MOODY'S INVESTORS SERVICE

SECTOR COMMENT
8 November 2019

Rate this Research

Contacts

Lesley Ritter +1.212.553.1607
Vice President – Senior Analyst
lesley.ritter@moodys.com

Abhishek Tyagi +65.6398.8309
VP-Senior Analyst
abhishek.tyagi@moodys.com

Toby Shea +1.212.553.1779
VP-Sr Credit Officer
toby.shea@moodys.com

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Jim Hempstead +1.212.553.4318
MD-Utilities
james.hempstead@moodys.com

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

Infrastructure & Project Finance – Global

Cyberattack on Indian nuclear plant shows vulnerabilities of critical infrastructure

On 30 October, the Nuclear Power Corporation of India Limited (NPCIL) announced that a cybersecurity breach had occurred at its Kudankulam nuclear power plant, the largest nuclear power facility in India. The breach affected the plant's information technology (IT) network but there is no indication that the attackers successfully compromised the operational technology (OT) network, which monitors and operates the plant's physical operation. Nuclear reactors are typically heavily defended because of the potential consequences of an attack on these assets. Therefore, the disclosure of a cyber breach on this facility is a stark reminder that nuclear generation assets remain front of mind for sophisticated attackers.

From a credit perspective, the attackers' ability to remotely hack into the internet-connected IT network of the plant is negative regardless of the intent of the attack. The motive is not known, but likely motives include operational disruption or degradation, or intellectual property theft. Additionally, the fact that attackers were able to compromise a computer in a location purported to be among the most secure in India calls into question the effectiveness of the company's corporate governance oversight. NPCIL is not a public company; therefore, its disclosures are limited.

To date, there have been only a handful of well-publicized examples of malicious cyberattacks on critical infrastructure physical assets globally (see Exhibit 1). However, the risks are rising as state actors grow more interested in hacking into these critical infrastructure assets, according to the US Department of National Intelligence's 2019 Worldwide Threat Assessment Report.

Exhibit 1
Examples of prior attacks on critical infrastructure assets, classified by motive

	Survey & Reconnaissance	Theft & Monetization	Disrupt & Destroy
Purpose	- Gather industrial control system (ICS) related information - Establish points of access in ICS network	- Gather trade secrets or economically valuable information - Leverage ICS criticality for extortion or ransom	- Deny, degrade or destroy ICS operations - Cause process disruption or physical destruction
Example	- ALLANITE - DYMALLOY - Dragonfly	- NorskHydro 2019 - Rheinmetal Group 2019	- Nuclear enrichment plant, Iran 2010 - Electric distribution, Ukraine 2015 - Electric distribution, Ukraine 2016 - Oil & gas refinery, Saudi Arabia 2017

Sources: Dragos and Moody's Investors Service

Although the technology that operates the plant and its reactor reportedly run on a different network than the one breached, we still view an infection of the IT network as a material risk. That is because the breach could conceivably allow the attackers to view or modify content

on the compromised computer by uploading and exfiltrating files, including additional malware, and spreading them laterally through the network. This could infect further systems. Maintaining a strategic foothold in a nuclear plant's IT network could also make it easier for a motivated, well-funded attacker to pivot into the critical OT environment later on and carry out a disruptive or destructive attack in the future.

OT networks are gaining attention for their vulnerabilities to cyberattacks. These networks have newer cybersecurity practices that trail those of IT networks. The physical assets operating in the OT environment began to adopt digital technology in a meaningful way only recently. Furthermore, these assets were not designed with cybersecurity in mind. They were set up to operate on a standalone basis, in a siloed environment and over multiple decades, with the primary goal of achieving the highest levels of availability and reliability. As a result, the inherent nature of OT networks does not lend itself particularly well to good cybersecurity practices such as patching for new vulnerabilities, which requires assets to be brought offline. According to cyber experts cited in an October 2015 report from The Center for Strategic and International Studies, the defenses around OT are a full decade behind the current levels of defenses for information technology.

