CITE AS
36 *Energy & Min. L. Inst.* 28 (2015)

Chapter 28

Cybersecurity in the Era of Unconventional Development: Is the Energy Sector Ready for Cyber Attacks?

Roberta D. Anderson
K&L Gates LLP
Pittsburgh, Pennsylvania

Thomas R. DeCesar
Stephen J. Matzura
K&L Gates LLP
Harrisburg, Pennsylvania

George A. Bibikos
Cozen O'Connor
Harrisburg, Pennsylvania

Synopsis

§ 28.01. Introduction.

The energy industry is vast and growing. As the industry continues to grow, it becomes a more frequent target for cybersecurity hacks and data breaches. As noted by the American Petroleum Institute: "The petroleum industry is a worldwide industry that is highly dependent on technology for its communications and operations. Technological advances that promote better efficiency and more automation within the petroleum industry also make information security an increasingly important issue." This article provides an outline of the risks in the energy sector for cyber attacks, evaluates the legal framework governing cybersecurity, identifies and evaluates insurance coverage issues, and provides general guidelines for cyber risk management that energy companies may wish to consider as they develop their cybersecurity programs.

[1] — Energy Development.

Like other industry sectors, energy companies must be aware of the looming and growing cyber threat so they can protect themselves accordingly. In general, the main industry sectors that make up the bulk of the energy industry include:

- *The Upstream Industry*. This energy sector generally consists of those companies engaged in the exploration and production phase of energy development, both on-shore and off-shore. This