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

includes lease and mineral rights acquisition, exploration efforts (including seismic), well site construction, drilling, casing/cementing, stimulation, and production.

- *The Midstream Industry*. The midstream industry generally consists of those companies engaged in the movement of oil or natural gas, including transportation by pipeline, rail, tankers, or barge. Midstream activities may also include some treatment and processing of oil or natural gas, marketing, and storage.

- *The Downstream Industry*. The downstream industry generally consists of those engaged in the refining process, the distribution and sale of oil or natural gas to consumers (utilities), or the manufacture of products.

- *The Service Industry*. The service industry consists of those companies that provide services to oil and gas development companies, including lease brokers, geophysical exploration companies, construction companies, drilling contractors, cementing and casing service providers, and providers of completions operations (fracture stimulation).

These various industry sectors have a number of different types of data that may be desirable to entities seeking to penetrate the energy sector for commercial benefit.

[2] — Types of Data in the Energy Sector.

While the susceptible information in some industries would only include personally-identifiable information or banking information – such as credit card numbers – the energy industry is different. Potential types of data that may be breached include:

- Business Information.
- Trade Secrets.
- Operations, Communications Control Systems, and Infrastructure.
- Employee or other Personal Information.
- Contractors and Supply Chain.

In addition, the energy industry has unique considerations given its role in the nation's infrastructure and importance to the national economy and national security. Since the nation relies on different types of energy for so many critical processes at all times, a significant cybersecurity breach in the energy industry would be particularly devastating.

[3] — Types of Cyber Attacks and Risks in the Energy Sector.

The resourcefulness of hackers and variety of potential cybersecurity attacks further complicates matters because the energy industry must be prepared for an incredibly wide range of potential threats. Such threats can range from mere theft to significant energy system takeovers affecting wide ranges of the country. Such attacks can include:

- Advanced Persistent Threats (APT)
- Cybercriminals, Exploits, and Malware
- Denial of Service (DDoS)
- Domain Name Hijacking
- Corporate Impersonation and Phishing
- Employee Mobility (Disgruntled Employees)
- Lost or Stolen Laptops or Devices
- Inadequate Security and Systems Provided by Third Party Vendors

Moreover, cybersecurity threats within the energy industry create several types of significant risks to the energy industry. Some threats are seen in a variety of industries, and are not particular to the energy industry. For instance, there is a risk that a data breach could cause loss of web presence, interception of emails and data communications, or brand tarnishment and reputational harm. However, there are also several types of risks particular to the energy sector. These include loss of intellectual property and trade secrets, compromising of personal information, and legal and regulatory implications.

[4] — High-Profile Cyber Attacks on the Energy Industry.

As a whole, the energy sector (especially in the United States) has thus far dodged some of the most extensive cybersecurity attacks. However, there have been several high-profile cybersecurity attacks within the energy industry. To illustrate:

- *Operation Night Dragon*. In this attack, hackers used several locations in China to compromise servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, and acquire proprietary and highly confidential information. The hack was elaborate and extensive, lasting approximately four years.
- *Saudi Aramco*. In this attack, hackers used malware to compromise 30,000 workstations of the Saudi company.
- *Operation "Oil Tanker": The Phantom Menace*. In May 2015, an IT (information technology) company issued a report detailing cyber attacks against ten or more companies in the oil-and-gas maritime transportation sector that were ongoing since August 2013. Panda Security reported that the unique email-based attacks against oil cargo companies did not use malware detectable by antivirus software. According to Panda Security, the companies affected are unwilling to come forward with information about the attacks for fear of bringing public attention to their cybersecurity vulnerabilities.

Although the energy industry has not been a significant victim of reported cybersecurity attacks to date, the risk of a future attack is rising given the growing flow of information within the industry. Moreover, with the positional sensitivity of the industry, a cybersecurity attack or data breach within the energy sector could be devastating.

§ 28.02. Legal Framework.

[1] — Federal Law.

There is currently no federal cybersecurity legislation that generally applies to the energy industry. However, the President has issued several

executive orders, and Congress has proposed legislation. In addition, several agencies have issued guidance or regulations dealing with cybersecurity and related security issues. Given the national implications of significant data breaches or cybersecurity attacks, many believe that federal legislation is inevitable and necessary to ensure national compliance and risk protection.

[a] — Executive Orders.

President Obama has issued three Executive Orders related to cybersecurity issues over the past few years. Most recently, on April 1, 2015, President Obama issued an Executive Order providing for the imposition of sanctions against those responsible for, complicit in, or engaged in (directly or indirectly), significant cyberattacks by foreign individuals.[1] The sanctions block the transfer of property or interests located in the United States to any such party. In order to qualify for sanctions under the order, the cyberattack must pose a significant threat to national security, foreign policy, financial stability, or economic health.[2] This Executive Order provides that the knowing use of trade secrets from cyberattacks or cyberespionage may be sanctionable as well.[3]

In addition, President Obama issued two Executive Orders promoting information-sharing practices. The first Executive Order, issued February 12, 2013, announced the policy of promoting increased information sharing.[4] In addition, the 2013 Executive Order called for the creation of a framework for entities to use when evaluating cybersecurity issues and protecting critical infrastructure. This would lead to the NIST framework.[5] The second Executive Order, announced on February 13, 2015, called for the promotion of information sharing and analysis organizations (ISAOs).[6] In addition, the Order provided that the Secretary of Homeland Security should contract with

---

1 Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (April 1, 2015).
2 *Id*.
3 *Id*.
4 Exec. Order 13,636, 78 Fed. Reg. 11,737 (Feb. 12, 2013).
5 *Id*.
6 Exec. Order No. 13,691, 80 Fed. Reg. 9,347 (Feb 13, 2015).

an outside ISAO standards organization, which will establish guidelines and standards for ISAOs.[7]

[b] — Proposed Legislation.

Along with the current regulations and guidance, there have been some notable federal bills proposed on cybersecurity issues. Although these bills have not been enacted yet, they provide a sense of how Congress will likely approach these issues in the future.

