EDJ The IEDC Economic Development Journal

734 15th Street, NW Suite 900 • Washington, DC 20005

Volume 12 / Number 3 / Summer 2013

When the Lights Go Out

By John A. Adams, Jr., Ph.D., CEcD

CYBER THREATS TO CRITICAL INFRASTRUCTURE

The wired world we live in today has proven both a tremendous boost to the economy as well as a potential for disruption. The purpose of this article is to introduce an awareness overview to economic developers and local leaders who daily work with public and private entities that are impacted by cyber threats. No longer is the realm of cyber threats left only to the IT experts. In today's connected world, the economic development community needs to have a heightened awareness of how cyber-attacks can impact the safety and security of their communities and regions.

when the lights go out

By John A. Adams, Jr., Ph.D., CEcD

Cyberspace has fundamentally transformed the global economy. Cyberspace is the new frontier – the new domain – full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers. These threats are real and they exist today. A cyber-attack perpetrated by nations, state or violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist could virtually paralyze the nation.

Imagine the impact an attack like that would have on your company or your business. For example, we know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems [SCADA] that operate chemical, electricity and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems; that could contaminate the water supply in major cities or shutdown the power grid across large parts of the country.

The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective results of these kinds of attacks could be a cyber-Pearl Harbor, an attack that would cause physical destruction and loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.

Secretary of Defense Leon E. Panetta
October 11, 2012

John Adams , Ph.D., CEcD, is a program manager for Knowledge Engineering at Texas A&M-TEEX, College Station. (john.adams@teex.tamu.edu)

The remarks of former Secretary Panetta highlight the tremendous amount of concern and attention on the identification and protection of critical infrastructure and key resources (CIKR). For decades, as we felt insulated from outside terrorist attacks, security was sacrificed for the economy of operations, expanded market demands, and low cost service. Outside of government regulations on safety, monopolies, and interstate trade – growth and market share have been the engine of the big four infrastructure services: electricity, telecommunication, water, and oil and gas. Prior to 9/11, infrastructure was generally taken as a given and few, other than the military and local base operations, raised the question of what should be protected and how? Our nation had been insulated from homeland disruptions and "attacks."

Protection of each critical infrastructure component is paramount, yet the electric grid is the most important element to the overall economy, security, and safety of the nation.

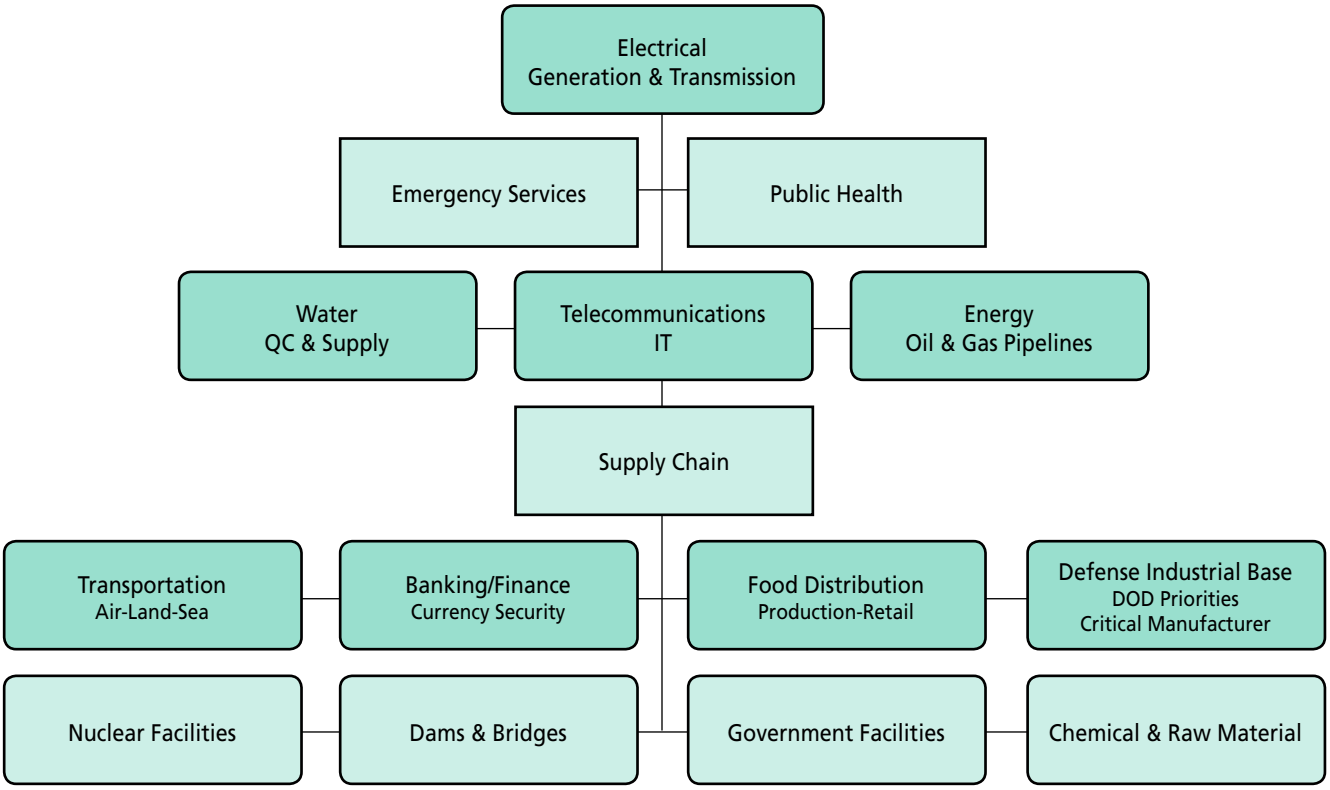
While there have been veiled incidents against the homeland, such as espionage threats and penetration of U.S. war production during World War I and German U-boat patrols in the Gulf of Mexico off New Orleans during World War II – the last time we were attacked at home was two centuries ago, during the War of 1812, when the British burned the White House. This all changed on 9/11, as cyber expert Ted Lewis notes: "The devastation of 9/11 demonstrates that attacks on the infrastructure can result in massive casualties, sizeable economic, political, and psychological damage, not to mention damage to the American psyche."[1]

