MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
8 November 2019

Rate this Research

TABLE OF CONTENTS

Analyst Contacts

Ryan Wobbrock +1.212.553.7104
VP-Sr Credit Officer
ryan.wobbrock@moodys.com

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

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

Jillian Cardona +1.212.553.4351
Associate Analyst
jillian.cardona@moodys.com

Michael G. Haggarty +1.212.553.7172
Associate Managing Director
michael.haggarty@moodys.com

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

Regulated utilities and power companies - North America

Grid modernization heightens vulnerability of utilities to cyberattacks

» **Adoption of digitally enabled grid modernization equipment expands utilities' cyberattack surface.** Electric, gas and large water utility companies are increasingly investing in advanced technology assets that aim to improve operational efficiencies, infrastructure reliability and enhance customer service. However, much of the technology used in these efforts also heightens the utility industry's exposure to cyber threats because the equipment is connected to the internet or allows for remote access that can be infiltrated.

» **Third party vendors also raise cyber vulnerabilities for utilities.** The operation of a power grid incorporates a considerable amount of equipment and monitoring provided by various third party vendors. Many of these companies have less sophisticated cyber defenses, thereby exposing utility operations and networks to threats that utilities cannot directly monitor or prevent.

» **Cyberattack scenarios point to a wide range of credit-negative consequences.** A successful hack could include small disruptions, such as a degradation of a process that erodes operational efficiency or large disruptions that cause a long-term service outage. Cyber attacks can also result in the destruction of property, plant and equipment or even impaired safety responses that threaten workforce health.

» **Cost recovery provisions authorized by regulators help mitigate credit impact.** For now, we continue to incorporate a view that an affected utility will be able to recoup any cyberattack costs. Even in the case of a large, widespread cyber event, we think both federal and state agencies will support a utility's recovery effort, because utilities are critical infrastructure assets.

» **Efforts to strengthen utility and grid cybersecurity have a long way to go.** Many federal, state and industry agencies are dedicated to mitigating cyber risk for the power grid. While each of these organizations are helping to address some of the risks facing utilities, there is no central oversight to harmonize these efforts or to ensure the overall effectiveness of piecemeal security measures. Moreover, what oversight there is can lead to a culture of compliance for utilities. Compliance standards have no material relationship to the actual level of protection provided by a utility's cyber defenses.

Adoption of digitally enabled grid modernization equipment expands utilities' cyberattack surface

North American electric, gas and water utilities are increasingly investing in advanced technology assets that aim to improve operational efficiencies and infrastructure reliability, while reducing costs and enhancing customer service. These investments are often the underpinning infrastructure through which states advance important public policy goals, such as carbon emission reduction through distributed renewable electric generation or water conservation through reduced pipe leakage and loss.

However, the technology used in these efforts also heightens the industry's exposure to cyber threats because the equipment uses communications technology that can ultimately connect to utility industrial control systems (ICS). In addition to accessing a utility's ICS, the equipment supplier or other vendor is also provided physical or remote access to operate and monitor the asset. As a result, we see the equipment as a path that can increase the attack surface for cyber hackers. The ability to infiltrate a utility's operating networks and ICS can provide opportunities to create service disruptions, damage equipment, cause injury and have harmful economic, environmental and even safety repercussions. If such an event were to occur, a utility could conceivably lose the support of its regulators and politicians.

In our grid modernization example, investments can take many forms and could include widely used equipment and systems, such as transformers, wind turbines, solar panels, electric vehicle charging stations, drones, cloud data storage and global positioning systems. We also see a widening attack surface affiliated with a utility's efforts to incorporate the use of advanced data analytics that include remote monitoring, information technology (IT) and operating technology (OT) control and other artificial learning technologies. Each of these investments carries its own type of cyber risk that utility management attempts to mitigate and defend against.