For instance, the *Cybersecurity Information Sharing Act* was introduced in the Senate in March of 2015.[8] The bill would combat cybersecurity breaches through enhanced information sharing of data breach events.[9] The bill also provides liability protection for those complying with the Act.[10] This element is missing from many current information-sharing requirements. The Senate recently passed this bill, but it has not yet been passed by the House or signed into law.

In addition, the *Data Accountability and Trust Act* was proposed in the House of Representatives.[11] The Data Accountability and Trust Act would require the Federal Trade Commission to promulgate regulations governing data protection.[12] The act would require each person engaged in interstate commerce that owns or possesses data containing personal information to establish specified security policies and procedures to treat and protect such information.[13]

[2] — Energy-Specific Statutes, Regulations, or Standards.

While global cybersecurity legislation (at least on the federal level) has not been passed to date, these issues have been addressed by a number of federal agencies through regulations or standards. With regard to the energy

---

7 *Id*.
8 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).
9 *Id*. at §§ 3, 5.
10 *Id*. at § 6.
11 Data Accountability and Trust Act, H.R. 580, 114 Cong. (2015).
12 *Id*. at § 2.
13 *Id*. at § 3.

industry in particular, several agencies have issued regulations and standards related to cybersecurity and data breach issues.

[a] — Federal Energy Regulatory Commission (FERC).

As directed by FERC, the North American Electric Reliability Corporation (NERC) promulgated standards related to cybersecurity. The NERC 1300 Standards are cybersecurity standards for energy-related industries.[14] These standards address cybersecurity issues for bulk electric systems.[15] The NERC standards were approved by FERC.[16] The NERC standards deal with a range of topics, including asset identification and ranking, electronic security management, employee training, incident reporting and mitigation/cyber attack recovery.[17]

[b] — Nuclear Regulatory Commission (NRC).

The NRC promulgated standards to address cybersecurity concerns related to nuclear power plants.[18] The NRC's regulations require nuclear power plant licensees to develop and submit a cybersecurity protection plan that will minimize cybersecurity risks and mitigate damage from data breaches.[19]

[c] — Department of Homeland Security (DHS).

DHS promulgated the Chemical Facility Anti-Terrorism Standards (CFATS). First, DHS promulgated an interim final rule, which is currently in place until a final rule is published.[20] A proposed rule was published by DHS, and is currently pending review by the agency.[21] Under the CFATS rules, covered facilities include many in the energy sector and utilities. The

---

14 *See* Critical Infrastructure Protection (CIP) 002-5 to CIP-011-1.
15 *Id*.
16 *See* 78 Fed. Reg. 72756 (Dec. 3, 2013).
17 *See* Critical Infrastructure Protection (CIP) 002-5 to CIP-011-1.
18 10 C.F.R. § 73.54.
19 *Id*.
20 6 C.F.R. Part 27.
21 79 Fed. Reg. 48693 (Aug. 18, 2014).

CFATS rules establish risk-based performance standards related to various aspects of a facility's security posture.[22] These include cybersecurity and other potential risks.

[d] — Department of Energy (DOE).

DOE has developed cybersecurity guidance for both the electricity and oil and gas industries. With regard to the electricity in particular, DOE published the Electricity Subsector – Cybersecurity Capability Maturity Model.[23] This guidance addresses the implementation and management of cybersecurity practices associated with information technology and operational technology specifically within the electricity industry. The guidelines help organizations evaluate their cybersecurity capabilities, communicate their capability levels, prioritize cybersecurity issues, and strengthen cybersecurity capabilities. With regard to the oil and gas industry, DOE published the Oil and Natural Gas Subsector – Cybersecurity Capability Maturity Model.[24] These guidelines are similar to those issued for the electricity subsector. The ONG-C2M2 addresses the implementation and management of cybersecurity practices associated with information technology and operational technology specifically within the oil and gas industry.

[3] — State Law.

While federal legal requirements have been slow to gain acceptance, the opposite is true on a state by state basis. Based on a survey of the National Conference of State Legislatures, 47 states have security breach notification laws and 32 states have data disposal laws.[25]

---

22 *See id.*; *see also* 6 C.F.R. Part 27.

23 *See* Department of Energy, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1 (Feb. 2014).

24 *See* Department of Energy, Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1 (Feb. 2014)

25 National Conference of State Legislatures, Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Oct. 29, 2015); National Conference of State Legislatures, Data Disposal Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx (last visited Oct. 29, 2015).

[a] — Security Breach Laws.

At least 47 states have data notification laws.[26] Typical laws provide that an individual or entity that owns data including the personal information of state residents must notify those residents when a breach of personal information occurs. Laws typically only require notification of (a) the state's residents and (b) some consumer groups if a certain threshold number of residents (usually 1,000 to 10,000) are notified.

Many laws include a provision for instances where a third party is acting as custodian for the data on behalf of an individual or entity that owns the data. In those instances, the custodian is obligated to inform the owner of the date, and the owner would still have the obligation to notify state residents. Laws differ with regard to how soon notification should take place, with some laws providing a deadline, and others relying on a general statement such as "as soon as reasonably practicable." Laws also differ with regard to acceptable types of notice. These can include notice by mail, electronic mail, telephone, or public posting.

Many laws contain a provision that failure to comply with breach notification laws may result in a civil penalty and that the state attorney general may pursue a cause of action. Most, if not all, laws do not create a private cause of action.

[b] — Data Disposal Laws.

At least 32 states have passed data disposal laws.[27] Typical laws provide that businesses should have procedures for the protection and retention of personal information from customers and individuals. When these records are no longer of use to the business, the business should properly destroy the individuals/customers' personal information. Generally, data disposal laws provide that records should be destroyed by shredding, erasing, or otherwise

---

26 Some examples in key energy producing states include: Pennsylvania, 73 P.S. § 2301 *et seq.*; Ohio Rev. Code § 1349.19; West Virginia, W. Va. Code § 46A-2A-103; Texas, Tex. Bus. & Com. Code § 521.053.