Protection of each critical infrastructure component is paramount, yet the electric grid is the most important element to the overall economy, security, and safety of the nation. (Figure 1) Electricity is the lifeblood of today's modern world and a prime necessity for all citizens. It powers economies, consumer conveniences, national security, critical tele-

CYBER THREATS TO CRITICAL INFRASTRUCTURE

The wired world we live in today has proven both a tremendous boost to the economy as well as a potential for disruption. The purpose of this article is to introduce an awareness overview to economic developers and local leaders who daily work with public and private entities that are impacted by cyber threats. No longer is the realm of cyber threats left only to the IT experts. In today's connected world, the economic development community needs to have a heightened awareness of how cyber-attacks can impact the safety and security of their communities and regions.

FIGURE 1 CRITICAL INFRASTRUCTURE HIERARCHY



Sources: White House. Executive Order 13010, Washington, D.C.:1996; White House. Comprehensive National Cyber Initiative (CNCI). July 2008; GAO. "Critical Infrastructure Production." December 2011

communications, and the industrial production/supply chain ability to deliver competitive advantages to global markets. Given the efforts to provide sector specific cyber information and procedures, there is a "plethora of guidance available" to manage and protect our critical infrastructure.

Cyber-note: Security is only as strong as its weakest link. The best attackers know instinctively to look for that weak link.

Each element of our overall infrastructure is vitally important; the simple fact remains that the cascading impact of local and regional failure of electrical power will impact all primary services – especially water, telecommunication, and oil and gas. The vastness of the country has resulted in the evolution of the interconnection of the power grid connecting over 3,000 power providers, generating more than 800 megawatts transmitted over more than 210,000 miles of transmission lines. Thus, in this review of the critical infrastructure, each critical sector will juxtapose a position against the role electricity has in the delivery, safety, security, and impact of any event that would diminish and disrupt overall service.[2] (Figure 2)

Disruption of the electric power grid can happen at a number of points, yet the most critical is at the site of generation, followed by the transmission to customers. While both are important, the ability of a cyber-attack to penetrate the SCADA (Supervisory Control and Data

FIGURE 2 INVENTORY OF CRITICAL INFRASTRUCTURE

Energy	5,800 power plants 824,847 oil and gas producing sites
Transportation	5,179 public airports 140,000 miles of active railroad with 21,178 passenger miles 600,000 bridges & tunnels 2.5 million miles of pipelines 361 ports
Telecommunications	2 billion miles of fiber and copper cable 14,000 radio & 1,700 television broadcasting facilities 252,000 cell phone towers 293 million wireless subscribers
Agriculture and Food	2,200,930 farms 28,000 food-processing plants
Water	1,048 federal reservoirs 14,780 public wastewater treatment facilities
Public Health	5,754 registered hospitals
Emergency Services	19,971 EMS agencies
Banking and Finance	7,280 FDIC insured institutions
Postal and Shipping	151.5 million delivery sites
Key Assets	87,265 historic places 104 commercial nuclear power plants 84,000 dams 1,500 government-owned facilities

