINK

HIGHLIGHTS

- **AltaLink has secured its smart grid network with multiple layers of protection from control room to substation edge points.**
- **AltaLink's multi-tier security concept makes full use of IP/MPLS intelligence, flexibility and control, and includes strong attention to managing the human dimension.**
- **AltaLink sees security as an integral aspect of any deployment – one that should be trumpeted from the upper management down through the organization.**

In 2010 Alberta's largest electricity transmission provider, AltaLink, set out to upgrade the distribution and communications infrastructure along its 12,000 km transmission grid in western Canada. Now in the second year of a four year build, its smart grid upgrade has reached more than 65 of its 300 substations. With support for general utility SCADA alongside teleprotection, engineering operations and other operational and corporate voice and data traffic, AltaLink has secured the network with multiple layers of protection that reach from control room to substation edge points.

"In addition to our focus on unauthorized access from the Internet, the command and control portion of the network is certainly a big concern, so architecting the control plane for maximum security on the MPLS network is a paramount," says Clint Struth, AltaLink's Principal Engineer, Telecommunications and Networking. "We also have numerous people, some of whom are not employees but on contract, who are physically inside our facilities, and we don't always have control over what they're doing, so certainly edge-level protection is also critically important."

AltaLink's multi-tier security concept makes full use of IP/MPLS intelligence, flexibility and control. Its intrusion-detection system of checkpoints for all users includes: Centralized authentication and logging

- Security policies for each service through access control lists, MAC-pinning, IP and bandwidth filters
- A centrally-managed and monitored firewall at every substation
- A per-service firewall policy for nodes bringing services into substations via a Layer 2 Virtual Private Network (VPN)
- Comprehensive password protection at different levels, which allows users to be quickly isolated and locked out, if necessary.

"We deploy industry best practices," says Cory Struth, AltaLink's Network Architect. "It's a default deny policy unless a particular access or action is permitted, and that applies to all levels of the network. We have centralized user management so that there is one button to push to take everybody off if necessary. On the edge we're looking at not just firewall but also IDS and IPS technologies. Pro-active monitoring fingerprints common and identified traffic, and alerts you to that being present. So there's a proactive force, a reactive force, and a design component that all fit together."

INHERENT SECURITY WITH MPLS

MPLS network architecture provides a high level of data security since there's a separation of the control and data planes – something the Struths see as a key benefit in protecting AltaLink's smart grid services. "If you were not to give the proper and due attention to securing your control plane, it could perhaps be more of a target just because it's IP," notes Cory. "However, the payload is encapsulated within an IP packet wrapped in MPLS labels. This affords an inherent level of security while in transit. Ultimately, it's really about how you secure your management platform."

The Struths note that teleprotection services are well protected on the network. "We run a QoS policy on the converged network backbone links on the transport side," says Cory. "Teleprotection is basically number-one on the list after network control packets. That's more about traffic engineering, though. The security of the teleprotection is basically encompassed in the overall security of the MPLS protection itself."

AltaLink's MPLS architecture provides a rigid service demarcation and separation of traffic while being label-switched across the network. Consequently, any reliability or security-related issues come into play occur more on the edge. "The edge is where you need to have a robust and scalable firewall solution that can handle converged services and apply a per-service security policy to your traffic when it's egressing an ingressing the network," Clint states. "The key is how you design that edge-level architecture, for example where you have one given port in substation that handles many services."

THE BIGGEST CHALLENGE: DEALING WITH THE HUMAN DIMENSION

As utilities evolve their communications technologies to support smart grid, they need to consider the impact of the human dimension on security. The Struths believe that implementing a technology or hardware solution is relatively easy in the grand scheme of things, whereas trying to change the human side of it, shaping a human mindset around a fully comprehensive security policy, is a much more difficult task.

"The technology itself is maybe 30 to 40 percent of the equation, with the human aspect the bigger wildcard in the whole migration," Clint notes. "Trying to get the people to buy in, learn the technology, and fully understand it and be capable with it is a much more difficult process. You've got to have the HR side of it, with the staff understanding the implications of security and why they have to be diligent about it."

The Struths add that firewall solutions or installing video surveillance at critical substations are tools, but not really security. "They will alert you if something is not normal, but you still need intelligent eyeballs looking at it to make an assessment as to what the threat is," says Clint.

SECURITY AND ULTIMATE BUSINESS SUCCESS

Clint and Cory Struth strongly believe that success for smart grid companies is critically tied to security – an integral, core aspect of any deployment that should be trumpeted from the upper management down through the organization in the same way that safety currently is in the electric power industry.

"The impact of a security breech is becoming much more serious to a company's bottom line and public reputation," Clint states. "Vulnerabilities need to be addressed and mitigated very early on.

As networks become IT aware, it may only take a few large security breaches to drag this transition to a halt. The whole industry needs to take a very comprehensive approach to network security very early on."

"You're seeing it in the news…Sony, Citibank, Amazon…even Google. They're all getting hacked," adds Cory "Security for the next five years is going to be front and center in everyone's mind. If you're not thinking about it now, it's going to be driven home through a variety of means. Cybercrime is taking off. People do want to own your network. This isn't just vandalism and changing your web page any more – it's getting into your network to control it, stealing your intellectual property and your money. You have to have defenses in place in case someone comes knocking on your door."

