Michael Best

April 13, 2020

Federal Agencies Warn of COVID-19 Implications for Energy Sector Cybersecurity

Federal agencies tasked with various aspects of energy regulation are encouraging situational awareness and coordination in light of increasingly frequent reports of ransomware and other cybersecurity attacks on utilities during the COVID-19 pandemic.

In particular, the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) has been closely monitoring the pandemic since January. CESER recently advised energy sector partners to "work with the Electricity Information Sharing and Analysis Center (E-ISAC), the Downstream Natural Gas ISAC (DNG-ISAC), and the Oil and Natural Gas ISAC (ONG-ISAC) to remain vigilant to cybersecurity threats, including COVID-19 themed phishing emails, and to ensure that the latest cybersecurity guidance is provided to their organizations." In the same statement, CESER also urged energy sector companies to "assess the full breadth of risk within the supply chain, including that of managed and industry service providers to evaluate how COVID-19 may affect service and their contractors' approach to service delivery."

For electric utilities, E-ISAC states that the Cybersecurity Risk Information Sharing Program (CRISP) platform remains fully operational and is being monitored continually by E-ISAC Watch Operations. Posting actionable and timely information in the event of a cybersecurity attack will allow E-ISAC to fulfill its role in providing coordination, communication and incident response services to mitigate damage. Additionally, E-ISAC is working to establish communication protocols with data analytics organizations including the Pacific Northwest National Laboratory (PNNL).

Currently, CESER maintains a COVID-19 landing page with links to cybersecurity guidance provided by the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Federal Emergency Management Agency (FEMA), and more. DHS and CISA recently issued a joint National Cyber Awareness Alert providing technical

Related Industries

Energy

Related Practices

CARES Act Relief
COVID-19 Resource Center
Energy Law
Privacy & Cybersecurity
Regulatory

details of recent attacks, as well as information regarding indicators of compromise and threat-specific guidance for mitigation.

In general, energy sector companies should ensure that they have established certain baseline cybersecurity defenses including:

- **Secure connections**. As organizations explore various alternate workplace options in response to COVID-19, companies must protect the security of information technology systems by implementing multi-factor identification ensuring that Virtual Private Networks and other remote access systems are fully patched.

- **Observation for abnormalities**. Companies must enhance system monitoring to receive early detection and alerts on abnormal activity. This includes ensuring that all machines have properly configured firewalls as well as anti-malware and intrusion prevention installed. Some routine monitoring can be automated, freeing time for relevant personnel to investigate suspicious activity.

- **Preparation for incident response**. It is now critical that companies have updated incident response plans to consider workforce changes in a distributed environment. Plans must also be updated to reflect the fact that incident response for the foreseeable future must be effective even with limited on-the-ground support and distributed remote-expert support. Companies should immediately seek the advice of counsel if they need assistance with these updates.

Michael Best & Friedrich remains committed to helping our energy sector clients navigate evolving challenges associated with the pandemic, including heightened cybersecurity threats. Our team can tailor response plans for your organization, and can also design and deliver tabletop exercises to practice and refine your organization's breach response procedures. For more information about the business and legal implications of the coronavirus pandemic, please contact any of us, or your Michael Best attorney.

Related People

William Booth
Partner
wdbooth@michaelbest.com
T 202.747.9568

Eric Callisto
Partner
ejcallisto@michaelbest.com
T 608.283.4437

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164