Van H. Wanggaard
Wisconsin State Senator

Testimony on Senate Bill 457

Thank you for listening to my testimony on Senate Bill 457, relating to trespass and damage to property owned or used by an energy provider, and providing a penalty.

Due to a rash of copper thefts, damage to utility property has been large issue for many years. For that reason, several years ago, the Legislature enacted a Class A misdemeanor for damage to utility property. Unfortunately, since that time, the threat of damage of utility property and the knowledge of the damage that can occur has grown.

The damage now goes beyond just stealing copper wire for scrap metal. Most of us expect and rely on a consistent and reliable power supply without thinking about how we receive it. A single trespasser or bad actor can cause a problem in a utility property that could disrupt services for hundreds or thousands of people. In addition, a single person may trespass on utility property and install a virus or malware. This may cause a disruption of services not to hundreds or thousands, but to hundreds of thousands. It could also create a breach of computer and billing systems, stealing passwords, billing, and banking information from customers. The disruption of service and related damage to our economy and public safety can be devastating.

This increased threat requires update our utility damage and trespassing laws. This bill increases penalties for intentional damage to property owned by an energy provider if the actor causes a substantial interruption of the energy provider's services. The bill also specifies that trespassing on an energy plant or generation, distribution or transmission system is also a Class H Felony.

There will be additional speakers who will speak to specific threats and cases they have seen. I have also circulated an article from the Milwaukee Journal Sentinel outlining the cyber threat that exists within our utility infrastructure. I urge your support for SB 457, and would take any questions.

Serving Racine and Kenosha Counties - Senate District 21
State Capitol, P.O. Box 7882, Madison, WI 53707-7882 • (608) 266-1832 • Toll-free (866) 615-7510
E-Mail: Sen.Wanggaard@legis.wi.gov • SenatorWanggaard.com

JOURNAL INTERACTIVE PRINTTHIS

Foreign hackers sneaking into vulnerable U.S. power grid

By Garance Burke and Jonathan Fahey, Associated Press
Dec. 20, 2015

San Jose, Calif. — Security researcher Brian Wallace was on the trail of hackers who had snatched a California university's housing files when he stumbled into a larger nightmare: Cyberattackers had opened a pathway into the networks running the U.S. power grid.

Digital clues pointed to Iranian hackers. And Wallace found that they had already taken passwords, as well as engineering drawings of dozens of power plants, at least one with the title "Mission Critical." The drawings were so detailed that experts say skilled attackers could have used them, along with other tools and malicious code, to knock out electricity flowing to millions of homes.

Wallace was astonished. But this breach, The Associated Press has found, was not unique.

About a dozen times in the last decade, sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on, according to top experts who spoke only on condition of anonymity due to the sensitive nature of the subject matter.

The public almost never learns the details about these types of attacks — they're rarer but also more intricate and potentially dangerous than data theft. Information about the government's response to these hacks is often protected and sometimes classified; many are never even reported to the government.

These intrusions have not caused the kind of cascading blackouts that are feared by the intelligence community. But so many attackers have stowed away in the systems that run the U.S. electric grid that experts say they likely have the capability to strike at will.

And that's what worries Wallace and other cybersecurity experts most.

"If the geopolitical situation changes and Iran wants to target these facilities, if they have this kind of information it will make it a lot easier," said Robert M. Lee, a former U.S. Air Force cyberwarfare operations officer.

In 2012 and 2013, in well-publicized attacks, Russian hackers successfully sent and received encrypted commands to U.S. public utilities and power generators; some private firms concluded this was an effort to position interlopers to act in the event of a political crisis. And the Department of Homeland Security announced about a year ago that a separate hacking campaign, believed by some private firms to have Russian origins, had injected software with malware that allowed the attackers to spy on U.S. energy companies.

"You want to be stealth," said Lillian Ablon, a cybersecurity expert at the RAND Corporation. "That's the ultimate power, because when you need to do something you are already in place."

The hackers have gained access to an aging, outdated power system. Many of the substations and equipment that move power across the United States are decrepit and were never built with network security in mind; hooking the plants up to the Internet over the last decade has given hackers new backdoors to come in. Distant wind farms, home solar panels, smart meters and other networked devices must be remotely monitored and controlled, which opens up the broader system to fresh points of attack.

