SIEMENS

Press

Washington, D.C., October 4, 2019

Siemens and Ponemon Institute study finds utility industry vulnerable to cyberattacks

- **Assesses the utility industry's risk, readiness, and solutions to secure operational technology on the grid and recommends action to help utilities combat cyber threats**
- **Results show risk is worsening, with potential for severe financial, environmental and infrastructure damage**
- **54 percent of those surveyed in the utilities industry expect an attack on critical infrastructure in the next 12 months**

Siemens and the Ponemon Institute today released a new report that assesses the global energy industry's ability to meet the growing threat of cyber attacks to utilities and critical infrastructure connected to the electrical grid. The report – *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* – details the utility industry's vulnerability to cyber risk, readiness to address future attacks, and provides solutions to help industry executives and managers better secure critical infrastructure. The results of the report were released at a forum hosted by the Atlantic Council in Washington, D.C. focused on the growing national, economic, and energy security threat that cyber attacks pose to the utility industry.

"The utility industry has woken up to the industrial cyber threat and is taking important steps to shore up defenses," said Leo Simonovich, Siemens VP & Global Head, Industrial Cyber & Digital Security. "We hope this report help utilities benchmark their readiness and leverage best practices to stay ahead of attackers."

The study surveyed 1,726 utility professionals responsible for securing or overseeing cyber risk in Operational Technology (OT) environments at electric utilities with gas, solar, wind assets, and water utilities throughout North America, Europe, Middle East, the Asia-Pacific region, and Latin America. It identified key

Siemens AG
Communications
Head: Clarissa Haller

Werner-von-Siemens-Straße 1
80333 Munich
Germany

Reference number: PR201910045399

vulnerabilities in energy infrastructure that malicious actors seek to exploit, including common security gaps that are created as utilities rely on digitalization to leverage data analytics, artificial intelligence, and balance the grid with intermittent renewable energy and distributed power generation.

As utilities increasingly adopt business models that connect OT power generation, transmission, and distribution assets to Information Technology (IT) systems, critical infrastructure is more vulnerable to cyber attacks according to the study. The survey results show the risk of cyber attacks on the utility industry may be worsening with 56 percent of respondents reporting at least one shutdown or operational data loss per year, and 25 percent impacted by mega attacks, which are frequently aided with expertise developed by nation-state actors. The vulnerability of critical infrastructure to cyber attacks has potential to cause severe financial, environmental and infrastructure damage, and according to all respondents, 64 percent say sophisticated attacks are a top challenge and 54 percent expect an attack on critical infrastructure in the next 12 months.

“Increasing electrification across a range of sectors is a crucial piece in the decarbonization puzzle, but, as the Siemens and Ponemon Institute report documents, an increase in grid-connected infrastructure creates additional vulnerabilities to cyber attacks. A devastating attack would not only harm the economy, but it could also slow down the rate of electrification. This report provides recommendations to help utilities better address these risks. Getting this right is not only important for the security of our electricity system, but also for achieving our climate goals,” said Randy Bell, Director of the Atlantic Council Global Energy Center.

Most surveyed global utilities say that cyber threats present a greater risk to critical infrastructure - compared to IT systems – and are concerned with unique industry challenges, including ensuring availability, reliability and safety of electricity delivery. Industry-wide, readiness to address cyber attacks is uneven and has common blind spots, especially with regards to the unique cybersecurity requirements for OT, and the importance of distinguishing between security for OT and security for IT. This remains a major challenge for many organizations across the industry. Only 42 percent rated their cyber readiness as high, and only 31 percent rated readiness to respond to or contain a breach as high.

Caught in the Crosshairs: Are Utilities keeping up with the Industrial Cyber Threat? follows two previous collaboration between Siemens and the Ponemon Institute, including *Assessing the Cyber Readiness of the Middle East's Oil and Gas Sector* and *The State of Cybersecurity in the Oil &Gas Industry: United States*.

A copy of the full report can be found here:
https://sie.ag/2lAWy3k

This press release and a press picture are available at https://sie.ag/2IjgYq4

For further information on Siemens Gas & Power please see
www.siemens.com/energy

For further information on Siemens cybersecurity for energy, please see
www.siemens.com/cybersecurity-energy

Contact for journalists
Amy Pempel
Phone: +1 407-408-1932; E-mail: amy.pempel@siemens.com

Follow us on Twitter at: www.twitter.com/siemens_energy

Siemens Gas and Power (GP) is a global pacesetter in energy, helping customers to meet the evolving demands of today's industries and societies. GP comprises broad competencies across the entire energy value chain and offers a uniquely comprehensive portfolio for utilities, independent power producers, transmission system operators, the oil and gas industry and other energy intensive industries. Products, solutions, systems and services address the extraction, processing and the transport of oil and gas as well as power and heat generation in central and distributed thermal power plants, power transmission and grid stability, as well as energy transition technologies including storage. With global headquarters in Houston in the U.S. and more than 64,000 employees in over 80 countries, Siemens Gas and Power has a presence across the globe and is a leading innovator for the energy systems of today and tomorrow, as it has been for more than 150 years.

Siemens AG (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability and internationality for more than 170 years. The company is active around the globe, focusing on the areas of power generation and distribution, intelligent infrastructure for buildings and distributed energy systems, and automation and digitalization in the process and manufacturing industries. Through the separately managed company Siemens Mobility, a leading supplier of smart mobility solutions for rail and road transport, Siemens is shaping the world market for passenger and freight services. Due to its majority stakes in the

publicly listed companies Siemens Healthineers AG and Siemens Gamesa Renewable Energy, Siemens is also a world-leading supplier of medical technology and digital healthcare services as well as environmentally friendly solutions for onshore and offshore wind power generation. In fiscal 2018, which ended on September 30, 2018, Siemens generated revenue of €83.0 billion and net income of €6.1 billion. At the end of September 2018, the company had around 379,000 employees worldwide. Further information is available on the Internet at www.siemens.com.