OT and IT environments are converging. The OT environment is changing as industrial asset owners rapidly add digital technologies to engineering equipment to realize the operational efficiencies and financial savings from adoption of these new tools. This move toward digitization and increased interconnectivity among networks is introducing new vulnerabilities to these critical sectors, and hackers are taking advantage of these attack vectors.

The Kudankulam plant, which has 2 gigawatts (GWs) of generating capacity, became operational only recently. Unlike the other 4.5 GW of nuclear plants operating in India that rely on domestically developed Pressurized Heavy Water Reactor (PHWR) technology, the Kudankulam plant relies on Russian Water-Water Energetic reactor technology (VVER) (see Exhibit 2). The plant also has another 2 GW under construction that will also use VVER reactor technology and is scheduled to go into operation in 2023.

Exhibit 2

Operational nuclear power plants in India

Power Station	Operator	State	Type	Units (MW)	Total capacity (MW)
Kaiga	NPCIL	Karnataka	PHWR	220 x 4	880
Kakrapar	NPCIL	Gujarat	PHWR	220 x 4	440
Kudankulam	NPCIL	Tamil Nadu	VVER-1000	1000 x 2	2,000
Madras (Kalpakkam)	NPCIL	Tamil Nadu	PHWR	220 x 2	440
Narora	NPCIL	Uttar Pradesh	PHWR	220 x 2	440
Rajasthan	NPCIL	Rajasthan	PHWR	100 x 1 200 x 1 220 x 1	1,180
Tarapur	NPCIL	Maharashtra	BWR PHRW	160 x 2 540 x 2	1,400
				Total	6,780

Source: Nuclear Power Corporation of India Limited

Nuclear power plants are within the electric utilities sector, which we view as highly vulnerable to cyberattacks. (See Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019.) The sector's foundational role in supporting most aspects of a country's broader economy and way of life amplifies the risk of a successful cyberattack and, consequently, makes it a prized target for attackers interested in causing widespread harm and disruption. Select segments of the industry also use cutting-edge technology, which makes these companies particularly exposed to intellectual property theft as well as operational risks.

Plant's forensics indicate targeted malware did not infect its OT systems

NPCIL notified the Indian Computer Emergency Response Team on 4 September that it had fallen victim to a successful targeted malware attack that infected a computer connected to its IT network. Forensics of the attack by Dragos, an industrial control system cybersecurity firm, identified computer code samples that appear to allow the attacker to establish a Remote Access Tool (RAT) in the victim's IT network. A RAT can be used to steal data as well as enable control over infected systems.

Cyber forensic experts think the analyzed samples could align with the RAT malware known as DTrack. Researchers first disclosed DTrack in late September 2019 and identified the tool as targeting Indian financial institutions and research centers. DTrack has no industrial control systems specific component that would interact with any control systems that monitor or operate the plant.

The number of victims affected by the DTrack RAT is still very low, and cybersecurity experts have not been able to identify a precise security hole that the attackers might have used to deliver the threatening program.

Moody's related publications

Sector In-Depth

» Regulated utilities and power companies - North America: Grid modernization heightens vulnerability of utilities to cyberattacks, November 2019

» Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, October 2019

» Electric and gas – US: Pipeline cybersecurity standards help plug security loophole in utility supply chain, July 2019

» Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019

» Regulated electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high, September 2018

» Public power electric utilities - US: Growing grid interconnectivity increases cybersecurity risks, June 2017

Sector Comments

» Norsk Hydro ASA, Severe cyberattack forces operations into partial manual mode, a credit negative, March 2019

» Utilities and power companies – US: GAO's call for improved electric grid cybersecurity oversight is credit positive, but highlights vulnerability risk, October 2019

» Utilities remain vulnerable and attractive target of cyber attacks, a credit negative, January 2017

Topic Page

» Cyber Risk

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

REPORT NUMBER 1201930

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

MOODY'S
INVESTORS SERVICE