Hundreds of contractors sell software and equipment to energy companies, and attackers have successfully used those outside companies as a way to get inside networks tied to the grid.

Attributing attacks is notoriously tricky. Neither U.S. officials nor cybersecurity experts would or could say if the Islamic Republic of Iran was involved in the attack Wallace discovered involving Calpine Corp., a power producer with 82 plants operating in 18 states and Canada.

Private firms have alleged other recent hacks of networks and machinery tied to the U.S. power grid were carried out by teams from within Russia and China, some with governmental support. Even the Islamic State group is trying to hack American power companies, a top Homeland Security official told industry executives in October.

Homeland Security spokesman SY Lee said that his agency is coordinating efforts to strengthen grid cybersecurity nationwide and to raise awareness about evolving threats to the electric sector through industry trainings and risk assessments.

As Deputy Energy Secretary Elizabeth Sherwood Randall said in a speech earlier this year, "If we don't protect the energy sector, we are putting every other sector of the economy in peril."

The Department of Homeland Security said it had helped more than 100 energy and chemical companies improve their cyber defenses, and the North American Electric Reliability Corp. — which oversees reliability of the grid — is tracking threats and issuing new standards for utilities to follow.

"As NERC appropriately adds more of those and places a greater emphasis on this, we have staffed up and do spend more time on cybersecurity," said Anne Spaltholz, spokeswoman for American Transmission Co., a utility that manages the eastern Wisconsin power grid.

In Madison, Alliant Energy moved two years ago to create one team responsible for physical, information technology and infrastructure security. In Milwaukee, We Energies says it's spending millions of dollars a year on cyber security.

The Calpine breach

The AP looked at the vulnerability of the energy grid as part of a yearlong examination of the state of the nation's infrastructure coordinated with the Associate Press Media Editors.

The attack involving Calpine is particularly disturbing because the cyberspies grabbed so much, according to interviews and previously unreported documents.

Cybersecurity experts say the breach began at least as far back as August 2013, and could still be going on today.

According to the AP investigation, the hackers got:

■User names and passwords that could be used to connect remotely to Calpine's networks, which were being maintained by a data security company. Even if some of the information was outdated, experts say skilled hackers could have found a way to update the passwords and slip past firewalls to get into the operations network. Eventually, they say, the intruders could shut down generating stations, foul communications networks and possibly cause a blackout near the plants.

■Detailed engineering drawings of networks and power stations from New York to California — 71 in all — showing the precise location of devices that communicate with gas turbines, boilers and other crucial equipment attackers would need to hack specific plants.

■Additional diagrams showing how those local plants transmit information back to the company's virtual cloud, knowledge that attackers could use to mask their activity. For example, one map shows how information flows from the Agnews power plant, near the San Francisco 49ers football stadium in San Jose, Calif., to the company headquarters in Houston.

Wallace first came across the breach while tracking a new strain of noxious software that had been used to steal student housing files at the University of California, Santa Barbara.

He had recently joined the Irvine, Calif.-based cybersecurity firm Cylance Inc., fresh out of college.

Wallace started digging. Soon, he found the FTP (file transfer protocol) servers, typically used to transfer large numbers of files back and forth across the Internet, and the hackers' ill-gotten data — a cache of more than 19,000 stolen files from thousands of computers across the world, including key documents from Calpine.

Before Wallace could dive into the files, his first priority was to track where the hackers would strike next — and try to stop them.

He started staying up nights, often jittery on Red Bull, to reverse-engineer malware. He waited to get pinged that the intruders were at it again.

Months later, Wallace got the alert: From Internet Protocol addresses in Tehran, the hackers had deployed TinyZbot, a Trojan horse-style of software that the attackers used to gain backdoor access to their targets, log their keystrokes and take screen shots of their information. The hacking group, he would find, included members in the Netherlands, Canada, and the United Kingdom.

Circumstantial evidence such as snippets of Persian comments in the code helped investigators conclude that Iran was the source of the attacks.

Calpine didn't know its information had been compromised until it was informed by Cylance, company spokesman Brett Kerr said.

Iranian U.N. Mission spokesman Hamid Babaei did not return calls or address questions emailed by AP.

Cylance notified the FBI, which warned the U.S. energy sector in an unclassified bulletin last December that a group using Iran-based IP addresses had targeted the industry.