27 Examples include New Jersey, N.J. Rev. Stat. § 56:8-162; Florida, Fla. Stat. § 501.171; Texas, Tex. Bus. & Com. Code § 521.053.

making records indecipherable. Similar to the security breach notification laws, many data disposal laws provide a cause of action that may be enforced by a state attorney general.

[4] — Industry Standards.

As a general matter, cybersecurity issues are largely governed by a series of standards that do not have the force of law but are widely used and instructive. Given the prominence of these industry standards, energy industry companies should be aware of these standards for several reasons. First, these standards will likely inform the scope and substance of future lawmaking and regulatory efforts in this area. Moreover, for liability purposes, it is possible that courts will look to compliance with industry standards to determine whether a company took adequate steps to protect against the risk of a data breach. Lastly, on a more basic level, compliance with these standards can help protect energy companies from cybersecurity and data breach risks.

[a] — National Institute of Standards and Technology (NIST).

NIST published the Framework for Improving Critical Infrastructure Cybersecurity.[28] NIST's publication provides a framework for companies to understand and address cybersecurity risks. Using this framework, companies can improve their cybersecurity and infrastructure through the framework's principles and best practices for risk management.[29] The NIST standards identify five key steps to cybersecurity protection: Identify; Protect; Detect; Respond; and Recover.[30]

[b] — Department of Justice (DOJ) Guidance.

On April 30, 2015, DOJ released cybersecurity guidance.[31] The guidance provides a general framework for developing and implementing

---

28 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014).

29 *Id*. at 1.

30 *Id*. at 7.

31 Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents, Version 1.0 (April 30, 2015).

a cybersecurity policy. Although DOJ notes that the guidance is targeted at smaller businesses, it can be used by any business to help guide the creation of a cybersecurity policy.[32]

[c] — American Petroleum Institute (API).

The API has several guidance documents that set forth standards for the petroleum industry, including its general security guidance, pipeline cybersecurity guidelines, and SCADA guidance. In the API's Security Guidelines for the Petroleum Industry,[33] the API adopts the ISO/IEC International Standard 17799, *Information Technology – Code of Practice for Information Security Management*.[34] Moreover, the API recommends an Eight-Step Standard for Information Security Process. This includes the following steps:[35]

- Create an Information Security Policy
- Select and Implement Appropriate Controls
- Obtain Upper-Management Support
- Perform Security Vulnerability Assessments ("SVAs")
- Create Statements of Applicability for Employees
- Create an Information Security Management System
- Educate and Train Staff
- Perform Regular Audits

In addition, the API published API 1164 on pipeline cybersecurity.[36] The primary objective of this guidance is to allow pipeline operators to control their lines in a way in which there are no adverse effects on employees, the environment, the public or customers as a result of any actions of the operator or other parties. API's standard on pipeline cybersecurity developed guidelines related to supervisory control and data acquisition (SCADA) as

---

32 *Id*. at 1.

33 American Petroleum Industry, Security Guidelines for the Petroleum Industry, 3rd Ed. (April 2005).

34 *See id*. at 31.

35 *Id*.

36 American Petroleum Institute Standard 1164, 2nd Ed. (June 1, 2009).

the means of remote monitoring and operation of pipeline equipment. This process is used by a variety of pipeline operators. The API recommends improving SCADA security and operations by: (a) analyzing vulnerabilities of the SCADA system that can be exploited by unauthorized entities; (b) listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks; (c) providing a comprehensive list of practices to harden the core architecture; and (d) providing examples of industry best practices.[37]

[d] — Information Sharing and Analysis Centers (ISACs).

Finally, ISACs are industry groups designed for industry-specific sharing of cybersecurity information. There are currently four energy-related ISACs. These include the Oil and Natural Gas ISAC, the Downstream Natural Gas ISAC, the Electric Services ISAC, and the Nuclear Energy Institute (NEI).

§ 28.03. Civil Litigation Resulting from Cyber Attacks.

Plaintiffs have attempted to state a variety of claims as a result of cyber attacks and data breaches. The government has also brought civil enforcement actions against companies for inadequate cybersecurity protection. Some of the potential civil causes of action are discussed below.

[1] — Civil Enforcement Actions by Government Agencies for Inadequate Cybersecurity.

Since 2002, the Federal Trade Commission (FTC) has used its authority under the FTC Act to pursue a number of actions against companies for data-security failures.[38] The FTC Act empowers the FTC to prevent companies (including oil and gas and energy companies) "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or

---

37 *Id*.

38 *See* FTC Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249.

practices in or affecting commerce."[39] The FTC may levy civil penalties and bring civil actions to enjoin violations of the FTC Act.[40] Pursuant to section 45(n) of the FTC Act, the FTC may declare an act or practice unfair and unlawful if it: "[1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] [which is] not outweighed by countervailing benefits to consumers or to competition."[41] Deceptive acts or practices include misrepresentations or deceptive omissions of material fact.

At least one court has allowed an FTC civil complaint based on data breaches to survive a motion to dismiss. In *FTC v. Wyndham Worldwide Corp.*,[42] the U.S. District Court for the District of New Jersey held that the FTC stated a claim against Wyndham hotel-chain entities (collectively, "Wyndham") under the FTC Act where the complaint alleged that Wyndham failed to provide reasonable and appropriate security for guests' personal information stored in the computer system and, therefore, exposed the data to theft. The system suffered three data breaches in less than two years, resulting in over $10.6 million worth of fraudulent charges on guests' accounts. The court rejected Wyndham's argument that the FTC lacks authority to file a cybersecurity-based action under the FTC Act, holding that the FTC stated a claim and denying the motion to dismiss. The court held that the FTC adequately pleaded both an unfairness claim and a deception claim based on the data breaches.

In support of the unfairness claim in *Wyndham*, the FTC complaint alleged that Wyndham (a) failed to use readily available security measures, such as firewalls; (b) stored payment card information in clear readable text; (c) failed to implement adequate policies and procedures before connecting local computer networks to the main network; (d) failed to remedy known

---

39 15 U.S.C. § 45(a)(2); FTC v. Atlantex Assocs., No. 87-0045, 1987 WL 20384, at *11 (S.D. Fla. Nov. 25, 1987), *aff'd*, 872 F.2d 966 (11th Cir. 1989) (holding that oil and gas companies violated § 45(a) and ordering restitution).