PROTECTING THE SMART GRID WITH TODAY'S SOLUTIONS

WITH: PETER JOHNSON, VICE-PRESIDENT SMART GRID, ALCATEL-LUCENT

HIGHLIGHTS

- **The emerging imperatives for smart grid security include getting a consistent level of the world's attention on the issues, and then implementing solutions in a productive fashion.**
- **From a security standpoint, it is extremely important for any utility to ensure homogeneous standards and applications across is entire smart grid solution, and before it is deployed.**
- **Although security considerations in the smart grid ecosystem can be varied and complex, the architecture, tools and expertise exist to fully address these issues now.**

The primary objective of the smart grid is securing the supply of energy and making sure that it will remain viable in the future. That means that we must keep grid itself safe from malicious attack or misuse while protecting the privacy of rich consumer data it generates. Although security considerations in the smart grid ecosystem can be varied and complex, the architecture, tools and expertise exist to fully address these issues now.

The one big difference between smart grids today and the conventional systems that came before is, of course, the move to converged IP/MPLS networks and the unprecedented level of timely reporting and control they enable. A key characteristic of this new model is that communications and other critical data are no longer contained inside traditional network boundaries, but now reach out to the edges where there is more opportunity for interception or attack, which means that more devices have to be protected.

Utilities also need to be concerned with the privacy of network data – for example, overall consumption and performance, how individual substations are performing, and the usage patterns of customers. How those factors are addressed will be highly dependent on the regulatory environment in each country and at various levels of local government and society.

Effective smart grid security must also fully address the human element, for at the end of the day, the network and its security is only as good or as strong as the human processes that support it. If a utility's processes are not well thought out and strictly enforced – if they either allow someone to deliberately misuse the network, or to accidentally do something that will jeopardize its functionality without any tracking or logging, then they have failed. The consequences of not addressing the human element will have an immediate and direct effect on energy supply.

Ultimately, security in all of its forms serves the purpose of making sure that there is a continual supply of affordable energy when you need it through widespread adoption of the smart grid environment by all stakeholders, from government to partners and consumers. For that you need to make sure that the grid itself is secure so that it can work as intended. The bottom-line benefit is more efficient use of energy.

ADDING VALUE THROUGH SMART GRID SECURITY

Solid security will add value to any smart grid deployment in two very fundamental ways. In its most tangible form, it protects the investments of the utility and of its customers by making sure that the control signals get through, that the measurements are returned, and that the entire value chain, from the generator down to the customer and back again works efficiently and continuously. It ensures that power supply is not interrupted, degraded, or otherwise compromised. The Stuxnet attacks last summer, which were targeted at a very specific type of equipment, are indicative of the sorts of threats we will see more often in the future.

A more intangible, but equally important value is the confidence the user community has that a utility's business will not be interrupted. So much business today depends on the reliable availability of electricity, that the failure of the power grid will have immediate impact. This is not something you can measure in straight dollars in utility accounts, but it does have direct impact on the ability of the community to do business safely and create more prosperity.

SECURITY BENEFITS AND CHALLENGES IN THE SMART GRID ECOSYSTEM

Global smart grid initiatives are fueling a rapidly expanding environment of collaboration among companies in the power, telecom and IT sectors. This activity is creating a new ecosystem that leverages diverse knowledge and technology for great benefit.

With so many players in the game, standards and solutions interoperability are the unifying glue of the modern communications infrastructure, and are essential for unprecedented levels of security and efficiency. This new level of interoperability has to be robust, and has to encompass all the component parts of the solution being deployed. Communication supported by IP/MPLS architecture is its key foundation and enabler, bringing greater cohesion to all operations and allowing security to be managed as a homogeneous whole.

Open standards in the security space are helping to ensure that smart grid utilities are strengthening their ecosystem, and that the partners within any particular ecosystem are well aligned on every level. Now that we are all talking to each other, highly effective security can be designed into a deployment, and it will be far stronger and more effective than anything that has come before because it has that homogeneity across the three contributing sectors. We at Alcatel-Lucent make sure that our solutions are open so that utilities aren't locked into a narrow set of vendors that could limit their operational and security effectiveness.

SMART GRID SECURITY AND ADOPTION

Regulation is the key enabler of the smart grid; and it also can be the obstacle. Generally utilities will only react to regulations since the regulators authorize investment, so cyber security tends to be driven by what regulators require. In North America the path forward is very clear, entailing very strict adherence to the standards and compliance enforcement established by North American Electric Reliability Corporation's Critical Infrastructure Protection program (NERC CIP). That's not the same in other countries, where the attention being given to the security of the grid can be considerably lower.

When it comes to data privacy, best practices are not as well defined at this point, and utilities can be constrained by local rules and regulations.

Whatever the political situation governing these areas, in both cases the role of Smart Grid technology is to provide the tool set that allows the utility to adequately protect its network and meet its obligations to both regulators and customers.

ACTING ON SMART GRID SECURITY NOW

The emerging imperatives for smart grid security include getting a consistent level of attention around the world for the issues, and then implementing solutions in a productive fashion. Central to this is the absolute imperative to design in security from the outset of smart grid design, and not to try and add it in after the fact.

Alcatel-Lucent not only understands the utility industry extremely well, but offers a wealth of unique expertise in communications and the security surrounding both data and communications. What we bring to the smart grid ecosystem is the understanding of security's imperative needs, and the tool set that allows the utilities to address them. We've got the tools both built into our products and within our solutions that allow us to protect the access, protect the data, and neutralize the threats. That adds up to an immense value that we are bringing to this industry and to smart grids. The expertise exists now, and every day is ensuring that smart grids are reliable, efficient, and secure.

SUBSCRIBE: www.alcatel-lucent.com/blogs/gridtalk/

CONTACT: lynn.hunt@alcatel-lucent.com

VISIT: www.alcatel-lucent.com/smartgrid

Alcatel·Lucent