Tech firms vie to secure energy sector against cyberattacks

January 22 2014

To hear cybersecurity companies tell it, the U.S. energy industry is a ticking time bomb.

Smart electric meters on the sides of houses can be entryways for cyberterrorists to shut off a city's power grid. Remote-controlled valves in oil refineries can be manipulated to cause costly spills.

As reports of hacking perpetuate around the globe, security and technology firms are rushing to introduce high-tech products and services to protect power plants, pipelines and oil companies from cyberattack.

The emerging business could soon be worth billions of dollars a year as agencies including the Federal Energy Regulatory Commission and the Nuclear Regulatory Commission order companies to better protect the infrastructure.

"It's huge," said Greg Bell, a partner with the consulting firm KPMG who works in its cybersecurity division. "Almost every device we put in a power plant or an oil refinery is computer-controlled. They all have to be secured. Cybersecurity is a growth area across all the different industries, but especially oil and gas and (power) transmission."

The U.S. Department of Homeland Security maintains a cybersecurity team that responds to hacking attacks in the country's private sector. Of the almost 200 cases it handled last year, more than 40 percent were in

the energy sector, according to an agency report.

Would-be attackers include anti-capitalist groups, criminal organizations, rival companies and those employed by foreign nations, Bell said.

So far, as a homeland security official acknowledged in a recent conversation, there has not been a successful large-scale cyberattack on the U.S. energy industry. No grids have lost power; no pipelines have been tricked into shutting down.

The most publicized incident came three years ago, when the FBI put out an alert that a criminal group in Puerto Rico had compromised a local utility's smart meters. The meters were rigged to underreport customers' electricity use, resulting in losses of up to $400 million, the agency said.

Now, companies such as Maxim Integrated, a semiconductor company with a large operation in North Dallas, are offering chips designed to protect against hacking and alert utilities when a smart meter is tampered with.

"It used to be if you wanted to take down the grid, you had to break into a control room or blow up a substation," said Kristopher Ardis, executive director of Maxim's energy solutions division. "Now all it takes is someone in the supply chain to load in some rogue code."

Verizon is also getting into the smart meter business. Last month, the wireless communications company released a cloud-based platform to protect smart meters, among other wireless devices, against hacking.

Asked about the suite of new products hitting the market, Chris Schein, a spokesman for the transmission company Oncor, said the company has long taken steps to protect smart meters and is confident in its security.

"We've been dealing with meter fraud for years," he said.

The degree of vulnerability within the electrical sector is up for debate.

The industry is one of the most proactive when it comes to cybersecurity, said Jonathan Shapiro, a former telecommunications entrepreneur who works for the University of Texas-Dallas on cybersecurity projects. Tampering with a grid might sound dramatic. But the financial incentive for criminals is modest when compared with what they can make stealing credit card numbers from banks.

"Here in Texas, everyone communicates and does scenarios. The Texas electric industry is ahead of other parts of the United States," he said. "With utilities, you don't attack to get rich. You need another reason. And in that case you're really talking about nation states."

Power companies generally keep the networks that control the grid disconnected from the Internet to deter hackers. But that policy is not always followed to the letter, and there has been evidence of hackers probing networks looking for an entryway, Shapiro said.

For the oil and gas industry, cybersecurity is an increasing concern. For the past eight years, the American Petroleum Institute has hosted a cybersecurity expo in Houston for industry consultants and executives.

Still fresh on the industry's mind is a series of attacks beginning in 2009 in which hackers believed to be working in China infiltrated the computers of executives at oil and petrochemical companies around the globe.

According to a report by the California computer security firm McAfee, the attack was nicknamed "night dragon." Using tools widely available on underground Chinese websites, the hackers were able to walk away

with emails and other documents.

Ed Goings, who leads investigations of cyberattacks for KPMG, said no security system is foolproof. All companies can do is make sure their systems are more secure than their competitors'.

"My father always used to say locks are for honest people," he said. "If a criminal wants in, they will find another way in. I can put enough locks on to make myself feel comfortable and safe. But always be aware there still may be a break-in. And (learn) how to minimize the damage if and when it does occur."