Sources: Department of Homeland Security, Department of Energy, Federal Energy Regulation Commission, Government Accountability Office and Department of Defense

Acquisition) systems that control electric production and delivery, some of which have outdated security features, presents a significant vulnerability. (Figure 3).[3]

FIGURE 3 TEN COMMON SCADA VULNERABILITIES

Common Vulnerability	Reason for Concern
* Unpatched published known vulnerabilities	Most likely attack vector
* Web Human-Machine Interface (HMI)	Supervisory control access
* Use of vulnerable remote display protocols	Supervisory control access
* Improper access control/authorization	SCADA functionality access
* Improper authentication	SCADA access
* Buffer overflows in SCADA services	SCADA host access
* SCADA data/command manipulation	Supervisory control access
* Structured Query Language (SQL) injection	Data historian access
* Use of IT protocols with clear-text authentication	SCADA host access
* Unprotected transport of application credentials	SCADA credentials gathering[4]

The potential attackers have far too much access to power providers and opportunities for a cyber-attack. Hackers and cyber-spies, from both nation-states and rogue groups, probe for the weakest link. They have already successfully penetrated our power grid at a number of locations that we know of and likely at locations we do not even know about. While rogue actors continue to explore ways to hack systems, the threat to the electrical power grid and other key infrastructures across the country long ago moved from amateur incidents to intentionally state-sponsored disruptive events and terrorism. According to the National Security Agency (NSA), both the Russian and Chinese intelligence networks have repeatedly probed the U.S. electric power grid for vulnerabilities. Thus, one of the most concerning aspects of cyber-attacks on the grid is that most "advanced persistent threats" (APT) have completely evaded detection. If and when a threat is detected, positive attribution as to source, scope of attack, and intent is often difficult.[5]

ADVANCED PERSISTENT THREATS

The range of attackers, including state-sponsored hackers, and the breadth of targets include intelligence gathering and high-value targets across many industry sectors and types of critical infrastructure. The scope of the APT is measured by the available resources and determination of the attacker. One element of persistence is the ability to adopt the attack to the target's security profile and neutralize access in order to extract data or disrupt critical infrastructure. Thus, this makes defending against APTs very problematic. The Director of the Counter Threat Unit of Dell Secure Works, Barry Hensley, noted, "The tools, procedures and other controls used to defend commodity security threats are often ineffective against targeted APTs. When actors are focused on a specific target, they customize and adopt their tactics, techniques and procedures to predict and circumvent security controls and standard incident responses."[6]

Such APT attacks can occur over months and years as the attacker responds to counter measures and explores security lapses. Once the hacker has gained access to the network, it is very difficult to rid the network of the intrusion. Stuxnet, Shady Rat, and Night Dragon are examples of highly successful APTs. The resourceful and adaptive adversaries generally have very specific targets and, when planned and encouraged by a nation-state actor, many times are executed by decentralized agents of the state. And the move to enhanced smart grids and cloud computing, while hyped as the "next best thing," is also the "next" great target for adversaries.[7]

In spite of new "smart grid" programs – new digital electricity networks – required by the Federal Energy Regulatory Commission (FERC) and supporting agencies, we are as a nation still highly exposed to APTs. This is due primarily because the utilities use commercial software operated over the Internet that has not been fully vetted and protected.[8] The smart grid is intended to open a new era beyond traditional grid interconnection and technologies – to enhance systems to be more flexible, accessible, secure, and reliable.[9] Notwithstanding, the power industry has expressed concern that coordination among agencies has been lacking and some have questioned whether FERC has the technical or intelligence-handling expertise to oversee hardening of the grid. Furthermore, there is a lack of enforceable requirements and standards thus making interoperability of the smart grid mandates costly and challenging. Blackouts from catastrophic electric power systems failure would produce significant cascading financial loss across the broader economy. An interdisciplinary approach to security measures is imperative to a robust cyber defense-in-depth.[10] (Figure 4)

Since some utilities do not think they are targets for monetary defalcation, espionage, or Internet theft, they fail to recognize the risk. The electric power industry is undergoing profound changes to address security concerns. Currently it is estimated that energy companies that do invest in computer/systems security are able to

The potential attackers have far too much access to power providers and opportunities for a cyber-attack. Hackers and cyber-spies, from both nation-states and rogue groups, probe for the weakest link. They have already successfully penetrated our power grid at a number of locations that we know of and likely at locations we do not even know about.

prevent about 70 percent of known cyber events. Increased spending, replacement of old systems, and employee training help reduce exposure, yet, there will always be threats. Despite the replacement of older equipment with "digital devices," exposure to hackers still remains a threat. Anywhere there is a digital system – from the generation plant to the smart meters to the home controls – the system is vulnerable to an ever-growing set of motivated and highly-skilled attackers.