Whether there was any connection between the Iranian government and the individual hackers who Wallace traced is unclear.

The Associated Press, in partnership with the Associated Press Media Editors association, has undertaken a yearlong collaborative project examining the nation's infrastructure needs. This is the fourth and final installment. Thomas Content of the Journal Sentinel staff contributed to this report.

Find this article at:
http://www.jsonline.com/news/usandworld/foreign-hackers-sneaking-into-vulnerable-us-power-grid-b99636639z1-363075701.html

☐ Check the box to include the list of links referenced in the article.

From: Ramirez, Zach
Sent: Thursday, December 10, 2015 7:11 PM
To: Walentowski, Nicole <Nicole.Walentowski@legis.wisconsin.gov>; Steffen, David <David.Steffen@legis.wisconsin.gov>
Subject: AB 547

Representative Steffen,

You asked for a description of the property that is covered under 2015 Assembly Bill 547 ("the bill"), as well as a description of the extent to which the bill changes current law with regard to cybercrime.

The bill relates to two types of activities: (1) intentionally damaging property; and (2) unlawfully entering property. For each activity, the bill separately addresses the property that is covered by the bill.

Property that is Covered by the Bill

Intentionally Damaging Property

The bill provides that whoever intentionally causes damage to any physical property of another without the person's consent is guilty of a Class H felony, if:

1) the property damaged is owned, leased, or operated by an energy provider; **and**
2) the actor intended to or did cause substantial interruption or impairment of any service or good provided by the energy provider.

Whether a specific piece of property is covered by this provision depends largely on the extent to which damage to the property actually causes or demonstrates an intent to cause impairment or interruption of a service or good. Damage to certain types of property, such as a transmission line, is more likely to cause or demonstrate an intent to cause interruption or impairment of service than is damage to other types of property, such as land beneath a transmission line. Therefore, the types of property that are covered by the bill are determined more by this criterion than by the criterion that the property be owned, leased, or operated by an energy provider. Property that is owned, leased, or operated by an energy provider encompasses a broad range of property.

Unlawfully Entering Property

The bill provides that whoever intentionally enters an ***energy provider property*** without lawful authority and without the consent of the energy provider is guilty of a Class H felony. The bill specifies that ***energy provider property*** means property that is part of an electric generation, distribution, or transmission system or part of a natural gas distribution system and that is owned, leased, or operated by an energy provider.

Whether a specific piece of property is covered by this provision depends on the extent to which it is considered to be part of one of the systems listed in the bill. Although neither the bill nor statutes provide a definition for each of the systems, the Public Service Commission's (PSC) administrative rules help provide an understanding of the types of property that are generally considered to be part of a system. Specifically, PSC's rules state that "Distribution system" means electric lines and associated facilities, designed and operated at less than 40 kV, that deliver power to customers. [s. PSC 112.02 (3), Wis. Adm. Code.] PSC's rules also state that "Transmission system" means electric lines and associated facilities, designed and operated at 40 kV or higher voltage, that transmit power from generating plants to and between distribution systems. [s. PSC 112.02 (9), Wis. Adm. Code.] Therefore, property that actually performs the function of generation, distribution, or transmission is considered to be part of a

system and is covered by the bill. Property that is too indirectly connected with these functions to be considered part of a system would not be covered under the bill.

Application to Cybercrime

Current law provides that a person is guilty of a Class F felony if the person causes an interruption or impairment of a supply of water, gas, or other public service by:

1) willfully, knowingly and without authorization:
   - Modifying data, computer programs or supporting documentation.
   - Destroying data, computer programs or supporting documentation.
   - Accessing computer programs or supporting documentation.
   - Taking possession of data, computer programs or supporting documentation.
   - Copying data, computer programs or supporting documentation.
   - Disclosing restricted access codes or other restricted access information to unauthorized persons.
2) Intentionally causing an interruption in service by submitting a message, or multiple messages, to a computer, computer program, computer system, or computer network that exceeds the processing capacity of the computer, computer program, computer system, or computer network. [s. 943.70 (2) (b) 3r., Stats.]

The bill does not make changes to these provisions of current law.

Please let me know if you have any follow-up questions that you would like to discuss.

Thanks,
Zach

Zach Ramirez
Staff Attorney
Wisconsin Legislative Council
(608) 267-9485
zach.ramirez@legis.wi.gov