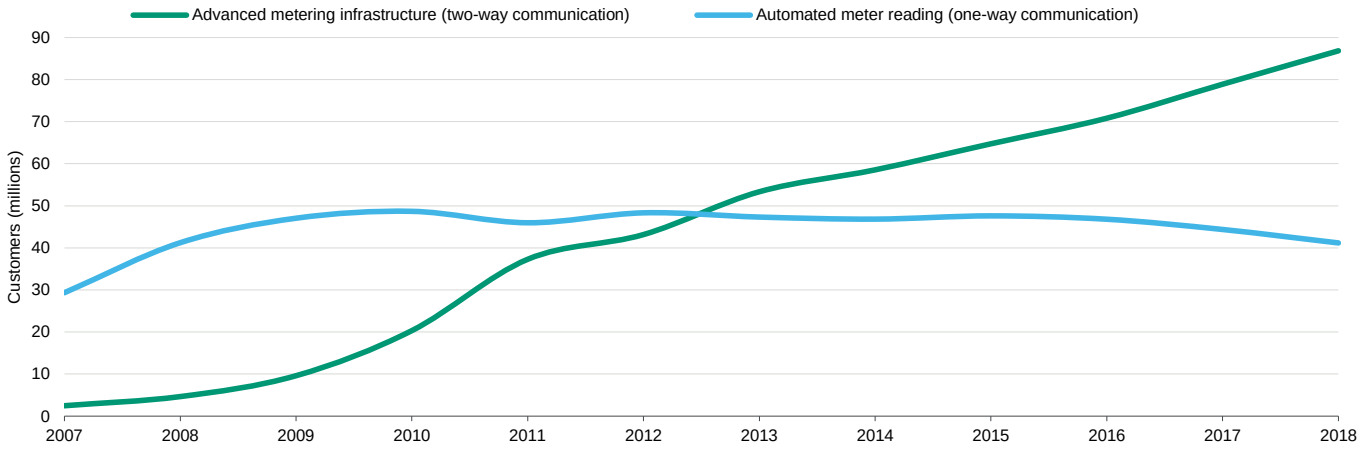
Advanced meter infrastructure illustrates the appeal and potential perils of grid modernization

A prime example of grid modernization investment has been the expanding use of advanced metering infrastructure (AMI). Advanced metering systems can monitor customer usage and asset performance, with the intent of sending the data back to utility operators as actionable information. Utilities can remotely access some meters to understand and control commodity flows within the infrastructure network. By contrast, older automated meters provide only one-way communication back to a utility.

Exhibit 1

Industry use of advanced meters is on the rise

US advanced electric utility meter adoption, 2007-2018



Source: US Energy Information Administration

By gaining access to a utility's AMI, a hacker could tamper with the operations of these assets on a localized, distribution level. Using demand-side communications, a hacker can generate inaccurate measurements of volume requirements or trigger incorrect responses from the victimized utility.

The risks posed by an attack on a utility's AMI could escalate if a hacker gained access to the AMI's two-way communication feature and used it as a pathway into a utility's ICS. But to do so, the attacker would need to have a much broader level of knowledge of the utility control environment and the ability to pivot and advance through multiple layers of network defenses.

Today, we see most utilities attempting to silo key management systems, best illustrated by the way the power sector manages distribution-level activities separately from the bulk electric system. The sophistication of these utility defenses are likely to vary greatly among electric, gas and water utilities, with significant disparities between larger companies with well-funded cyber defense programs and smaller utilities that lack of the same level of financial resources or workforce talent.

Third-party vendors also pose cyber vulnerabilities for utilities

Utility operations incorporate the equipment and services of various third parties throughout the energy and commodity delivery supply chain. These companies often have a different set of cyber defenses, thereby exposing utility operations and networks to indirect threats that utilities cannot accurately monitor or prevent.

For example, equipment manufacturers in China and Russia supply critical infrastructure components that are widely used throughout the industry, like certain software applications and telecommunications equipment. According to the US Computer Emergency Response Team (US-CERT), these countries are known for active cyber espionage and tampering with the physical operations of utility facilities.

Similarly, numerous small vendors can have access to utility networks to perform a myriad of services including engineering, construction, information technology and consulting advice. As trusted vendors, these outside parties may be provided access authority to a utility's operational networks. For these reasons, the sector is actively looking to improve the vetting process and best practices regarding third-party vendors and supply-chain management.

Another source of potential utility disruption exists in the interdependencies between sectors, such as oil and gas production, natural gas pipeline transportation and local gas distribution, through vertically integrated or intersector touch points. These connections mean that a cyber disruption affecting another industry could have a cascading impact on a utility's operations. For instance, if a natural gas pipeline was disrupted, it could affect the fuel source for an electric generation plant. Similarly, an extended power outage could impact the operations of water treatment plant or the pumping system of a water or wastewater utility with insufficient backup generation.