The sophistication of new malware attacking systems, including zero-day attacks, control systems rootkits, and software has shown it is difficult to prevent and/or detect attacks. The simplest intrusions may be the most damaging. For example, new systems that allow home owners to remotely set their thermostats are a direct portal for hackers to penetrate. Furthermore, there is only modest sharing of cyber information between private utilities and government agencies.[11]

To date, there has been an alphabet soup of government agencies that have compiled extensive reports, data, and technical briefs, driving the creation of regulations and oversight that has done little more than cost the industry millions of dollars. Since most of the grid is owned by the private sector, there has been a natural push back to invest adequate funding to keep pace with security requirements. Safety is paramount and has been a world-class hallmark of the industry. As such, the security aspects – due to cost and oversight – have not kept pace with the increased threats. A number of risk management models have been developed to define techniques and methodologies to assess cyber-security risk. Electrical providers across the nation deal daily with risk, yet few have ever dealt with a cyber-attack. Thus, many questions remain – has management defined risk constraints, does each organization have a risk tolerance profile, do they know their cyber security requirements and have they organized them accordingly, and is there a creditable and flexible plan for recovery.[13]

Cyber-note: Cyber deterrence has to be repeatable because no feasible act of cyber-retaliation is likely to eliminate the offending state, lead to the government's overthrow, or even disarm the state. Thus, a state could attack, suffer retaliation, and live to attack another day.[14]

When the lights go out as a result of a cascading cyber-attack over a wide area of the country, there will be little concern for mission or vision statements, financial limitations, legislation, or stockholders. Elaborate outlooks promoting a "holistic" approach will be useless. The prime objective will be to safely assess the problem, defend against the threat – if possible – and restore service. Thus the most important objective of the industry working with government agencies at all levels is, and always will be, to first "frame the risk" as clearly as possible – given all the best data, training, and intelligence available; second, conduct a "risk assessment" which is shorthand for, what are the priorities?; and third, given the assessment of the situation and priorities, determine what will be the "response" or recovery time objective.

In a classic sense, risk management is the process of risk avoidance, mitigation, sharing and/or transference. What may initially appear as an isolated cyber-attack on a local system, could without the ability of the operators to act fast enough cascade into a statewide or regional outage. In other words, a "systems" attack could not only create damage and disruption to the grid, but escalate into widespread physical damage as vital services shut down and routinely sustainable basic services such as transportation, water, food supplies, and telecommunications are disrupted.[15]

As such, the security aspects – due to cost and oversight – have not kept pace with the increased threats. A number of risk management models have been developed to define techniques and methodologies to assess cyber-security risk. Electrical providers across the nation deal daily with risk, yet few have ever dealt with a cyber-attack.

FIGURE 4

A robust cyber security defense-in-depth strategy includes:

- Concise and accountable command and control guidelines
- Well defined and monitored boundary for controls of cyber authorizations
- Robust authentication, authorization, and accounting controls
- Restricting physical access to industry control system (ICS) network and devices
- Established risk tolerance and risk methodology: threats and vulnerabilities
- Monitored and defined encryption techniques for data processing and storage
- High-level cyber policies, procedures, authentication, and standards
- Documented purpose, functions, sensitivity, and capabilities of each function
- Clearly crafted roles and responsibilities for cyber incident response
- Implementing a network topology for the ICS that has multiple layers
- Secure assessment of organizational affiliations, access rights, and privileges
- Ensuring that critical components are redundant and are on redundant networks
- Operating standards that provide defense in depth and defense in breadth
- Clear requirements for implementing controls and cyber-attack response
- Robust operational standards for addressing high-impact risk
- Effective monitoring and measurements of cyber security programs[12]

RISK-BASED DECISIONS

Framing the risk depends on assumptions about the threats – how likely is the occurrence, can the initial impact be quickly measured, and what is in place to protect our perceived vulnerabilities. If a tree falls across a power line, the disruption is quickly noted, traced to the location, the grid is rerouted, and crews are dispatched to service the outage. Procedures are in place and action taken. In the case of a cyber-attack, a Trojan Horse or sleeper virus could go unnoticed for days or weeks, planting the seeds of corruption and doing unnoticed damage. The risk tolerance could be mishandled or misinterpreted because of false positive and false negative responses to system checks, and operators crippled by the speed of the disruption once it starts. In the event of such a catastrophic event, there will be only two key elements to addressing the attack and responding in kind.

