THE WALL STREET JOURNAL.
U.S. Edition ▾ | August 24, 2018 | Today's Paper | Video


U.S. NEWS
Michael Cohen Guilty Plea Reveals Link to Qatari Royal Family


POLITICS
Allen Weisselberg, Longtime Trump Organization CFO, Is ...


REAL ESTATE
Warren Buffett Slashes Price on Longtime Beach House

BUSINESS

PG&E Identified as Utility That Lost Control of Confidential Information

As a result of 2016 failure, 30,000 records about PG&E's cyber assets were exposed on the internet

By Rebecca Smith
Updated Aug. 24, 2018 5:35 p.m. ET

San Francisco-based PG&E Corp. was identified Friday as the large utility that authorities had fined in May for losing control of a database with confidential information about its systems and leaving it exposed on the internet for 70 days.

The breach happened in 2016 and, until this week, the Federal Energy Regulatory Commission had declined to identify the utility that it fined $2.7 million earlier this year, a small amount compared with a potential fine of as much as $140 million.

PG&E Identified as Utility That Lost Control of Confidential Information

As a result of 2016 failure, 30,000 records about PG&E's cyber assets were exposed on the internet

0 COMMENTS

By
Rebecca Smith
Updated Aug. 24, 2018 5:35 p.m. ET

San Francisco-based PG&E Corp. PCG -2.62% was identified Friday as the large utility that authorities had fined in May for losing control of a database with confidential information about its systems and leaving it exposed on the internet for 70 days. The breach happened in 2016 and, until this week, the Federal Energy Regulatory Commission had declined to identify the utility that it fined $2.7 million earlier this year, a small amount compared with a potential fine of as much as $140 million.

Heavily redacted documents released Friday showed correspondence among regulators related to the incident, which referenced PG&E, but they provided no additional details. However, other previously available documents provided information about the incident, so together they show how PG&E's systems were exposed.

In a written statement, PG&E said that "once we learned of the exposure, we communicated proactively with the appropriate government agencies and regulators and have since worked with them on corrective actions."

It added that its cybersecurity measures are "robust and consistent with the best practices being employed in the industry."

PG&E's identity was revealed because of a Freedom of Information Act request filed to FERC by Secure the Grid Coalition, a nonprofit group focused on critical infrastructure protection. Michael Mabee, a New Hampshire representative of the group, said he petitioned for the information, because he thought it was "disturbing and wrong" for federal officials to protect a utility whose actions endangered the public.

As a result of the failure, 30,000 records about PG&E's cyber assets were exposed to the internet—without password protection—at a time when authorities have said Russian agents were trying to gain access to U.S. energy companies.

An investigation into the data breach by the North American Electric Reliability Corp. and a related organization found that an unnamed vendor hired by PG&E to assist with an asset-management program downloaded records from a cyber-asset database to his own computer—without the utility's permission and in violation of company policy—then left it exposed to the internet until it was brought to PG&E's attention by an internet-security researcher.

The records included information on systems that control physical as well as remote access to the utility's control centers and electrical substations as well as the utility's system that regulates electricity flows.

It also included usernames for more than 100 people with network access and "hashed" passwords that could have been cracked by a skilled adversary to garner actual log-in credentials, according to an investigation by federal authorities.

Federal investigators said they don't know who may have accessed the data but said there was evidence others had found it. An investigative report said there was "residual risk" that malicious actors established a foothold in PG&E's networks and could be positioned to cause harm in the future.

PG&E owns power plants, natural gas pipelines, a nuclear generating station and electric power lines that are vital to California and the western power grid. It furnishes electricity to nearly one in 20 Americans.

Utilities have been subject to cybersecurity rules for a decade. They require utilities to secure sensitive information to prevent unauthorized access.

California's chief utility regulator attempted to confirm that PG&E was the unidentified utility fined by FERC in May but was rebuffed. Recent laws have given federal authorities more ability to keep information from state officials. "We're all wrestling with it," said Michael Picker, president of the California Public Utilities Commission.

The Securities and Exchange Commission recently warned public companies that they must improve their cyber disclosures, noting that cyber breaches "pose grave threats to investors, our capital markets and our country."

It doesn't appear that PG&E disclosed the event in its SEC filings.