Even a utility's customer base can pose risks to how a utility operates, through internet-connected devices like digital thermostats or water heaters. As customers increasingly employ demand-side technology, hackers could tamper with the settings and cause artificial demand signals to be sent to utilities and regional planning organizations, which could place stress on utility assets if automated or manual responses react in an unnecessary way.

Cyberattack scenarios point to a wide range of credit negative consequences

If a threat actor were to access the ICS of a utility, there are wide-ranging consequences that would be negative for the affected utility's credit. These could include small disruptions, such as degradation of a process that erodes operational efficiency, to large disruptions that cause a long-term service outage, the destruction of property, plant and equipment or even impaired safety protocol that threatens workforce health.

Small operational disruptions could lead to reputational or branding problems for utilities, which may hurt regulatory and stakeholder relationships. These events would more directly affect utilities that are held to operational standards as part of regulatory reviews, including utility performance against required customer service metrics, management effectiveness audits and benchmarking/indexing around operations and maintenance (O&M) expenses.

We continue to consider large disruptions, with a prolonged service impact, as Event Risk. In these cases, we believe that federal assistance and governmental intervention is likely and that a more broad suite of resources would be deployed to help an affected utility respond to, and recover from, the impact. However, it could also result in an immediate increase to the cost of capital for the utility and the broader sector if equity and fixed-income investors become more cautious and view the sector as higher risk.

Historical progression of high profile ICS and other events

We think one of the largest cyber risks that utilities face is a compromised ICS. If a hacker gains access to a company's ICS, past events have shown that facilities could experience equipment manipulation, impaired operations and compromised safety. We summarize three of the more prominent ICS attacks, below.

Stuxnet: This event was an attack on an Iranian uranium enrichment facility. Attackers used malware to modify operational processes of the plant to cause failures in enrichment equipment. In summary, the operators were not receiving accurate, real time readings of their equipment, resulting in damage to the equipment.

Ukraine attacks: The ICS of the Ukraine power grid was penetrated in 2015 and 2016 (named "CRASHOVERRIDE"), resulting in the manual opening of breakers at a transmission substation and disabling machines infected by malware. The attack also included a denial of service to the site's communications systems, and disabled the grid system's protective measures. This impacted the utility's ability to take reactive response measures, although the power was restored in a relatively short duration. Since the hackers had control of the breakers, it is possible they could have reopened the breakers out of phase, thereby resulting in more catastrophic damage to the equipment.

TRISIS: In 2017, attackers gained access to the safety instrumented system of a petrochemical plant in Saudi Arabia. Here, the attack compromised the operations of safety equipment, which cybersecurity experts say could have resulted in the denial of access to operations (i.e., telling operators that the plant was unsafe), destruction of equipment (i.e., allowing operations to continue despite hazardous conditions) or a more basic trip of the equipment.

Utah communications outages: In March 2019, a cyberattack on Utah renewable energy developer sPower momentarily cut off communication between its control center and its wind and solar generation assets. The North American Electric Reliability Corporation provided the following account of what happened: "A vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. This resulted in a denial of service condition at a low-impact control center and multiple remote low-impact generation sites. These unexpected reboots resulted in brief communications outages (i.e., less than five minutes) between field devices at sites and between the sites and the control center." (See "Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities," North American Electric Reliability Corporation, September 4, 2019.)

Malware attack on Indian nuclear plant: On 30 October 2019, the Nuclear Power Corporation of India Limited (NPCIL) confirmed that the Kudankulam power plant, the country's largest nuclear power plant, was the target of a malware attack through an infected personal computer that was connected to the plant's system for administrative purposes. The NPCIL also stated that the malware attack was isolated from the plant's critical internal network and that plant systems were not affected.

Cost recovery provisions will be key to future credit implications

The ability of affected utilities to recoup costs incurred after a cyberattack in a timely manner will be a key determinant of credit impact. We expect that state commissions will be supportive of recovering costs related to a cyber breach and the bolstering of system defenses.

While it is possible that utility commissions could act punitively toward an affected utility by disallowing cost recovery or reducing future allowed returns, it is more likely that the industry will react to a notable cyber event by improving safety precautions, requiring additional capital to be deployed for defense and enhancing cost recovery for utilities.