The first and foremost element is a "trusted relationship" among all the players, both public and private, addressing the event. These relationships need to form long before such an incident, due to experience, training exercises, cyber education, and constant communication. The second critical item is communications; point-to-point over secure lines is paramount among vendors, those with interconnections to the system, and government agencies. Those with communications access should be based on a prequalified access control list. For example, security protocols need to be in place in writing and easily accessible long before an incident to allow third parties and vendor access to sensitive data and systems. When the lights go out, so do the cell towers, land lines, and given the presence of electromagnetic pulse or EMP – radio frequency traffic can also be disturbed.[16]

Cyber-note: security and the smart grid: It remains to be seen how the industry will guard the security and privacy of the data while also integrating smart metering data into the utility smart grid analytics frameworks.[17]

Incident response to a cyber-attack on the electric grid or sub-system will need an organization-wide response. Determination of the attack and resulting damage will be driven by the ability of all responders to mitigate the impact. A clear and informed assessment of the situation must occur followed by the development of alternatives to correct and defend against the attack. If in fact there is a multi-level attack regionally or in a specific area, the response could be a mixed approach to both the cyber damage and the resulting physical damage due to disrupted systems. At this stage, the government should engage economic development professionals and community leaders at all levels to participate in the response as well as coordinate the triage for the recovery.[18]

To insure a robust response to a cyber-attack, there needs to be a very clear chain of command to address the levels of priorities needed to combat the threat and insure recovery. It is imperative that command and authority are driven by the person in charge. There is always a concern that the experts who solve and lead the response and recovery will be undercut by those interjecting political clout or perceived authority – generally resulting in confusion, uniformed pronouncements, and costly delays in addressing the situation.

While attribution of a cyber-attack is important to federal officials, the immediacy of action takes low priority unless it is directly related to the immediate recovery of first responders against an imminent attack. Nevertheless, fresh forensic evidence is important, as long as it doesn't interfere with the first responders and recovery efforts.[19]

Thus, a better understanding of the means and impact of a cyber-attack should be key in training civilians, employees, elected officials, or responders who could and will come in contact with the results of a cyber-attack. Although volumes are written on these topics, awareness of the cyber threat must be conveyed in the clearest terms possible. The awareness is not for computer programmers, but for those who drive policy, economic development (recovery), and respond to cyber incidents.[20]

ACRONYMS

APT – advanced persistent threats

CIKR – critical infrastructure and key resources

COOP – continuity of operations plan

EMP – electromagnetic pulse

FERC – Federal Energy Regulatory Commission

HMI – Human-Machine Interface

ICS – industry control system

NSA – National Security Agency

RTO – response or recovery time objective

SCADA – supervisory control and data acquisition

SQL – Structured Query Language

FOOT PRINTING

The first step in hacking a system or network is to gather information. Attackers systematically glean data and information from whichever "door" they can find open or unprotected. Like a burglar in the dark of night casing a break-in opportunity, cyber attackers accumulate a systematic footprint of an organization, site, or component of the grid by completing a detailed profile on the organization's security posture. The ultimate strategies of a covert attack are to sift through the data to develop a list of intrusion detection systems, domain names, specific IP addresses, access control functions, and possible passwords. Such information is often found in open access sites across the Internet. Following a data probe, hackers can refine footprint information by identifying related companies, phone numbers, email addresses, and reviewing privacy policies. One of the best backdoor means of gathering data is developing a list of web servers and links related to the target. The more enticing the information, the easier it is to focus a hackers' attack.[21]

The threats to the critical infrastructure in transmission and distribution systems have not been reduced or fully managed but instead are becoming more and more complex and growing. (Figure 5) The range of threatening cyber exploits from possible rogue hackers, espio-

nage, or terrorists in our daily more wired world have only compounded.[22] Those who intend an attack are able to mix and match a deadly combination of system damaging "cyber exploits" resulting in interruptions, driven by: Denial-of-service, Phishing, Worm, Trojan horse, Zero-day-exploit, and Virus – only a sample of intrusion methods that are growing daily.[23]

The greatest threat to the electrical grid is the aging SCADA control systems and the lag in updating these systems to prevent a cyber-intrusion. Assessing vulnerability, determining the best risk mitigation means, and managing the resources to reduce vulnerability are largely the responsibility of the entity that owns and operates infrastructure.[24] The ability of organizations to provide strategic information and security investments may be compromised based on the strategic funding and resources available. Thus, the penny wise and pound foolish approach retards industry attempts to reduce cybersecurity vulnerabilities.