40 *See* §§ 45(l)-(m), 58(b).

41 § 45(n).

42 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).

security vulnerabilities, putting personal information at risk; (e) allowed connection of insecure servers to the main network, including servers using outdated operating systems that could not receive security updates; (f) allowed servers to connect to the main network, although the default user IDs and passwords were enabled on the servers and easily available to hackers; (g) failed to employ commonly used methods to require complex user IDs and passwords; (h) failed to adequately inventory computers connected to the main network to properly manage devices on its network; (i) failed to employ reasonable measures to detect and prevent unauthorized access to the network or to conduct security investigations; (j) failed to follow proper incident response procedures, including failing to monitor for malware used in a previous intrusion; and (k) failed to adequately restrict third-party vendors' access to the network and property management systems.

The FTC's deception claim relied on certain representations in Wyndham's privacy policies available online, including that the Wyndham entities: "recognize the importance of protecting the privacy of individual-specific (personally identifiable) information"; "safeguard . . . personally identifiable information by using industry standard practices"; "make commercially reasonable efforts" to comply "with all applicable laws and regulations"; "utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users"; "take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards."

Wyndham appealed to the Third Circuit, but the Third Circuit affirmed the district court's decision to deny Wyndham's motion to dismiss.[43] The Third Circuit addressed only the unfairness claim; specifically whether the FTC has authority to regulate cybersecurity under section 45(n) of the FTC

---

43 FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015). Similar challenges to FTC's data-security authority were dismissed in another case because FTC lodged the complaint internally, not in a federal district court. LabMD, Inc. v. FTC, 776 F.3d 1275, 1279-80 (11th Cir. 2015) (dismissing laboratory's challenge to FTC complaint, alleging data-security practices failed to prevent unauthorized access to patient information, for lack of subject-matter jurisdiction because FTC proceeding was ongoing).

Act and, if so, whether Wyndham was denied due process for lack of fair notice that its practices might violate the unfairness standard in section 45(n).

The court first rejected all of Wyndham's arguments that its alleged conduct was not "unfair" under the FTC Act.[44] Wyndham argued that the three requirements of section 45(n) (see above) are not the only prerequisites to an unfairness claim, but rather the plain meaning of "unfair" requires additional indicia of wrongdoing. The court rejected Wyndham's various arguments and affirmed that the FTC adequately pleaded an unfairness claim. In doing so, the court relied on the FTC's allegations that "Wyndham had published a misleading privacy policy that overstated its cybersecurity" and explained that such alleged facts pertain to both the deception claim and the unfairness claim.[45] Wyndham argued that unfairness requires some sort of inequity or injustice. In response, the court explained that the alleged conduct fits that meaning because "[a] company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[46] In the court's view, such conduct would meet the plain meaning of "unfair" advocated by Wyndham. The court also rejected Wyndham's argument that recent statutes and legislation precluded the FTC's regulation of cybersecurity under the FTC Act.

The court also held that Wyndham received fair notice of the requirements of section 45(n), and was not deprived of due process, based on the court's interpretation of the FTC Act.[47] Because the FTC had not yet issued a formal interpretation concerning whether cybersecurity practices may be "unfair" under the FTC Act, the court viewed its role as interpreting "the meaning of the statute in the first instance," without any sort of deference to the agency. Instead, the court framed the issue as follows: "The relevant question is not

---

44 *Wyndham*, 799 F.3d at 244-49.
45 *Id*. at 245-46.
46 *Id*.
47 *Id*. at 249-59.

whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires."[48]

The court explained that Wyndham did not challenge whether the FTC Act itself fails to provide fair notice, but instead only challenged the standard as applied to the facts in this case. Based on the allegations of fact in the complaint that Wyndham was hacked three times and that it wholly failed to implement certain cybersecurity measures, the court held that Wyndham was on notice that its conduct would not meet the statutory standard in section 45(n). The court also noted that the FTC issued a guidebook on sound cybersecurity practices and had filed complaints and settled administrative cases related to inadequate cybersecurity, with notice provided on its website and in the Federal Register. Wyndham did not argue that it was unaware of the statute or the FTC's prior actions, but argued that it did not specifically know what the law required or which cybersecurity failures triggered the violations. Based on the standard of review, however, the court concluded that Wyndham was not "entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a)."[49]

Based on *Wyndham* and other cases, companies may be civilly liable for failure to implement adequate cybersecurity measures,[50] but may not yet fully understand the types of cybersecurity measures that must be implemented to avoid liability. The Third Circuit recognized in *Wyndham* that the standard of liability might be unclear, at least until the FTC issues further guidance:

> We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Fair notice is satisfied here as long as the company can reasonably foresee that a

---

48 *Id*. at 253-54.

49 *Id*. at 259.

50 *Cf*. Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 213 (1st Cir. 2012) (bank's failure to implement additional cybersecurity measures was commercially unreasonable under UCC provision applicable to financial institutions in light of the bank's knowledge of recent fraud incidents).

court could construe its conduct as falling within the meaning of the statute.[51]

Until the FTC issues additional guidance on the issue, which might limit the scope of its enforcement actions, the prior FTC complaints available on its website will serve as guidance for courts and the regulated industry concerning the types of cybersecurity deficiencies that might result in liability. For example, the Third Circuit in *Wyndham* used a 2006 FTC complaint for purposes of comparison, noting that it contained "close corollaries" to the allegations against Wyndham.[52]

In addition to potential federal enforcement, it is important to remain aware of developments at the state level. Some states have statutes that provide for enforcement by state attorneys general or government agencies.[53]

[2] — Claims Against Entities that Experienced a Data Breach.

Plaintiffs have attempted to state different types of claims against companies that experienced a data breach, leaving the plaintiffs' information vulnerable to disclosure. Some types of claims are discussed below.

[a] — Negligence for Failure to Protect Data.