This view is premised on the reaction to the 2010 explosion of a Pacific Gas & Electric Company natural gas pipeline in San Bruno, California, which resulted in the deaths of eight people. In response to this event, state politicians and regulators encouraged pipeline operators to invest more heavily in the system in an effort to accelerate the replacement of old and leak-prone pipe. In the case of cyber safety, an increased focus on building stronger defenses would be credit positive for the sector and could even improve financial performance, just as the proliferation of pipeline replacement trackers did for many local gas distribution companies following the San Bruno incident.

It appears that state regulatory commissions have been supportive of cybersecurity expenditures to date, given that very little has been disallowed or has been a point of contention as part of cost proceedings. But this is based on largely anecdotal evidence because cyber defense budgets and expenditures are not widely publicized. One public example is found in the state of Virginia, where the Virginia State Corporation Commission denied the vast majority of Virginia Electric and Power Corporation's (A2 stable) $6 billion, 10-year, grid modernization plan in January 2019. The one item that the commission did approve was a roughly $155 million investment for cyber and physical security.

The ratemaking process has elements that can indirectly interfere with the way utilities use cybersecurity vendors. Many vendors employ business models which are predicated on generating regular fees for service. This type of contractual arrangement is generally considered an O&M expense for utilities and is recovered dollar-for-dollar in rates. However, utilities usually favor investments that are characterized as capital spending, as opposed to O&M expense, because the former is allowed to generate a return on the capital deployed.

As cyber risks become better understood by stakeholders, we envision that the recovery of costs related to cybersecurity will evolve as well. Some of the developments could come in the form of shorter depreciable lives for obsolete or at-risk equipment; implementing a standard level of cyber expense in base rates or certain costs allowable as capital expenditures; creating cyber event funds, similar to storm reserves; or even adjustments to allowed return on equity levels as cyber risks become more easily identifiable (similar to the "size" adder that some regulators grant small utilities that are more sensitive to financial disruptions).

Efforts to strengthen cybersecurity of utilities and grid have been piecemeal to date

There is a myriad of organizations with industry oversight that apply security standards and best practices to bolster utility cyber preparedness, enhance intercompany communication and coordinate industry response to cyber attacks.

Agencies like the Department of Energy, the Department of Transportation, the Department of Homeland Security, the North American Electric Reliability Corporation (NERC) are rule making authorities that create compliance standards, whereas industry groups like the Edison Electric Institute, the American Gas Association and the National Association of Water Companies are some of the more prominent agencies that seek to communicate, share and promote best practices across the sector landscape.

These entities are continually enhancing industry practices with regard to cybersecurity and addressing topics such as supply chain procurement practices and vendor requirements. While each of these organizations are helping to mitigate some of the risks facing utilities, there is no central oversight to harmonize these efforts or to ensure the overall effectiveness of piecemeal security measures.

Bulk electric systems are subject to NERC critical infrastructure protection standards, which date back over a decade and offer the best example of electric industry coordination. Once again, differences in oversight and sector responses are likely to occur among electric, gas and water utilities and between critical infrastructure industries and those with less regulatory oversight, such as manufacturing or even telecommunications.