Real and present threats have seemed to elude both the industry and consumers who harken for more access, lower rates, and growth. The nature of these demands has increased the number of entry points that can be exploited and the introduction of new and yet unknown vulnerabilities as systems are either only updated or replaced. The biggest vulnerability lies with the overall "connectivity" both internally and with surrounding systems and networks of so-called shared information. This gives potential adversaries the incentive to hack – driven in the final analysis by – electricity! The sources of "cyber threats," either unintentional or intentional, vary by source, intent, and expertise: criminal groups, rogue hackers, insiders, aggressive nation-states or terrorists.[25]

Incident attacks on the power grid are only seldom reported, yet data indicated that "reported" SCADA systems attacks in the industry have increased from three in 2009 to 25 in 2011. Across federal agencies, "reported" cyber incidents have increased 680 percent over the past six years. The FBI has hundreds of energy related cases under investigation, including sophisticated hackers of large amounts of power through smart meters – largely by remotely changing the power consumption recording settings with software commonly available on the Internet – or phishing attacks collecting customer data. Moreover, the August 2003 northeast power blackout, due to an over loaded transition line making contact with trees, caused the failure of 508 generating units at 265 power plants across eight states…that cascaded from Ohio through the east coast and up to Canada. Were these cyber related? Could advanced cyber systems have prevented the incidents?[26]

Cyber-note: the privacy hurdle – there is no political consensus, at least in the United States, on how to strike the balance between preserving privacy and preventing criminal activity.[27]

FIGURE 5

Sector-Specific Agency and CIKR Sectors

Sector- Specific Agency	Critical Infrastructure and Key Resources
Department of Energy	energy, generation, refining, distribution
Department of Defense	defense industrial base and sourcing
Department of Agriculture	food and agriculture
Dept. Health and Human Services	healthcare and public health
Department of Treasury	banking, finance, currency
Environmental Protection Agency	water and wastewater systems
Department of Interior	national monuments and icons
Department of Homeland Security	
Cyber Security	IT and communication sectors
Transportation Security	postal and shipping transportation systems and infrastructure
U.S. Coast Guard	maritime security
Federal Protective Service	government facilities
Infrastructure protection	emergency services, commercial facilities, critical manufacturing, chemical sectors, dams, and nuclear reactors, materials

Source: 2009 National Infrastructure Protection Plan

THE CHALLENGE

The general public as well as local leaders have little or no concept of the dynamic and fragility of the electrical grid system across America. In August 2012, a blackout hit northern India leaving 600 million people – nearly twice the population of the United States and ten percent of the world's population – in the dark. This is the largest known blackout in history in terms of population. Delhi commuters discovered "electricity [is] the life blood of an economy."[28] What was reported as an "unprecedented grid failure as a result of negligence and incompetence," is the first of massive rolling blackouts in years to come that will likely impact the less industrialized world mired in debt and operating outdated power production facilities facing daily growing shortages of coal and natural gas. As demand for critical resources outstrips supply, it is little wonder that the Chinese, also stretched to capacity, are globally sourcing tremendous hoards of oil, coal, and natural gas.

To date, customers in America expect and have received a level of reliable service unequal in any other country. Electrical companies, which are owned by over 95 percent of private industry, work to maximize service, increase efficiency, and by so doing – enhance the revenue curve to generate profits. In so doing, the electrical industry has heavily focused investment and new technology in advanced metering infrastructure driven

RELEVANT WEBSITES

Community: http://msisac.cisecurity.org/ A review of best practices and suggestions offered by each state government.

DHS: http://www.dhs.gov/topic/cybersecurity Offers a broad overview of U.S. cyber security awareness at the national and local level including safety precautions individuals can take to protect themselves.

DOE: http://energy.gov/oe/services/cybersecurity An in-depth focus on the steps taken by the DOE to protect one of the U.S.'s most vulnerable targets: our energy grid.

NIST: http://csrc.nist.gov/nice/awareness.htm The National Initiative for Cyber Security Education (NICE) is designed to disseminate safer practices and knowledge to the general population.

