



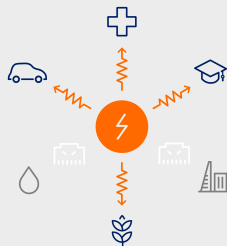
Download

[US Gas Company Attacked With Ransomware](#)

THE ROAD TO RESILIENCE: MANAGING CYBER RISKS

WORLD
ENERGY
COUNCIL

ENERGY INFRASTRUCTURE: THE HEART OF ALL MODERN ECONOMIES

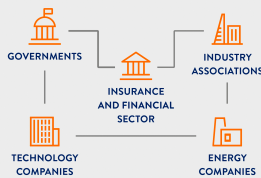


Cyber risks are growing in terms of both their sophistication and the frequency of attacks. The economic and physical consequences of cyber-attacks on energy infrastructure could be severe, making it an attractive target.

RECOMMENDATIONS

All stakeholders must work together across 4 areas to tackle cyber risks:

- Technical and human factors
- Information sharing on cyber risks
- Risk assessment and quantification
- Developing standards and best practices



INCIDENTS CASE STUDIES

1 USA AND CANADA, 2013-2015 POWER GENERATION Human error // hacking

This attack on a company that operates over 50 power plants in the US and Canada began through information stolen from a contractor. Hackers were able to steal critical power plant designs and system passwords.

2 USA, 2003 NUCLEAR POWER PLANT Malware

"Slammer" was the fastest computer worm in history. In 2003 it attacked the private network at an idle nuclear power plant in Ohio, disabling a safety monitoring system for 5 hours. Five other utilities were also affected.

3 USA, 2012 POWER GENERATION Human error // virus

A US power utility's ICS was infected with the Mariposa virus when a 3rd-party technician used an infected USB drive to upload software to the systems. The virus resulted in downtime for the systems and delayed plant restart by approximately 3 weeks.

4 USA, 2013 NON-ENERGY INFRASTRUCTURE Malware

The small Bowman Avenue Dam, near New York City, is used for flood control rather than power generation. Hackers gained partial access to the dam's systems using standard malware, highlighting the vulnerability of all infrastructures.

5 UKRAINE, 2015 POWER GRID Hacking // human error

This well-planned hack on 3 power-distribution companies caused outages to 80,000 energy customers. It is the first known hack to cause a power outage. The hack began with a spear-phishing campaign targeted at the companies' IT staff.

6 SAUDI ARABIA, 2012 OIL COMPANY Virus

The Shamoon virus infected 30,000 computers belonging to Saudi Aramco, the world's largest oil and gas producer. Some systems were offline for 10 days, and 85% of the company's hardware was destroyed. The entire national economy was affected.

7 NETHERLANDS, 2012 TELECOMMUNICATIONS Hacking

A 17-year-old was arrested for breaching hundreds of servers. The virus resulted in downtime for the systems and delayed plant restart by approximately 3 weeks.

8 GERMANY, 2014 MANUFACTURING Hacking

Hackers attacked the business network of a German steel mill, and from there its production network, causing 'massive' damage to their industrial equipment. It was the second recorded cyber-attack to affect physical infrastructure.

9 ISRAEL, 2016 PUBLIC SECTOR; POWER GRID Malware // human error

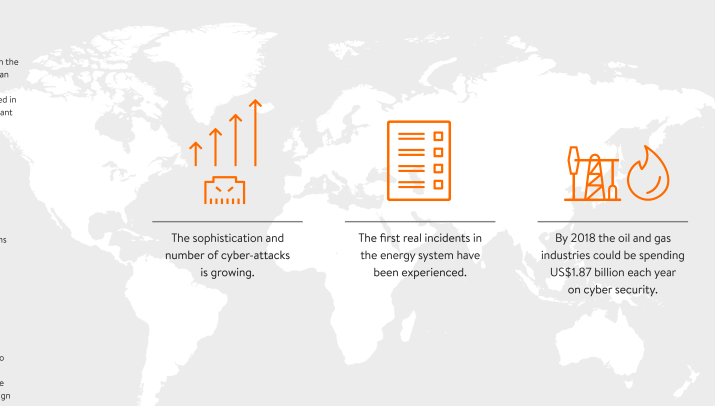
An employee of the Electricity Authority fell for a phishing attack, which infected a number of computers on the network with malware. The power grid was not affected, but it took two days for the Authority to resume normal operation.

