TURNING THE POWER ON CYBERSECURITY

by Jenny Mangelsdorf

Increasingly sophisticated cyber attacks are putting the energy sector on the defensive. As demand climbs for electricity, even slight disruptions can cascade into major outages, causing serious consequences in our power-hungry digital world. And that's before the fleets of electric cars and oceans of smart appliances plug into our grids. To meet growing demand, the utility chain is adding links and becoming more complex; simultaneously, the bad guys are looking to create chaos.

"In the last 10 years, the threat environment has changed, even as the domain in which we use information technology has been enlarged," says Mark Rasch, director, CSC cybersecurity and privacy consulting. "What was adequate security for the threats of five years ago may not be adequate today, even if the technology had stayed the same."

Last year's Stuxnet attack was a wake-up call. To date, this malware, which targets industrial equipment, has infected 24 of Siemens' industrial customers' systems worldwide,[1] including the centrifuges used in Iran's uranium enrichment program. And while it wasn't the first cyber attack on critical infrastructure — Stuxnet was reported in mid-2010 — it stands out for the amount of resources used for its development, its sophistication and because the software apparently caused actual physical damage in the real world.

Stuxnet also succeeded at the unexpected. Since their emergence in the 1960s, most of the world's industrial control systems, which run every type of process ranging from uranium enrichment to food canning, and Supervisory Control and Data Acquisition (SCADA) systems, which coordinate infrastructures, were not linked to external systems. Instead, their key security controls were physical perimeters. Stuxnet's creators got past that by having the virus carried in through a removable device, like a CD or flashdrive.

"One limitation the energy industry faces is that they always have to segregate their industrial control and SCADA systems so drastically from the business side of their networks or related supporting systems," says CSC Technical Security Expert Hank Hensel. "If they could connect, it would save them money, time and personnel."

It's about connections

Connections — to users and their equipment, to energy suppliers and distributors, even to weather systems to help with predictive analytics — are a key part of smart technology. Utilities are searching for resources and efficiencies, and the lure of new technologies like intelligent meters and real-time usage data beckons.

"If you can add 10 to 15 percent more capacity without building anything, just by being smarter, that's a huge benefit," says Gabriel d'Eustachio, CSC security consulting lead. "It makes a huge impact on your net power usage, but to do that you need interoperability. That's a lot of connectivity."

Three years ago, CSC began helping a large electricity distributor in Australia with its program to deploy an Advanced Metering Infrastructure (AMI) solution. The work requires an overhaul of corporate systems, the deployment of systems integration technology and a wireless mesh network to more than one million customers. With the new technology, the company can collect interval metering data every 30 minutes, and consumers and distributors will be able to better manage their power consumption.

Linking to those consumers and suppliers, however, creates new security and risk issues, such as vulnerable entry points and data leakage. For the project, the CSC team is helping evaluate all aspects of an AMI infrastructure, including providing detailed smart-meter 'hacking' at our hardware security lab in Canberra, Australia.

"We divided our hardware testing into two phases: One was penetration testing, where we turned our smart guys loose to see what they could do, but 75 percent was validating the meters' controls and the effectiveness of those controls," says d'Eustachio.

"We know for a fact hackers are already acquiring meters, pulling them apart and using small probes to read metrology data and crack security keys," says Thomas Strickland, chief architect for CSC's Utilities Division. This year he attended an invitation-only, week-long advanced cybersecurity training session at the U.S. Industrial Control System (ICS) National Test Lab. Sponsored by the U.S. Department of Homeland Security's Control System Security Panel, its goal is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

"The biggest risk is not so much home owners losing their power, but attackers gaining access to the network and altering use or control data for grid switching," says Strickland. "Currently the systems are not intelligent enough to do more than say, 'I need more power,' or, 'I have too much.' This and many other risk scenarios could cause similar cascading catastrophic effects."

Smart — it's all relative

Making grids truly smart and safe challenges those working in the utility chain and public sector. Earlier this year, McAfee and the Center for Strategic and International Studies released their findings from a survey[2] of 200 IT security executives at electricity infrastructure enterprises in 14 countries. Eighty percent of respondents said they've "faced a large-scale distributed denial of service (DDoS) attack, and a quarter reported daily or weekly DDoS attacks and/or were victims of extortion through network attacks."

Countries and regions are issuing requirements and standards to help plug vulnerabilities and strengthen infrastructure. Later this year, the U.S. statutory organization, the North America Electric Reliability Corporation (NERC), will release a new version of its Critical Infrastructure Protection (CIP) standards, which is expected to have a greater focus on and address more IT security issues.

"NERC-CIP is the most mature and complete energy-related CIP framework available today," says Mario Dini, CSC key account manager, who is directing a security study for a European utility that will include an analysis of how their current International Organization for Standardization (ISO) framework stacks up against NERC-CIP's. The study will help the utility determine how beneficial it would be to adopt energy-specific standards.

Some say regulation and standards, as opposed to market drivers, will be the only way the utility industry will become safer. However, the risk of a cold shutdown to a company's industrial systems can also be persuasive. Even though standards are still evolving, the utility chain can still strengthen its links.

"This next evolution of the power industry should be more about implementing an appropriate and secure IT and communication foundation and less about inventing and quickly adopting 'new' technologies," says Strickland. "Once the foundation is secure and solid, then it can build a smart architecture." ■

[1] http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=43876783&caller=view

[2] www.mcafee.com/us/about/news/2011/q2/20110419-01.aspx

JENNY MANGELSDORF is a writer for CSC's corporate office.

SEC MOVES TO CYBER-RISK DISCLOSURE

by Mark Rasch

The U.S. Securities and Exchange Commission's new guidance to public companies on cyber-risk disclosure is likely to be the first salvo in a move to make private companies not only disclose cybersecurity risks, but mitigate them, as well.

Publicly traded entities have long been required to disclose material risks that might significantly impact their bottom lines, such as having a key manufacturing plant in an earthquake-prone zone or even an outbreak of avian flu. With the new guidance, the SEC has explicitly recognized that cyber threats, vulnerabilities and incidents pose significant risks to companies that have not adequately prepared for them, and therefore to their shareholders, too.

The commission has instructed companies to move beyond a generic "disclose risks of operations" and now expects them to fundamentally examine how they conduct cyber business in light of modern threats and vulnerabilities. It's clear that generic responses such as "we regularly conduct examinations of our cyber-risk posture" or "we comply with all laws and regulations regarding protection of data" are likely to be inadequate and that companies must conduct, and disclose to shareholders, business impact assessments that relate to cyber risks and vulnerabilities.

While a company need not disclose specifics, as by doing so could in fact make it a target, it should have a plan for both knowing and ultimately reducing its cyber risk posture. This includes knowing the nature and scope of potential threats and having the ability to appropriately respond. If companies do not heed the SEC's guidance, we can expect greater and more detailed disclosure requirements.

MARK RASCH is director, CSC cybersecurity and privacy consulting.

CSC SECURES SYSTEMS GLOBALLY

Our nearly 2,000 cyber experts serve public and private sector clients worldwide, providing a full range of cyber services — from vulnerability analysis, penetration testing and data-loss prevention to a full range of managed security services.

Learn more at **www.csc.com/cybersecurity**.