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. 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.

5. 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. The second recorded cyber-attack to affect physical infrastructure.

6. SOUTH KOREA, 2015  
NUCLEAR POWER PLANT  
Hacking
Korea Hydro and Nuclear Power Co. was attacked by malware, causing nuclear reactors to malfunction.

7. 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.

8. AUSTRALIA, 2015  
PUBLIC SECTOR  
Hacking // virus
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.

9. 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.

10. USA, 2012  
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.

11. 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.

GOVERNMENTS
INSURANCE AND FINANCIAL SECTOR
TECHNOLOGY COMPANIES
ENERGY COMPANIES

The sophistication and number of cyber-attacks is growing.

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

GOVERNMENTS
INSURANCE AND FINANCIAL SECTOR
TECHNOLOGY COMPANIES
ENERGY COMPANIES

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