Plaintiffs have successfully stated negligence claims based on companies' alleged breaches of their duties to protect data from hackers.[54] A key issue for negligence claims based on cyber attacks is whether the harm to the

---

51 *Wyndham*, 799 F.3d at 255-56 (internal citation omitted).

52 *Id*. at 258.

53 *See In re* Target Corp. Data Sec. Breach Litig., No. 14-2522, 2014 WL 7192478, at *11-14 (D. Minn. Dec. 18, 2014) (explaining that some states' data-breach notification statutes allow attorneys general or government officials to enforce them).

54 *See, e.g.*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 162 (1st Cir. 2011) (plaintiffs adequately alleged negligence claim against grocery chain based on hackers' breach of electronic payment system and theft of credit and debit card information); Lone Star Nat'l Bank, N.A. v. Heartland Payment Systems, Inc., 729 F.3d 421, 423 (5th Cir. 2013) (banks successfully stated negligence claims against credit-card processor for hackers' breach of credit card processor's data systems).

plaintiffs is foreseeable, or whether the criminal activities of the third-party hackers is an unforeseeable superseding cause of the harm.[55]

[b] — Breach of Contract (Express or Implied) for Failure to Protect Data.

A company's contracts may require it to protect other persons' data, which can give rise to a breach of contract action for a data breach. Whether or not an express contract exists between a company and persons whose data is compromised as a result of a data breach, the persons may state breach-of-contract claims based on the relationship between the parties.[56]

[c] — Failure to Comply with State Statutes Related to Computers and Electronic Data.

Several states have data-breach notification laws and other statutes regulating computer-based conduct that may authorize private civil actions for lack of notice, untimely notice, or other noncompliance related to a data breach. Some state statutes do not authorize private civil enforcement or are unclear on the subject.[57]

---

55 *See, e.g.*, *In re* Target Corp. Data Sec. Breach Litig., No. 14-2522, 2014 WL 6775314, at *3 (D. Minn. Dec. 2, 2014) ("Although the third-party hackers' activities caused harm, Target played a key role in allowing the harm to occur. Indeed, Plaintiffs' allegation that Target purposely disabled one of the security features that would have prevented the harm is itself sufficient to plead a direct negligence case.").

56 *See, e.g.*, *Anderson*, 659 F.3d 151, 159 (1st Cir. 2011) (class-action plaintiffs stated a claim for breach of an implied contract because a jury could reasonably conclude that the grocery chain implicitly agreed to safeguard its customers' data); *In re Target Corp. Data Sec. Breach Litig.*, No. 14-2522, 2014 WL 7192478, at *20-21 (D. Minn. Dec. 18, 2014) (holding that putative class-action plaintiffs adequately alleged breach of implied contracts, but failed to allege breach of Target's REDcard debit-card agreement provision requiring Target to "use security measures that comply with federal law").

57 *See In re Target Corp. Data Sec. Breach Litig.*, No. 14-2522, 2014 WL 7192478, at *9-14 (D. Minn. Dec. 18, 2014) (analyzing various state data-breach statutes and concluding that plaintiffs did not state a claim under the following state's statutes: Florida, Oklahoma, Utah, Arkansas, Connecticut, Idaho, Massachusetts, Minnesota, Nebraska, Nevada, Texas and Rhode Island).

[d] — Other Types of Claims Related to Data Breaches.

Other types of claims that have been asserted based on data breaches include, for example: breach of fiduciary duty/confidential relationship,[58] violation of state unfair trade practices/consumer protection statutes,[59] and privacy infringement.[60]

[3] — Shareholder Derivative and Securities Claims Resulting from Data Breaches.

Officers and directors of a company that suffers a data breach may face derivative and securities claims by shareholders of the company. In *In re Heartland*, shareholders brought a derivative action against officers and directors of Heartland for securities fraud under the Private Securities Litigation Reform Act of 1995 (PSLRA)[61] after hackers accessed internal corporate information that was confidential, including employees' names, addresses, and social security numbers.[62] The hackers also stole 130 million credit and debit card numbers.

---

58 *See, e.g., Anderson*, 659 F.3d 151, 157-58 (1st Cir. 2011) (plaintiffs failed to allege breach of fiduciary duty, in part because they alleged no facts establishing the "trust and confidence" element required by Maine confidential-relationship cases).

59 *See, e.g., In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966-73 (S.D. Cal. 2014) (plaintiffs alleged claims under various California consumer protection statutes).

60 *See, e.g., In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 21, 29 (D.D.C. 2014) (plaintiffs alleged that data breach resulting from theft of tapes violated their expectation of privacy under statutes, state tort law, and possibly contract, but court dismissed for lack of standing claims of plaintiffs who failed to allege their data was accessed). For further examples of claims that might be alleged in a data-breach case, see generally *In re Sony Gaming Networks*, 996 F. Supp. 2d 942, 959 (S.D. Cal. 2014) ("The fifty-one claims alleged in the [complaint] can be categorized into nine sub-groups: (1) negligence; (2) negligent misrepresentation; (3) breach of express warranty; (4) breach of implied warranty; (5) unjust enrichment; (6) violation of state consumer protection statutes; (7) violation of the California Database Breach Act; (8) violation of the federal Fair Credit Reporting Act; and (9) partial performance/breach of the covenant of good faith and fair dealing.").

61 15 U.S.C. § 78u-4(b)

62 *In re* Heartland Payment Sys., Inc. Sec. Litig., No. CIV. 09-1043, 2009 WL 4798148, at *1 (D.N.J. Dec. 7, 2009).

After Heartland disclosed the data breach, its stock price dropped by almost $10 per share in less than a month. The shareholders claimed that Heartland's officers concealed the cyber attack during a conference call and made misrepresentations about the adequacy of its computer network security in statements made by its officers and in its SEC filings, which amounted to fraud because the officers "were aware that Heartland had poor data security and had not remedied the problem." The court held that the plaintiffs failed to state a claim under the heightened pleading standards for fraud under the PSLRA because the statements made by the officers were not fraudulent and the statements in the SEC filings were not false or misleading.

