HOUSTON
BUSINESS JOURNAL

7 steps for greater energy industry cybersecurity

J.C. BOGGS
Expert contributor

Earlier this year, the U.S. Department of Energy published guidance to help electricity, oil, natural gas and other energy companies assess and improve their cybersecurity systems' abilities to withstand attacks while maintaining critical functions.

The DOE's "Energy Sector Cybersecurity Framework Implementation Guidance" identifies risk management tools, processes, standards and guidelines that are currently being used across the energy sector and are well-aligned with National Institute of Standards and Technology's cybersecurity framework.

In particular, the DOE's guidance provides energy companies with information on how to assess their current and targeted posture, as well as how to identify gaps or strengths in their current programs.

The guidance is comprised of seven distinct steps:

1. Identify where you should apply the NIST framework to evaluate and potentially guide the improvement of your cybersecurity capabilities. This decision is typically based on risk management considerations, organizational and critical infrastructure objectives and priorities, availability of resources and other similar factors.

2. Review your systems, assets, requirements and cybersecurity and risk management practices. A good general rule is to focus initially on critical systems and assets, and then, expand your focus to less critical systems and assets as resources permit.

3. Create a current profile by identifying your company's cybersecurity and risk management practices. Quite a few organizations already perform regular evaluations of their cybersecurity programs through internal audits or similar activities.

The DOE's guidance provides energy companies with information on how to assess their current and targeted posture, as well as how to identify gaps or strengths in their current programs.

4. Conduct a risk assessment to evaluate cybersecurity risks and determine which are outside of current tolerances. For companies that have a risk-management program in place, this activity should be part of regular business practices.

5. Create a target profile that will include current risk management practices, current risk environment, legal and regulatory requirements, business and mission objectives, and any applicable organizational constraints.

6. Analyze and prioritize gaps between your current and target profiles, and determine the potential consequences of failing to address those gaps.

7. Implement an action plan, and track its progress over time, ensuring that gaps are closed and risks are closely monitored.

This seven-step approach is designed to help electricity, oil, natural gas and other energy companies establish robust cybersecurity programs but may also be used to validate the effectiveness of existing programs. It is intended to be a continuous process – repeated according to company-defined criteria to address the evolving risk environment – and should also include a plan to communicate progress to senior management and other stakeholders.

By helping energy companies better understand how they can leverage the NIST framework's prioritized approach, the DOE's guidance will likely prove a valuable resource to entities looking to create and sustain resilient systems that can survive a cyberattack.

J.C. Boggs is a partner with King & Spalding's government advocacy and public policy practice group in Washington, D.C. He is also a member of the firm's data, privacy and security practice. He can be reached at jboggs@kslaw.com.