U.S. Cyber Command: http://www.arcyber.army.mil/org-uscc.html The forefront of the U.S. military's defensive and offensive strategy related to cyber.

by vendors, and not focused on industry control systems (ICS). The realm of vulnerability is growing daily through the increased points of entry in the high-tech smart meter. One industry analysis concluded: "The utility cyber security market will be characterized by a frantic race to gain the upper hand against the attackers."[29]

Without extensive security, smart meter technology is only as good as the next major systems intrusion and attack. The systems today are not secure. The magnitude and stealthiness of the Stuxnet worm by highly motivated attackers on the Iranian nuclear SCADA systems is a troubling case in point. The electrical grid is only as strong as its weakest link. The Stuxnet code and others developed by hackers in the cyber domain, instinctively look for the weakest link through the "back door."[30] Most for now have evaded detection. Compounding the protection of the electric grid and smart system is the fact that there are no enforceable smart grid security measures anywhere in the world for power distribution grids. Industry invests in cyber security only when the bottom line is threatened or with financial penalty.[31]

The cooperation of private sector providers of electricity, vendors, and government agencies at all levels continues to be critical to a continued robust approach to risk. All three entities share a common concern to protect system data from unauthorized access, disruption, and modification. The keys going forward include establishing clear protocols for data security and integrity of information, while simultaneously protecting the confidentiality of private information, ensuring data availability to authorized users on a timely basis and maintaining safe and secure operations.[32]

Cyber-note: opaque transactions – technology-facilitated transactions can be designed to be invisible; alternatively, they can be designed to be visible but anonymous.[33]

Thus, leaders in the economic development community should increase their knowledge of cyber-threats and how to respond to minimize loss and restore critical systems. While Hurricane Sandy in late October 2012 was not a cyber-event, the massive storm did highlight the damage and cascading impact of over 8 million customers without electricity.[34] When the lights go out – there is a corresponding impact on fuel and water supplies, health care services, transportation systems, and communications. And a cyber-attack that cripples the electric grid could in fact have a much longer period of disruption. The future threats are real, as noted by Kenneth Van Meter, GM of Energy and Cyber Services for Lockheed Martin. "By the end of 2015 we will have 440 million new hackable points on the grid. Every smart meter is going to be a hackable point…if you can communicate with it, you can hack it."

ENDNOTES

1 Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security,"* Hoboken: John Wiley & Sons, 2006, p. 6. See also White House, Presidential Policy Directive – PPD-8: National Preparedness, Washington, D.C.: March 30, 2011 and Henry Landau, *The Enemy Within: The Inside Story of German Sabotage in America*, New York: Putnam Sons, 1937.

2 Homeland Security, National Infrastructure Protection Plan. Washington, D.C.: 2009. Note: In terms of actions dealing with infrastructure and cyber there are some 20 laws in statute, over 25 Homeland Security Presidential Directives, and a half dozen presidential executive orders. See also GAO, "Critical Infrastructure Protection," Washington, D.C, December 2011, pp. 7-8, 46-7.

3 U.S. House, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, "The Cyber Threat to Control Systems: Stronger Regulations Are Necessary to Secure the Electric Grid," 100 Cong., 1st sess., October 17, 2007. Note: SCADA encompasses several types of "control systems" that typically remotely control critical infrastructure devices and operate processes in the electricity, oil and gas, and water industries.

4 DOE, Idaho National Labs, "Vulnerability Analysis of Energy Delivery Control Systems," September 2011, p. v-vi.

5 Dan Verton, *Black Ice*, pp. 39-54; Bob Lockhart and Bob Gohn, "Utility Cyber Security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond," Pike Research, 4Q 2011. See also Le Xie, "False Data Injection Attacks in Electricity Markets," *IEEE Proceedings*, 2010, pp. 226-231.

6 Quote seen in GTCSS, "Emerging Cyber Threats: Report 2012," p. 10, www.gtisc.gatech.edu.

7 Ibid., pp. 10-12.

8 Testimony of Joseph McClelland, Director, FERC, before the U.S. House, Committee on Homeland Security, Subcommittee of Emerging Threats, Cyber Security, and Science and Technology, Washington, D.C., September 12, 2012.

9 Y. Yang et al, "Impact of Cyber-Security Issues on Smart Grid," Belfast: 2011, pp. 1-7; Rebecca Smith, "Power Shortage Vexes Texas," *Wall Street Journal*, June 5, 2012.

10 Brian Wingfield, "Power-Grid Cyber Attacks Seen Leaving Millions in Dark for Months," February 1, 2012, www.bloomberg.com; James Lewis, ed. "Cybersecurity Two Years Later," January 2012, pp. 4-7. See also House Cyber Threat Report, pp. 7-29 and Huma Khan, "Cyber Attack on U.S. Electric Grid 'Gravest Short Term Threat' to National Security, Lawmakers Say," May 31, 2011, www.abcnews.go.com.