Shareholders have also alleged that officers' and directors' failure to protect data from hackers is a breach of their fiduciary duty, a waste of corporate assets, an abuse of control, and gross mismanagement.[63] Shareholders may also attempt to force a company's directors to bring a lawsuit on behalf of the company in response to a data breach.[64]

[4] — Claims by Hacked Entities Against Hackers (Assuming They Are Identified).

[a] — Computer Fraud and Abuse Act.

The Computer Fraud and Abuse Act (CFAA)[65] is the primary federal criminal statute that penalizes hacking. It prohibits unauthorized access of "protected computers" (*i.e.*, certain computers of financial or government

---

63 *See, e.g.*, La. Mun. Police Employees' Retirement Sys. v. Alvarez, No. 5620, 2010 WL 3780308 (Del. Ch. Sept. 27, 2010) (approving settlement of derivative action for breach of fiduciary duty against directors for data breach involving company that operates Marshall's, T.J. Maxx, and other retail stores); Complaint, Kulla v. Steinhafel, No. 14-cv-00203 (D. Minn. Jan. 21, 2014) (alleging breach of fiduciary duty and waste of corporate assets against Target's officers and directors); Complaint, Collier v. Steinhafel, No. 14-cv-00266 (D. Minn. Jan. 29, 2014) (alleging breach of fiduciary duty, gross mismanagement, waste of corporate assets, and abuse of control against Target's officers and directors).

64 *See, e.g.*, Palkon v. Holmes, No. 2:14-CV-01234, 2014 WL 5341880, at *3-6 (D.N.J. Oct. 20, 2014) (relying on the business judgment rule to grant motion to dismiss Wyndham shareholder's suit for Wyndham's refusal to follow his demand to bring a lawsuit based on data breaches).

65 18 U.S.C. § 1030.

institutions or computers connected to interstate commerce).[66] Any computer connected to the Internet is protected because such a connection means it is used in interstate commerce. The CFAA authorizes a civil action where the defendant:

- Knowingly, with the intent to defraud
- Accesses a protected computer
- Without authorization or exceeds authorized access
- Furthers the intended fraud; and
- Obtains anything of value.[67]

An action may be brought where the defendant "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[68] A plaintiff may receive compensatory damages and injunctive or other equitable relief.[69] Damages are limited to economic damages of at least $5,000 during any one-year period, or other damages related to medical care, physical injury, a threat to public health or safety, or affecting government computers.[70] The CFAA expressly excludes any cause of action "for the negligent design or manufacture of computer hardware, computer software, or firmware."[71]

Companies have used the CFAA to pursue civil actions against employees and third-parties, alleging that they were not authorized to access their data. In *Dresser-Rand Co. v. Jones*,[72] a corporation that provides technology, products, and services to develop energy and natural resources filed a civil suit against former employees who took sensitive data on external devices upon leaving the company. The court granted summary judgment on the CFAA

---

66 § 1030(a)(4), (e)(2)(B).

67 § 1030(a)(4), (g).

68 § 1030(a)(2)(C).

69 § 1030(g).

70 *See* § 1030(g), (c)(4)(A)(i)(I)-(V); Advanced Fluid Systems, Inc. v. Huber, 28 F. Supp. 3d 306, 327 (M.D. Pa. 2014) (company failed to state a CFAA claim against former employee and his new employer because company failed to allege facts supporting damages of at least $5,000, such as impairment to data or computer system or costs incurred for restoration).

71 § 1030(g).

72 *See, e.g.*, Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 621 (E.D. Pa. 2013).

claim in favor of the employees because one employee had not accessed Dresser-Rand's computers and the others acted within their authorization to access the computers. A key issue under the CFAA is the definition of the term "authorization," but that definition will likely not be an issue where a hacker who never had any authority to access data steals information.[73]

[b] — Wiretap Act and Electronic Communications Privacy Act.

The Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA),[74] allows private civil actions for unauthorized interception of electronic communications, as well as use or disclosure of such communications in certain circumstances.[75] The remedies include equitable or declaratory relief, damages (including statutory and punitive damages), and attorneys' fees and costs.[76] There is no liability where the interceptor is a party to the communication or received consent to the interception, "unless such communication is intercepted for the purpose of committing any criminal or tortious act."[77] Certain entities, such as providers of electronic communication services, and their agents may be immune from claims under the Wiretap Act.[78]

---

73 *See id*. at 615-21 (noting a circuit split regarding the meaning of "authorization" and concluding that the company's policies did not govern access, but only use); Paradigm Alliance, Inc. v. Celeritas Technologies, LLC, 659 F. Supp. 2d 1167, 1190-92 (D. Kan. 2009) (producer of GIS for pipeline safety demonstrated genuine issue of fact regarding whether IT companies' unsuccessful attempts to log on to website with another user's ID and password was violation of CFAA).

74 18 U.S.C. §§ 2510 *et seq*.

75 18 U.S.C. §§ 2511(1)(a), 2520(a).

76 § 2520(b).

77 § 2511(2)(d).

78 *See, e.g.*, *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382, 2013 WL 6248499, at *10 & n.86 (N.D. Cal. Dec. 3, 2013) ("[A]s a provider of electronic communication services, Google is immune from claims alleging interception by a 'device' based on equipment used 'by a provider of wire and electronic communication service in the ordinary course of business.'").

[c] — Stored Communications Act.

The Stored Communications Act (SCA)[79] authorizes private civil actions against any person who engages in the following activities:

- Intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- Intentionally exceeds an authorization to access that facility; and
- Thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.[80]

Certain persons are exempt from this prohibition, including those providing a wire or electronic communications service and users of the service that made or are the intended recipients of the communication.[81] But the SCA also forbids certain conduct that may give rise to a civil action against providers of electronic communication services or remote computing services.[82]

Civil actions under the SCA are authorized only for violations committed with a knowing or intentional state of mind.[83] The SCA provides exclusive remedies (except when there are constitutional violations), including equitable and declaratory relief, damages, attorneys' fees and costs, punitive damages, and profits made by the violator from the violation.[84]

[d] — Trade Secret Protection Laws.

