

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.....	1081
	[1] — Energy Development	1081
	[2] — Types of Data in the Energy Sector	1082
	[3] — Types of Cyber Attacks and Risks in the Energy Sector	1083
	[4] — High-Profile Cyber Attacks on the Energy Industry	1084
§ 28.02.	Legal Framework.....	1084
	[1] — Federal Law	1084
	[a] — Executive Orders	1085
	[b] — Proposed Legislation	1086
	[2] — Energy-Specific Statutes, Regulations, or Standards	1086
	[a] — Federal Energy Regulatory Commission (FERC).....	1087
	[b] — Nuclear Regulatory Commission (NRC)	1087
	[c] — Department of Homeland Security (DHS)	1087
	[d] — Department of Energy (DOE)	1088
	[3] — State Law	1088
	[a] — Security Breach Laws.....	1089
	[b] — Data Disposal Laws	1089
	[4] — Industry Standards.....	1090
	[a] — National Institute of Standards and Technology (NIST).....	1090

	[b] — Department of Justice Guidance	1090
	[c] — American Petroleum Institute (API).....	1091
	[d] — Information Sharing and Analysis Centers (ISACs)	1092
§ 28.03.	Civil Litigation Resulting from Cyber Attacks	1092
	[1] — Civil Enforcement Actions by Government Agencies for Inadequate Cybersecurity	1092
	[2] — Claims Against Entities that Experienced a Data Breach	1097
	[a] — Negligence for Failure to Protect Data	1097
	[b] — Breach of Contract (Express or Implied) for Failure to Protect Data	1098
	[c] — Failure to Comply with State Statutes Related to Computers and Electronic Data	1098
	[d] — Other Types of Claims Related to Data Breaches	1099
	[3] — Shareholder Derivative and Securities Claims Resulting from Data Breaches	1099
	[4] — Claims by Hacked Entities Against Hackers (Assuming They Are Identified).....	1100
	[a] — Computer Fraud and Abuse Act.....	1100
	[b] — Wiretap Act and Electronic Communications Privacy Act.....	1102
	[c] — Stored Communications Act	1103
	[d] — Trade Secret Protection Laws	1103
	[e] — Other Types of Claims Against Hackers	1104
	[5] — Claims by Hacked Entities Against Cybersecurity Vendors	1104
	[a] — Negligence for Failure to Protect Data	1104
	[b] — Breach of Contract for Failure to Protect Data	1104
	[c] — Other Types of Claims for Failures of Cybersecurity Vendors	1105
	[6] — Barriers to Claims and Limits on Liability Related to Data Breaches	1105
	[a] — Standing for Asserting Claims Based on Data Breaches.....	1105
	[b] — Absence of Cognizable Injury from Data Breaches.....	1106
	[c] — Contractual Limits on Claims Arising from Data Breaches.....	1107
§ 28.04.	Contracts that May Be Impacted By Data Breaches.....	1108
	[1] — Contracts with Software Vendors.....	1108

[2] — Contracts with Third Parties in the Supply Chain.....1109

[3] — Drafting Considerations for Contracts to Address Issues
Arising from Data Breaches1109

§ 28.05. CyberSecurity Training/Planning/Remediation1110

[1] — A Cybersecurity Plan 1111

[2] — Before Creating a Cybersecurity Plan 1111

[3] — Creating a Cybersecurity Plan 1111

[4] — Training 1112

[5] — Model Plan (Adapted from Department of Justice
Guidance) 1112

[6] — Information Sharing 1113

§ 28.06. Insurance Coverage1113

[1] — Potential Coverage Under “Legacy” Policies 1113

[2] — Cybersecurity Insurance Policies..... 1116

§ 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