Write to Rebecca Smith at rebecca.smith@wsj.com

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FERC Pressured To Disclose Cybersecurity Violators

By **Alison Noon**

Law360 (February 19, 2019, 9:31 PM EST) -- The Federal Energy Regulatory Commission was hit with renewed criticism on Tuesday for shielding the names of power companies whose cybersecurity deficiencies pose a threat to the U.S. electric grid.

Motions asking FERC to compel information from the North American Electric Reliability Corp. argued that public interest, local law enforcement and a need for deterrence should outweigh the industry's concerns that disclosure will make utilities more vulnerable to cyber attacks.

Public Citizen, a liberal think tank that focuses on consumer advocacy, pressed regulators to unmask the company that agreed last month to pay a **record $10 million fine** for violating federal cybersecurity standards for over five years.

Michael Mabee of Secure the Grid Coalition filed a separate motion asking FERC to disclose the subjects of nearly 200 cases resolved between five years and nine years ago, and is also in the process of penning a request for the identity of the record-setting settlement.

Public Citizen's motion claimed disclosure would benefit state regulators and other local watchdogs, the public and even the industry. Mabee's filing echoed concerns about public awareness and added that the secrecy appears legally unjustified.

"FERC needs to shine a light on utility violations that place the public at risk of long-term and widespread electric grid outage from cyberattack and other deliberate actions of foreign adversaries," Mabee's motion said.

Tuesday's motions came as regulators make incremental steps on **cybersecurity standards** and lawmakers consider the implications of a 2017 Russian hacking spree. Sen. Angus King, I-Maine, suggested at a hearing last week that "Russians are already in the grid."

Mabee said potentially successful attacks like Russia's undermine NERC's primary reason for shielding companies where regulators find bad security practices — to protect that entity from further attack.

"If keeping the names of violators private was going to help, one would think it would have helped by now," Mabee told Law360. "The public should be able to take a look at who the violators are and who the repeat violators are to evaluate the issue."

Mabee compiled FERC data that shows out of 243 cases between 2010 and 2018, 1,465 energy entities violated the government's critical infrastructure standards. The agency did not identify any of them.

He asked FERC to force NERC to name the companies involved in dockets that are five years or older — the regulatory limit, he said, for their confidential designation. In his request, Mabee claimed regulators have been abusing the rule that allows them to shield specific engineering, vulnerability or detailed design information that, if disclosed, could help someone attack the grid.

"NERC has been basically twisting the language and the definitions to have an excuse to not release these things," Mabee said.

A FERC representative declined to comment on the pending motions. Representatives for NERC did not return a message seeking comment Tuesday.

Public Citizen, Mabee and other advocates filed inquiries last year asking FERC and NERC to unveil the subject of a $2.7 million fine. The requests were denied, but records Mabee secured from FERC through a Freedom of Information Act request later identified the organization as Pacific Gas & Electric Co. PG&E has since told Law360 that it was the subject of the fine.

"Concealing the name of the recipient of the largest fine in history sends a confusing message to the public that large penalties do not come with full accountability, as future violators may be able to similarly hide behind the veil of anonymity," Public Citizen's motion said. "In fact, that is exactly what another utility, PG&E, has been able to do."

Several media reports have identified Duke Energy Corp. as the subject of the $10 million settlement announced last month. A representative for Duke Energy, David Scanzoni, declined to comment on the charges Tuesday, citing a company policy prohibiting speaking on any industry enforcement actions.

--Editing by Amy Rowe.

THE WALL STREET JOURNAL.

https://www.wsj.com/articles/pg-e-among-utilities-cited-for-failing-to-protect-against-cyber-and-physical-attacks-11554821337

BUSINESS

PG&E Among Utilities Cited for Failing to Protect Against Cyber and Physical Attacks

Cases, newly revealed but years old, raise questions about system aimed at encouraging self-disclosure by keeping names of violators quiet