11 Alvaro A. Cardenas, et al. "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," *ASIACCS '11 Proceedings*, March 2011, pp. 355-366; Gail Reitenbach, "Regulators Cannot Move Fast Enough to Protect Grid, FERC Warns," September 12, 2012, www.powering.com; Wingfield, Power Grid Cyber Attacks, February 1, 2012.

12 DOE, "Cybersecurity Risk Management," pp. 43, 49, 53, 61; Keith Stouffer et al, NIST "Guide to Industrial Control Systems (ICS) Security," Washington, D.C., NIST, June 2011, p.3.

13 DOE, "Electricity Subsector Cybersecurity Risk Management Process," Washington, D.C.: DOE, May 2012.

14 Martin C. Libicki, "Cyberdeterrence and Cyberwar," Rand Corporation, 2009, p. 31.

15 DOE, "Electricity Subsector Cybersecurity Risk Management Process," p. 26; Brian Wingfield, "Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months," February 1, 2012, www.bloomberg.com/news.

16 McClelland, FERC, testimony to U.S. House, September 12, 2012; Libicki, "Cyberdeterrence and Cyberwar," pp. 11-36.

17 Kevin Cornish, "Smart Grid and Intelligent Infrastructure," 2012 Strategic Directions in the U.S. Electric Utility Industry, Overland Park: Black & Veatch, 2012, p. 51.

18 DHS, *National Cyber Incident Response Plan,* Interim version, September 2010, pp. 26-9.

19 Ibid., Appendix A: B3—4, C1-2.

20 Libicki, "Cyberdeterrence and Cyberwar," pp. 91-115.

21 Oliver Kusut, et al, "Malicious Data Attacks on Smart Grid State Estimations: Attack Strategies and Countermeasures," IEE Proceedings, 2010, pp. 220-5; Stuart McClure, et al, *Hacking Exposed: Network Security Secrets and Solutions*, Osborne/McGraw-Hill, 1999, pp. 5-28.

22 "Cybersecurity: Challenges in Securing the Modernized Electricity Grid," GAO 12-507T, Washington, D.C.: February 2012.

23 Jacob Kitchel, "2011 NERC Grid Security Exercise After Action Report Review," May 27, 2012, http://blog.industrialdefender.com/?p=1271.

24 James J. Carafano, *Wiki at War*, p. 224. See also Steve Kroft and Graham Messick, "Stuxnet," *60 Minutes*, March 4, 2012 and DOE, INL, "Vulnerability Analysis of Energy Delivery Control Systems," September 2011, pp. 1-162.

25 Clay Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CSR Report, April 1, 2005, www.history.navy.mil/library.

26 "Cybersecurity: Threats Impacting the Nation," GAO 12-666T, Washington, D.C, April 2012, pp. 9-11. Note: According to US-CERT "reported" cyber incidents have increased from 5,503 in FY 2006 to 42,667 in FY 2011.

27 Christopher Bronk et al, "The Dark Side of Cyber Finance," *Survival*, April 2012, p. 139.

28 "Blackout Nation, *The Economist*, August 4, 2012, pp. 10-1, 35-6; Cassell Bryan-Law, "U.K. Blocks Extradition of Alleged Hacker," *Wall Street Journal*, October 17, 2012.

29 Lockhart and Gohm, "Utility Cyber Security," 2011,, p. 1; Amol Sharma et al, "India's Power Network Break Down," *Wall Street Journal*, August 1, 2012; Gardiner Harris, "Power Is Restored Across India After Crippling Blackout," *New York Times*, August 1, 2012: Russell A. Green, "India outage illustrates infrastructure woes," *Houston Chronicle*, August 2, 2012. Note: India in 2012 had an estimated population of 1.22 billion, of which 300 million have no access to electrical power, and at least an additional 300 million have only sporadic access.

30 NERC, "2011 NERC Grid Security Exercise: After Action Report," March 2012.

31 Ibid., pp. 1-17; Yan Sun and Haibo He, "Understanding Cascading Failures in the U.S. Power Grid," Cybersecurity Symposium, University of Rhode Island, 2011. See also James Kimmance, "Infrastructure Risk & Resilience," BCI Workshop, Bristol, 2011.

32 DOE, INL, "Vulnerability Analysis," pp. 1-150.

33 Christopher Bronk et al, "The Dark Side of Cyber Finance," *Survival*, April 2012, p. 130.

34 George Pataki, "In Sandy's Wake, Time to Upgrade the Power Grid," *Wall Street Journal*, November 26, 2012.