Depending on the sensitive nature of the information that is subject to a data breach, companies may bring claims under state laws for misappropriation of trade secrets.[85]

---

79 18 U.S.C. §§ 2701 *et seq.*

80 18 U.S.C. §§ 2701(a), 2707.

81 § 2701(c).

82 *See* § 2702(a).

83 § 2707(a).

84 §§ 2707(b)-(c), 2708.

85 *See, e.g.*, *Advanced Fluid Systems, Inc.*, 28 F. Supp. 3d 306, 314-23 (M.D. Pa. 2014) (holding that a designer of hydraulic machine systems stated a claim for misappropriation

[e] — Other Types of Claims Against Hackers.

Plaintiffs may assert a variety of other types of claims, including, for example, breach of copyright and trademark protection laws,[86] violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act,[87] and state-specific statutory and common-law claims.

[5] — Claims by Hacked Entities Against Cybersecurity Vendors.

[a] — Negligence for Failure to Protect Data.

Companies have stated claims against cybersecurity providers for ordinary or gross negligence for alleged breaches of their duties to protect data from hackers.[88]

[b] — Breach of Contract for Failure to Protect Data.

Companies have stated breach-of-contract claims against cybersecurity providers based on the terms and representations in the contracts governing the parties' relationship.[89]

---

of trade secrets under Pennsylvania law where it alleged that a former employee saved the confidential information to an external hard drive and transmitted it to the employee's new employer).

86 *See, e.g.*, SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593, 610-13 (E.D. Va. 2005) (holding that cybersecurity company stated a civil claim for copyright infringement against competitors for using confidential information regarding software).

87 *See, e.g.*, *SecureInfo Corp.*, 387 F. Supp. 2d 593, 613-15 (E.D. Va. 2005) (holding that cybersecurity company failed to allege a "pattern of racketeering activity" pursuant to 18 U.S.C. § 1962(c) to state a civil claim under RICO against consultant and competitor employees for sharing and using confidential information).

88 *See, e.g.*, Baidu, Inc. v. Register.com, Inc., 760 F. Supp. 2d 312, 320 (S.D.N.Y. 2010) (claim for gross negligence based on security provider's failure to follow own protocols survived motion to dismiss, despite contractual limits on liability); *see also* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 881 (N.D. Ill. 2014) (plaintiff lacked standing to bring negligence claim against cybersecurity company that provided products and services to South Carolina Department of Revenue, which suffered a cyber attack).

89 *See, e.g.*, *Baidu, Inc.*, 760 F. Supp. 2d 312, 320 (S.D.N.Y. 2010) (claim for breach of contract based on cybersecurity provider's failure to follow own protocols survived motion to dismiss, but required showing of gross negligence due to contractual limits on liability).

[c] — Other Types of Claims for Failures of Cybersecurity Vendors.

Other types of claims that might be raised depending on the factual circumstances include negligent or intentional misrepresentation,[90] products liability for defective security software,[91] and state-specific statutory and common-law claims.

[6] — Barriers to Claims and Limits on Liability Related to Data Breaches.

There may be barriers to claims raised as a result of data breaches, including, most notably, Article III standing.

[a] — Standing for Asserting Claims Based on Data Breaches.

Article III standing remains a significant hurdle for plaintiffs who bring an action against a company for failure to protect their data from hackers. Many courts have held that plaintiffs' allegations of an increased risk of harm from a data breach is not alone sufficient to meet standing requirements because the mere disclosure of information, without misuse (*e.g.*, unauthorized purchases using credit card information), is not an injury in fact.[92] These

---

90 *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 974-75 (S.D. Cal. 2014) (dismissing misrepresentation claims for failure to allege pecuniary loss).

91 *But see* 18 U.S.C. § 1030(g) (CFAA exclusion for causes of action "for the negligent design or manufacture of computer hardware, computer software, or firmware.").

92 *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42-46 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012); Peters v. St. Joseph Servs. Corp., No. 4:14-CV-2872, 2015 WL 589561, at *4-5 & n.10 (S.D. Tex. Feb. 11, 2015) (rejecting that increased risk of future identity theft or fraud constitutes "imminent" injury, and noting that Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) "[a]rguably . . . has resolved the circuit split" on the issue); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014) (relying on *Clapper* to conclude that "the increased risk that Plaintiffs will be victims of identity theft, identity fraud, medical fraud, or phishing at some indeterminate point in the future does not constitute injury sufficient to confer standing where, as here, the occurrence of such future injury rests on the criminal actions of independent decisionmakers and where, as here, the Complaint lacks sufficient factual allegations to show such future injury is imminent or certainly impending"); Green v. eBay Inc., No. CIV.A. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) ("[T]he

courts typically hold that alleged costs incurred by plaintiffs for mitigation or prophylactic measures, such as for monitoring financial information for unauthorized activity, are insufficient to establish an actual or imminent injury as a result of a data breach.[93] Some courts have held that plaintiffs who fail to allege unreimbursed financial costs lack standing, although their data was misused to generate fraudulent charges.[94] In contrast, other courts, particularly within the Ninth Circuit, have held that an increased risk of harm from a data breach is sufficient to meet Article III standing requirements, even in light of recent Supreme Court authority that suggests otherwise.[95]

[b] — Absence of Cognizable Injury from Data Breaches.

Under state negligence and contract law, damages must generally be reasonably foreseeable for courts to allow recovery. This requirement is similar to the injury requirement for Article III standing.[96] Some courts

---

potential threat of identity theft or identity fraud, to the extent any exists in this case, does not confer standing on Plaintiff to pursue this action in federal court.").

93 *Reilly*, 664 F.3d at 46; *Green*, 2015 WL 2066531, at *5.

94 *See, e.g.*, Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735, 2014 WL 4627893, at *3 (N.D. Ill. Sept. 16, 2014) ("Plaintiffs have not alleged that any of the fraudulent charges were unreimbursed. On these pleadings, I am not persuaded that unauthorized credit card charges for which none of the plaintiffs are financially responsible qualify as 'concrete' injuries."), *rev'd*, 794 F.3d 688, 693-96 (7th Cir. 2015) ("The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft . . . are sufficient to satisfy the first requirement of Article III standing.").