By Rebecca Smith
April 9, 2019 10:48 a.m. ET

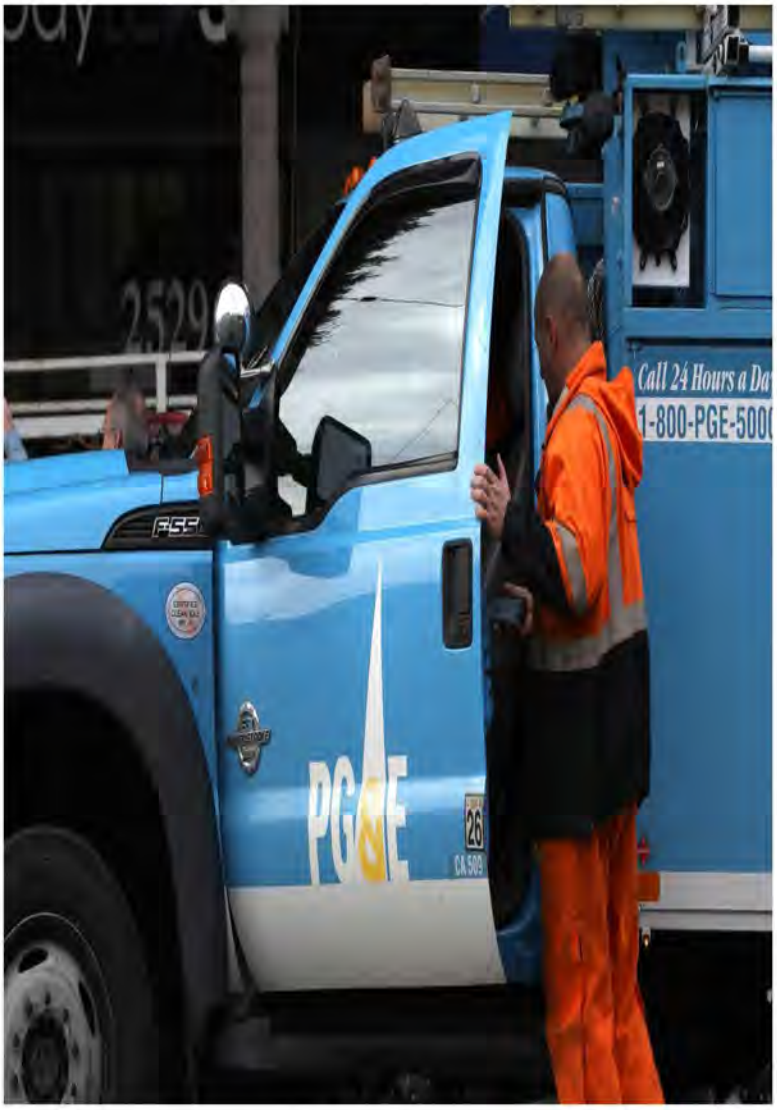
PG&E Corp. PCG **-3.35%** ▼ and a municipal utility in Missouri broke rules designed to protect the nation's electric system from cyber and physical attacks and were sanctioned by federal regulators, according to newly released documents that provided the identities of the violators.

In addition, PG&E was the utility sanctioned in a separate case for violations of these critical infrastructure protection rules, along with Detroit-based utility DTE Energy Co. DTE **+0.18%** ▲ , according to people familiar with the cases and redacted documents reviewed by The Wall Street Journal.

The identification of the violators follows the recent revelation that Duke Energy Corp. DUK **-0.09%** ▼ broke the same set of rules.

The cases against DTE, PG&E and City Utilities of Springfield, Mo., were lodged from 2014 to 2016—a time when Russia was in the midst of a major campaign to penetrate utility defenses, according to federal officials.

What is unusual isn't that companies were penalized, but that the public now knows some of the identities. Most violators are kept confidential in a system designed to



PG&E, California's biggest utility, says its cyber-security measures are 'robust and consistent with the best practices being employed in the industry.' **PHOTO:** JUSTIN SULLIVAN/GETTY IMAGES

encourage self-disclosure by the utilities but some critics say is too protective of the industry.

Although about 250 penalty cases have been lodged against U.S. utilities in the past decade for violating rules designed to protect essential infrastructure, few identities have been divulged by the Federal Energy Regulatory Commission, the agency that oversees the interstate electric system.

When the identities do come out, the reason is usually because regulators released them in response to public-records requests after they believe vulnerabilities have been remedied. That was the case in FERC releasing documents disclosing City Utilities in its case and PG&E in one of its cases.