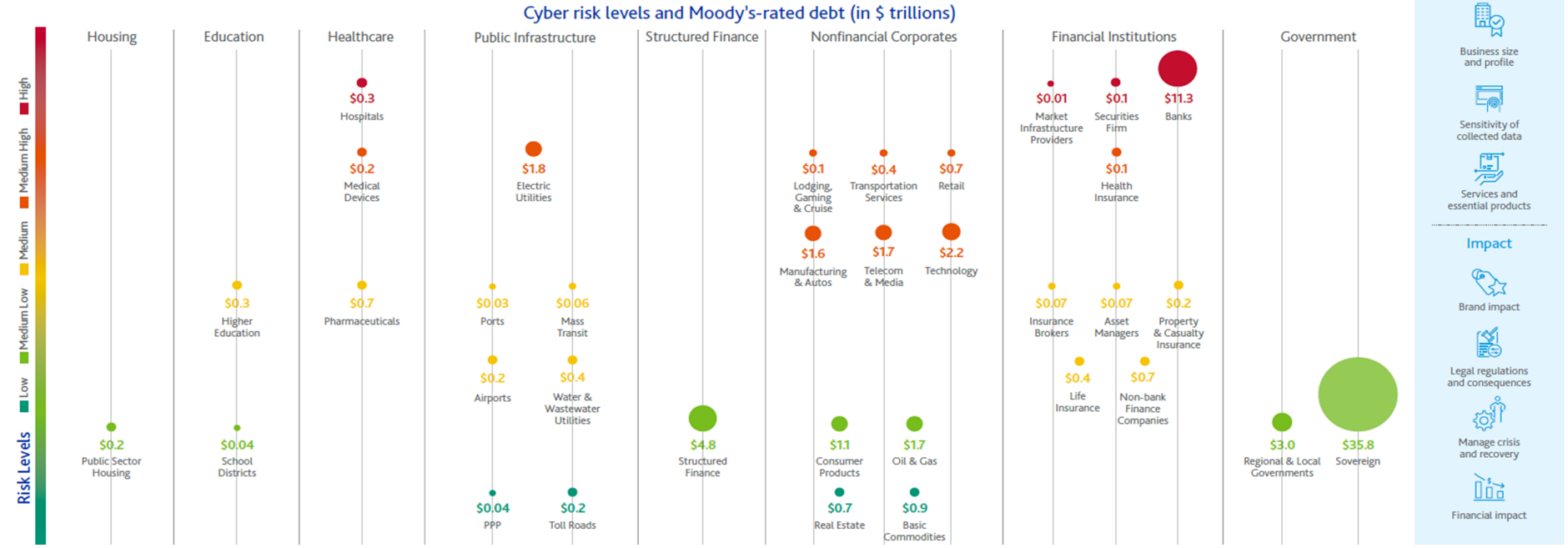
As such, there are generally no significant penalties for noncompliant utilities and few measures to ensure best practices are being followed. Moreover, none of these regulations are directly applied to external third parties that might still have access to utility ICS. This patchwork of defense oversight exposes the sector to a weakest-link risk that cannot be fully secured and could have an indirect impact on other utility or sector operations.

Differences in utility size and financial wherewithal can also lead to significant disparities in cyber defenses and security practices. Larger, better funded utility systems have more resources to deploy toward cyber defense, both by way of capital budgeting and in their ability to attract and retain workforce expertise. Therefore, these utilities can afford to employ the most sophisticated security measures that go beyond compliance measures and focus more on overall risk mitigation. Smaller utilities, on the other hand, can only do so much with their resources. They may be limited to more of a compliance approach to cyber issues, versus a robust security plan.

Appendix

Cyber Risk: Credit Risk Exposure by Sector

The growing intersection of supply chains, connectivity and access to data is increasing the potential for significant cyberattacks, creating new risks for governments and businesses worldwide. Moody's assessed the inherent cyber risk exposure of 35 broad sectors based on two factors: vulnerability to a cyber event or attack, and impact in terms of potential disruption of critical business processes, data disclosure and reputational effects.



Source: Moody's Investors Service

Moody's related publications

Sector In-Depth

» Retail and Commercial Banks – Global: Growing digitalization increases banks' cyber risk exposure, October 2019

» Cyber Risk – Global Investment Banks: GIBs heighten readiness against constant cyber threat, October 2019

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

» Local government - US - Ransomware attacks highlight importance of IT investment and response planning, October 2019

» ESG – Global: Governance considerations are a key determinant of credit quality for all issuers, September 2019

» Hospitals & health service providers - US: Cyberattacks pose growing operational and financial risks for hospitals, September 2019

» Corporates - Global: Deepfake disinformation campaigns pose reputational risks to businesses, August 2019

» P&C Insurance — Global: Battling hidden cyber exposures, insurers position for growing opportunity, July 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

Sector Comments

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

» Financial Institutions – South Korea: Korean banks bolster investment in cybersecurity, a credit positive, September 2019

» Exchanges and Clearing Houses – US: Options Clearing Corporation's risk management failures are credit negative, September 2019

» Medical products and devices – US: Innovation improves patient outcomes, but brings cyber risk and tech interlopers, July 2019

» For-Profit and Not-For-Profit Hospitals – US: Hospitals invest in data collection, telemedicine to reduce cost, July 2019

» Healthcare - US: Data breach at Quest and LabCorp highlights cyber risk in vendor relationships, June 2019

» Defense – US: Greater cybersecurity accountability for defense contractors would be credit negative, May 2019

» Financial Institutions – Europe: European financial authorities recommend cybersecurity legislation, a credit positive for financial institutions, April 2019

Non-Credit Rating Assessment Framework

» Non-financial companies – Global: Corporate governance assessments for publicly traded non-financial companies, July 2019

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 1198162

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