intelligentutility®

VOL 7, ISSUE 2 » SUMMER 2015

Realizing the digital utility evolution

THIS MEANS WAR

energycentral

AN ENERGY CENTRAL PUBLICATION

» WWW.INTELLIGENTUTILITY.COM

THIS WA

By Jim Hoecker and Marvin T. Griff

CYBER THIEVES TAKE PERSONAL AND financial data. Cyber pirates steal industrial and commercial intellectual property. But the cyber attacks that threaten to destroy or disarm critical infrastructure systems like the electric grid are true declarations of war. Pernicious cyber warriors seek to undermine society's sense of security and its standard of living. A survey conducted by McAfee and the Center for Strategic and International Studies reveals that 80 percent of critical infrastructure providers have faced threats ranging from denial-of-service attacks (flooding servers with hits that overwhelm servers or locking out users), to extortion and advanced persistent attacks. While physical attacks on the grid are likely to be geographically limited, the potential harm and economic dislocation from just a few cyber warriors can rapidly cascade across a broad geographic area that could be catastrophic. The nation's highly interconnected bulk power system makes it a prime target for those hoping to inflict significant physical damage and economic destruction. In 2003, when the Northeast U.S. and part of Canada was blacked-out, it cost the economies of both countries between $7 and $14 billion—despite the industry's quick action to restore power. The threat that cyber warriors pose to the nation make this a critical public policy priority.

MEANS

AR

+ But are we prepared for cyber warriors?

The grid as a potential casualty

Grid modernization generally means greater digital control and greater integration. With the advantages of improved dispatch of power over greater distances and smarter, self-healing power networks, come more sophisticated and multidimensional cyber risks.

Even before cyber attacks featured so prominently as a public policy challenge, the electric industry and federal government began addressing the security of the grid outside the legislative process. Collaboration between the White House and agencies of the executive branch first became institutionalized after 9/11 through the National Infrastructure Advisory Council. Electric utilities brought together public policy experts and private sector technical expertise to assess cyber readiness in the electric industry.

Today, only critical electric infrastructure is subject to mandatory and enforceable cybersecurity standards because Congress recognized the gravity of the threat. Following the enactment of the Energy Policy Act of 2005, the North American Electric Reliability Corporation developed Critical Infrastructure Protection, or CIP, cybersecurity reliability standards that the Federal Energy Regulatory Commission subsequently approved in 2008. The Energy Independence and Security Act of 2007 gave FERC and the

National Institute of Standards and Technology responsibilities related to coordinating the development and adoption of smart grid guidelines and standards so that this new information technology can be incorporated safely into grid operations.

Timely access to information is key to the grid's defense. Without this, defeating the cyber warriors will be impossible. Few electric industry employees presently have the national security clearances needed to access information that could strengthen grid protections. Analysts often find tips from the FBI or the Department of Homeland Security too late and vague to help counter cyber attacks. This is often attributable to the "classification" of government information. Legal roadblocks can also prevent electric utilities from sharing information with each other and with the government.

> "Timely access to information is key to the grid's defense."

Close coordination is also required to meet cyber warriors at the threshold. Utilities are not in the law enforcement or intelligence gathering business, and most government agencies (with some exceptions) cannot master grid operation. And, it can be expected that emergencies may quickly scramble all but the most hardened lines of communication.

Congress to the rescue?

With recent high profile cyber breaches at Sony and health insurer Anthem Inc., the time may be ripe for new national cyber legislation and fresh initiatives to combat cyber threats that can benefit the electric industry.

The president last month called on Congress to pass legislation promoting greater information sharing between the government and the private sector, and announced the creation of the Cyber Threat Intelligence Integration Center, or CTIIC, to coordinate real-time analyses of cyber threats between governmental agencies and the private sector. The president wants companies and industries to set up information sharing and analysis center hubs to exchange information rapidly with each other. A common set of standards is supposed to be developed, including protections for privacy and civil liberties, so that the government can share threat information. One obvious question is whether this sharing of information itself could become vulnerable.

Members of the 114th Congress, not to be outdone, introduced nine cybersecurity bills in their first six weeks in legislative session. Many focus on protecting consumer privacy, requiring data breach notifications and promoting information sharing among agencies and the private sector. Other bills have been introduced that include some cybersecurity-related language that is not the primary focus of the broader bill.

The proposed Cyber Threat Sharing Act of 2015, S. 456, is largely based on President Obama's cybersecurity information-sharing proposal and is aimed at increasing the communication and coordination of cyber threat data between private industry and the federal government. The legislation would grant liability protections to companies for sharing cyber-threat data with the Department of Homeland Security's National Cybersecurity and Communications Integration Center and with information-sharing and analysis organizations that have self-certified that they follow best practices for the operation of such organizations.

The Cybersecurity Information Sharing and Protection Act, H.R. 234, better known as CISPA, is also designed to help the public and private sectors share information following a cyber attack. But the bill is controversial and it is given little chance of passage. Critics of the bill argue that the ability of the government to gain and transfer personal user information collected from private companies is virtually unlimited. In addition, the bill grants broad liability protections to the very entities placed in a position to abuse this information collection authority. The president threatened to veto a similar bill in 2013.

Thankfully, cyber legislation is starting to move. In 2015, committees started holding hearings on cybersecurity issues in an attempt to address public concerns about protecting privacy and to take up components of measures the president put forward in January. In February, the Senate Select committee on Intelligence circulated a draft version of the Cybersecurity Information Sharing Act that it plans to introduce soon. It may garner bipartisan support because, while the committee is now led by a Republican, the previous CISA bill was introduced under Democratic leadership. It is expected that the Senate will move sometime in March to mark up the 2015 CISA bill and move it to the floor.

Cyber warriors beware.

Hoecker, a senior counsel member of Husch Blackwell's Energy & Natural Resources team, is a former chairman of the Federal Energy Regulatory Commission. Griff is an Energy & Natural Resources partner with Husch Blackwell.