MORE ON CYBERSECURITY

- Channeling China, Russia Eyes Its Own Great Firewall (April 2)
- FBI, Retooling Once Again, Sets Sights on Expanding Cyber Threats (March 29)
- U.S. Trade Negotiators Take Aim at China's Cybersecurity Law (March 29)
- EU Election Poses 'Tempting Target' for Hackers Intent on Interfering (March 29)

The other way that identities are revealed is when they are disclosed by people with knowledge of the matter. Such was the case for DTE and another PG&E case, though redacted information about their violations was already public.

Charlotte, N.C.-based Duke was outed in February as the company that committed 127 violations of safety rules in recent years. Among other things, Duke failed to protect sensitive information on its most critical cyber assets, officials said. FERC is reviewing the case and a $10 million settlement agreement.

Public officials are becoming more vocal about threats to critical infrastructure. In late January, U.S. intelligence agencies said Russian and Chinese agents possess the ability to knock out power temporarily and disrupt gas pipelines "for days to weeks" through cyber means.

A Journal investigation, published in January, showed how Russian hackers targeted the unprotected computer systems of small vendors in an attempt to move up the supply chain and compromise defenses of electric companies.

Increased public attention on grid vulnerabilities has sent a shudder through the electric industry.

Last week, three trade groups asked FERC to look at its rules on disclosure practices and, in the meantime, to halt processing records requests, including those by the Journal.

David Ortiz, deputy director of FERC's Office of Electric Reliability, said cyberattacks are happening in large numbers, but utilities report almost no successful attacks even

when assured of confidentiality. Recently, FERC has started requiring utilities report attempts, not just successful hacks.

There is debate on how much of that information should be public.

Regulators rely on utilities to self-report their violations and accept audit findings. They fear that system will break down if companies are exposed to public scrutiny.

Security researcher and blogger Michael Mabee, who has asked FERC to identify utilities associated with more than 200 penalty cases, said the regulatory system needs fixing, and "the only way for that to happen is by shining the light of day on it."

Mr. Mabee also said penalties negotiated through settlement agreements are too low. So far, they have not been made public.

FERC's Mr. Ortiz said identities are protected to honor confidentiality requests from the North American Electric Reliability Corp., called NERC, the federally appointed organization that crafts utility standards and audits compliance. It refers penalty cases to FERC for enforcement.

The cases involving DTE, City Utilities and PG&E demonstrate why officials are worried about security.

DTE agreed to pay $1.7 million in 2016 to settle 36 infractions of rules in prior years, according to people with knowledge of the case. The utility said it takes a duty "to protect the bulk power system very seriously," but declined additional comment.

NERC said auditors found "serious, systemic security and compliance issues" that persisted from one examination to the next, according to public case documents.

The utility failed to apply 75 security patches to its Energy Management System, a set of computer-aided tools that guides engineers and helps control power flows. Auditors found the utility stopped making updates as soon as a prior audit ended.

The utility also failed to keep backup software that it would need to recover from a catastrophic cyber event.

City Utilities of Springfield, Mo., violated security rules by failing to identify its primary and backup control centers as critical facilities requiring special protections. Its identity was disclosed in the 2014 case in response to a FOIA request by the Journal and Mr. Mabee.

The utility didn't respond to requests for comment.

PG&E, California's biggest utility, now is known as the company behind three penalty cases.

FERC said PG&E was fined $98,500 in 2014 for failing to keep proper logs for 30 critical workstations. Without logs, auditors said, the utility couldn't have identified hackers' "attacks, multiple bad password attempts or irregular logons to these workstations." PG&E later found similar issues with 150 other workstations and servers.

Separately, PG&E was fined $1.125 million in 2016 for failing to adequately protect new electrical substations against potential attacks, according to one person familiar with the case.

PG&E said its cybersecurity measures are "robust and consistent with the best practices being employed in the industry." It added that confidentiality "promotes self-reporting" and disclosure "may jeopardize national security by exposing potential grid vulnerabilities."

Last year, PG&E was identified by the Journal as the company that lost control of a confidential database of its cyber assets in 2016 resulting in their internet exposure.

Write to Rebecca Smith at rebecca.smith@wsj.com