



Energy companies say NERC standards inadequate

[Angela Moscaritolo](#)

August 05 2009

Meeting the cybersecurity standards required by the [North American Electric Reliability Corp. \(NERC\)](#) is not enough to safeguard the nation's electric grid, according to study released Wednesday.

A [survey](#) of 100 information security professionals at U.S. energy companies, conducted by log management firm LogLogic, found that more than half of respondents handle some 150 serious attacks each week and two-thirds respond to at least 75 attempted intrusions per week.

Energy companies are facing attacks aimed at their websites and network infrastructures, which could result in cybercriminals gaining access to employee or customer personal information, possibly causing a denial-of-service (DoS) on companies' websites or shutting down electrical systems, Tony Flick, a principal at security services firm FYRM Associates, told SCMagazineUS.com on Wednesday.

“Attacks range from foreign nation states and criminal organizations attacking our power grid to more benign phishes, worms and viruses launched by individuals,” Dominique Levin, executive vice president of marketing and strategy at LogLogic told SCMagazineUS.com in an email Wednesday.

And, when it comes to protecting themselves from the threats, respondents “unanimously” agreed that being in compliance with NERC regulations does not guarantee security.

“This points to an argument that is being discussed in the security industry as a whole,” said Flick, who last week gave a [Black Hat](#) talk on the vulnerability of [smart grid technology](#). “You can be compliant, but that doesn't mean you are actually secure.”

In January 2008, the Federal Energy Regulatory Commission (FERC) approved eight cybersecurity standards that extend to all entities connected to the power grid. NERC is tasked with enforcing them – violators can face fines up to \$1 million.

The guidance covers asset identification, management controls, personnel and training, perimeters, physical security, systems management, incident response and reporting and disaster recovery.

Respondents to the LogLogic survey, however, noted a number of issues with the standards, including ambiguity over what they require.

“While NERC provides a good starting point for the energy industry, it doesn't currently outline how to go about implementing critical infrastructure technologies or explain which individuals within a company should own and manage security initiatives,” Levin said.

According to the survey, one respondent said that meeting regulations “sometimes requires him to lower security standards in order to maintain consistency during audit reviews.” Another said: “NERC doesn't clearly outline the

definition of roles and responsibilities, nor the definition of what cybersecurity actually is. You ask 10 different people, you'll get 15 definitions.”

But respondents did admit that compliance requirements are helpful for gaining the attention of senior leadership and generating budget dollars for security.

Representatives from NERC and FERC could not be reached for comment on Wednesday.

One of the problems with NERC is that even though it is overseen by FERC, it is not itself a government entity, Flick said. NERC is a nonprofit corporation that, in essence, polices other corporations -- the utilities.

“Self-policing leads to concerns of there being not strict enough regulations that utility companies comply with,” Flick said.

He said strengthening and clarifying NERC compliance mandates is necessary to improve the overall security posture of energy companies.