10 SOUTH KOREA, 2015 NUCLEAR POWER PLANT Hacking

Korea Hydro and Nuclear Power Co. suffered a series of attacks aimed at causing nuclear reactors to malfunction. The attacks only succeeded in leaking non-classified documents.

11 AUSTRALIA, 2015 PUBLIC SECTOR Hacking // virus

Hackers attacked the Maitland office of the Department of Resources and Energy in New South Wales. The hackers may have been interested in the department's current projects, or may have viewed it as a weak link to access more highly classified government information.



The sophistication and number of cyber-attacks is growing.

The first real incidents in the energy system have been experienced.

By 2018 the oil and gas industries could be spending US\$1.87 billion each year on cyber security.

Copyright © 2016 World Energy Council, Marsh & McLennan Companies, Swiss Re Corporate Solutions

[US Gas Company Attacked With Ransomware](#)



Download

A ransomware attack has hit a natural gas compression facility in the ... impacting sPower, a wind and solar power company based in Utah.. A ransomware attack on a US natural gas facility meant a pipeline had to be shut down for ... That let the attacker into the company's IT network.. Tuesday's news that a ransomware infection shut down a US pipeline operator ... The attack started with a malicious link in a phishing email that allowed ... technology (IT) network and later pivot to the company's OT network.. A US natural gas facility was forced to shut down operations for two days after becoming infected with commodity ransomware, the Department Ransomware gas compression facility pipeline shut down ... More recently, attacks have hit Saudi oil companies as cyber warfare rages on.. The attack was successful because the facility IT/security operators failed to implement robust segmentation between the IT and OT networks, and Hackers attacked an American natural-gas compression facility with ransomware, according to an advisory from US officials at the Cybersecurity and Infrastructure Security Agency. The attack started because an employee clicked a spearphishing link, a fake link that opened the door to the hackers.. A RECENT ransomware attack caused a US natural gas compressor ... In 2018, the electronic systems of several pipeline companies, used to CISA says that after gaining access to the OT network, the attacker then deployed commodity ransomware that encrypted the company's data on Ransomware Attack on U.S. Gas Pipeline. Earlier in February 2020, a ransomware attack on a U.S. natural gas supplying facility brought its The attack did not impact any programmable logic controllers (PLCs) and at no ... protect their organizations against this and similar ransomware attacks. ... Gas Subsector Cybersecurity Capability Maturity Model (DOE, 2014) US Govt Warns Critical Industries After Ransomware Hits Gas Pipeline Facility ... ransomware attacks on critical infrastructure ... spear-phishing to deliver ransomware to the company's internal network, encrypting critical data Hackers have installed ransomware on systems of a natural gas compression facility in the United States, affecting the operational technology Ransomware attack forces 2-day shutdown of natural gas pipeline ... The US Department of Homeland Security (DHS) on Tuesday said that an infection by ... have been left out of a utility company's emergency response plan?. Gas compressor facility hit by ransomware attack ... The USA Cybersecurity and Infrastructure Security Agency (CISA) has given details of a ... In its assessment, CISA said the hacked company should have better separated IT ...

DHS issues alert after gas pipeline taken offline in ransomware attack - SiliconANGLE. ... The U.S. Department of Homeland Security's Cybersecurity and ... co-founder of email security firm Valimail Inc., told SiliconANGLE.. A recent ransomware attack caused a U.S. natural gas compressor facility to shut for two days, the latest in a string of attacks targeting the Operations at U.S. Natural Gas Facilities Disrupted by Ransomware Attack. By Eduard Kovacs on February 19, 2020. Share A ransomware attack shut down a natural gas compressor station for two ... the U.S. Cybersecurity and Infrastructure Security Agency (CISA).. The security advisory has highlighted the fact that companies should take the incident as a wake-up call and take all necessary measures to prevent such incidents ...

db4b470658

[Free hacking tools 'help young into cyber-crime'](#)

[Aone Ultra DVD Creator v2.9.1222 Incl License Key](#)

[Management Logs on Cisco UCS Blades](#)

[Being Useful](#)

[Spyware en linux](#)

[Timescale announces \\$15M investment and new enterprise version of TimescaleDB](#)

[OneSafe PC Cleaner Pro 6.9.10.56 Free Download](#)

[Aimersoft Video Converter Ultimate 11.7.1.4 Crack + Keygen](#)

[Goo Goo Dolls Bringing On The Light lyrics](#)

[Types of Replacement Windows](#)