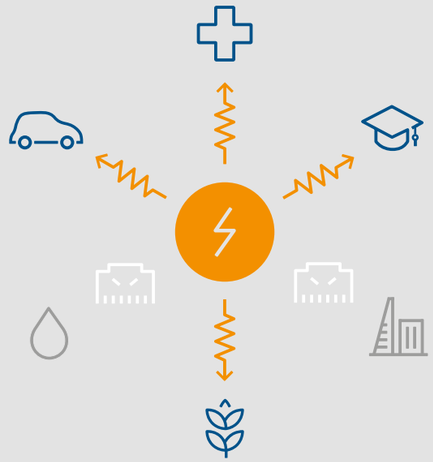
THE ROAD TO RESILIENCE: MANAGING CYBER RISKS

WORLD ENERGY COUNCIL

ENERGY INFRASTRUCTURE: THE HEART OF ALL MODERN ECONOMIES

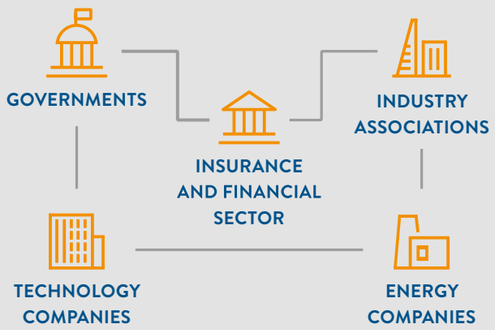


Cyber risks are growing in terms of both their sophistication and the frequency of attacks. The economic and physical consequences of cyber-attacks on energy infrastructure could be severe, making it an attractive target.

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 servers were maintained by a telecommunications company providing smart-meter services to utilities.

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.