Cybersecurity and the Electric Utility Sector

By Nadine S. Bartholomew

On July 16, 2015, the Federal Energy Regulatory Commission (FERC) acted to improve the cybersecurity of the bulk electric system (i.e., the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kilovolts or higher) by proposing revisions to critical infrastructure protection (CIP) Reliability Standards to address risks to communication networks and related bulk electric system assets and the development of standards for supply chain management security controls to protect the bulk electric system from potential security vulnerabilities and malware threats.

MBE magazine spoke with **Chris Eisenbrey**, director of Business Continuity and Operations for the **Edison Electric Institute** (EEI) to gain new insight about what cybersecurity means for the electric utility sector and to explore how diverse business enterprises (DBEs) can play a role in helping the industry to be more resilient.

Advancements in technology have allowed businesses to become increasingly interconnected with their suppliers and customers. The number of Internet users has increased from 738 million in 2000 to 3.2 billion in 2015, according to the **International Telecommunication Union** (ITU). This represents a major transformation in the digital world that has the potential to affect every industry and every business.

Eisenbrey

As the number of mobile users, digital applications, and data networks increase, so do the opportunities for exploitation. Network outages, data compromised by hackers, computer viruses and other incidents can affect our lives in various ways. The Internet of Things (IoT) is the network of physical devices embedded with electronics, software, sensors, and connectivity to enable objects to exchange data without requiring human-to-human or human-to-computer interaction. More and more business communication is mediated and conducted via machines; as a result, there is an increased possibility of cyber attacks.

According to a recent report co-produced by the **University of Cambridge Centre For Risk Studies** and **Lloyd's**, the London-based insurance service, a major cyber attack on the U.S. electric grid could cause over $1 trillion in economic impact and roughly $71.1 billion in insurance claims. This report, entitled "Business Blackout: The insurance implications of a cyber attack on the US power grid", used some real life, publicly known cases to create these projections.

Cybersecurity is becoming increasingly important to many DBEs. Generally speaking, cybersecurity is the body of technologies, people, processes, and practices designed to protect networks, computers, programs, and data from unintended or unauthorized access, change or destruction. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. Unfortunately, there is no way to completely eliminate the risk around these threats, so for the electric utility sector, cybersecurity involves managing the risk around computer, capital networks from both the physical (e.g., people who engage with systems) and digital (e.g., computer data flow) perspectives to secure systems and assets upon which the electric utility infrastructure depends.

"Cybersecurity is a national issue," says Eisenbrey. "The electric grid's operation depends on control systems called **Supervisory Control and Data Acquisition** (SCADA) that monitor and control the physical infrastructure. As cyber threats continue to grow and become more sophisticated, the electric power industry must manage this risk. Ensuring the reliability and resiliency of the North American electric grid is one of our top priorities, and addressing cyber threats is an important part of our core reliability assurance mission. The industry has a strong record of working together and with government partners to identify, assess, protect against, and respond to cyber threats."

As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide-scale events that could cause harm or disrupt services upon which our economy and well being depend. The Aurora Generator Test conducted at the Idaho National Laboratory in 2007 demonstrated how a cyber attack could destroy physical components like a back-up diesel generator. In light of the risk and potential consequences of cyber events on both physical and digital systems, strengthening the security and resilience of the electric grid has also become important to major suppliers in the industry.

According to Eisenbrey, "the energy sector faces threats to both its business side and its operations side. On the business side, as is the case with other industries, examples of cyber threats include data theft, denial of service attacks, website defacement, and customer information disclosure or privacy breaches. On the operations side, cyber threats could target the generation and delivery of power. One security threat to electricity delivery is a sophisticated and coordinated cyber-physical attack on the operations side, aimed at causing regional power outages. It is important that diverse suppliers understand that these cyber risks are shared. In the past, it was after a component was received in-house that cybersecurity measures were initiated by the utility. Going forward, the industry will rely more heavily on the suppliers to incorporate cybersecurity measures into the manufacturing processes and specifications. If diverse suppliers can work in partnership with utilities to help them manage these risks throughout the supply chain, then they will add great value as vendors."

EEI coordinates with their members, federal agencies, and other private sector partners to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. This collaborative approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of the electric utility sector, and is consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

"As business and society becomes increasingly reliant on the power grid and the array of devices connected to the Internet, security and protection must be a high priority. Utilities are working collaboratively on the issue of cybersecurity, likewise innovative DBEs should work together to get out in front of the cybersecurity conversation. Demonstrating awareness and adaptability on this issue could be a huge point of differentiation for diverse businesses who want to offer core products and services to the electric power industry. I encourage DBEs to stay educated by following industry standards development processes, including NERC CIP and the NIST Cybersecurity Framework and to stay engaged by initiating the conversation and listening to the concerns of utilities," concludes Eisenbrey. "We must remember that we are all in this together and it is only by working together that we can ensure a secure and resilient power grid." ◆

Nadine S. Bartholomew*, principal consultant at the* ***Bartholomew Group (BG)****, has more than 15 years of experience developing and implementing communication strategies and programs to facilitate stakeholder engagement on cutting-edge issues such as corporate social responsibility (CSR) and supplier diversity. She received her MBA from Loyola University Maryland and is based in Washington, DC. Her extensive knowledge and experience of the food wholesale and retail markets affords BG the ability to challenge convention and transfer lessons learned from past successes to help clients anticipate market conditions and maximize future business opportunities.*

Reprinted with permission from the September/October 2015 issue of
Minority Business Entrepreneur
For subscription information, go to: *http://mbe.magserv.com* or call **(818) 286-3171**