95 *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (applying *Clapper* and holding that "Plaintiffs' allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [are] sufficient to establish Article III standing at this stage in the proceedings"); *In re* Adobe Sys., Inc. Privacy Litig., No. 13-CV-05226, 2014 WL 4379916, at *8 (N.D. Cal. Sept. 4, 2014) (applying and distinguishing *Clapper* and disagreeing with *Galaria* because "the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real" and the intent of the hackers to use the data was clear).

96 *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 964-66 (S.D. Cal. 2014) (dismissing negligence claims based on untimely notice of data breach because, although plaintiffs had standing, they failed to allege injury from untimely notice).

have held that damages resulting from cyber attacks were foreseeable and, therefore, recoverable.[97]

Certain types of damages may be inherently speculative or relate only to future injuries, in which case courts may hold that they are not recoverable.[98] Actions under state data-breach statutes may require the unauthorized use of the information to result in *actual* damages. In *Ponder v. Pfizer, Inc.*,[99] a Pfizer employee filed a putative class action against the company, alleging that it failed to comply with Louisiana's Database Security Notification Law in response to a data breach disclosing employee information. The employee alleged that the notice letter was untimely, as nine weeks passed between the data breach and the notice. The court held that the plaintiffs failed to allege recoverable damages because there was no allegation that the information was actually used to the plaintiffs' detriment. The costs and burdens of credit monitoring, opening and closing accounts, and reviewing statements were too speculative to be recoverable.[100]

[c] — Contractual Limits on Claims Arising from Data Breaches.

Contracts may include indemnification provisions and/or limits on liability that will affect the types and extent of claims the parties may assert against each other. The "economic loss doctrine" generally requires plaintiffs to use contractual remedies to recover purely economic losses, and it may

---

97 *See, e.g.*, *Anderson*, 659 F.3d 151, 164-65 (1st Cir. 2011) (holding that it was foreseeable under Maine law that a customer whose credit or debit card information was stolen and expected fraudulent charges as a result of data breach would replace the card to mitigate against misuse, and that a customer who experienced unauthorized charges would purchase insurance to protect against data misuse).

98 *See* Holmes v. Countrywide Fin. Corp., No. 5:08-CV-00205, 2012 WL 2873892, at *10 (W.D. Ky. July 12, 2012) ("Since credit monitoring expenses are not compensable injuries under these circumstances, Plaintiffs have failed to state a claim in this regard.").

99 *See* Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793, 796-98 (M.D. La. 2007).

100 *Id.*; Pinero v. Jackson Hewitt Tax Serv. Inc., 594 F. Supp. 2d 710, 717 (E.D. La. 2009) ("[P]laintiff's damages are not based on an actual injury, but the speculative future injury of identity theft.").

bar negligence claims in some states depending on the circumstances.[101] Contract claims may also bar certain statutory claims as a matter of law.[102]

§ 28.04. Contracts that May Be Impacted By Data Breaches.

[1] — Contracts with Software Vendors.

There are a wide variety of software vendors available in the market. Their products range based on industry and purpose. For instance, some software is designed specifically for the oil and gas industry or utilities. Software can serve a variety of purposes, including billing, work-site management, and inventory tracking. While many of the relevant software vendors are not focused exclusively on the energy sector, there are a significant number of specific oil and gas, utility, or energy-related programs adapted and/or designed for specific industry purposes.

Although the terms of service and software contracts are subject to change and updating, there are a few typical provisions seen among contracts with regard to cybersecurity issues. For instance, many contracts provide general provisions limiting liability or indemnifying the software company for issues related to use of the software. With regard to cybersecurity in particular, some contracts note that users of their software accept the risks of using the software and that no software is perfectly secure. In addition, some terms of service/contracts have provisions related to the loss of data.

---

101 *See* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013) (holding that the economic loss doctrine under New Jersey law did not bar banks' negligence claims against credit-card processor for hackers' breach of credit card processor's data systems because banks' economic losses were foreseeable and limited to the banks); *In re Target Corp. Data Sec. Breach Litig.*, No. 14-2522, 2014 WL 7192478, at *15-20 (D. Minn. Dec. 18, 2014) (analyzing application of the economic loss doctrine in various states and concluding that it barred plaintiffs' negligence claims under Alaska, California, Illinois, Iowa, and Massachusetts law); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966-73 (S.D. Cal. 2014) (granting Sony's motion to dismiss negligence claims under California law based on the economic loss doctrine).

102 *See, e.g.*, Genesco, Inc. v. Visa U.S.A. Inc., No. 3:13CV202, 2013 WL 3790647, at *21 (M.D. Tenn. July 18, 2013) (explaining that breach-of-contract claim may preclude statutory claim under California Unfair Competition Law).

Overall, however, the terms of service/contracts related to many software products do not include specific cybersecurity provisions.

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

Companies may have contracts with various entities and oilfield service companies that may be affected by data breaches or touch on cybersecurity issues. These include master service agreements, drilling contracts, and similar common arrangements. Those contracts may not deal directly with cybersecurity beyond typical indemnity or risk-of-loss provisions.

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

Companies must consider provisions that might protect or harm their interests when drafting or entering into contracts. For example, when entering into contracts with cybersecurity vendors that are providing the important service, companies should consider:

- Does the contract address the cybersecurity vendor's failure to prevent a cyber attack or timely repair a data breach?[103]
- Does the contract make representations about products, protections, or services that may provide the basis for a cause of action against the cybersecurity vendor?
- Is there an indemnification clause?[104]
- Are there limits on liability?[105]

---

103 *See, e.g.*, INX, LLC v. Music Group Services U.S., Inc., No. C13-2126, 2014 WL 51142, at *2-4 (W.D. Wash. Jan. 7, 2014) (cybersecurity vendor demonstrated probable validity of breach of contract where company subject to cyber attack failed to pay for restoration services after cyber attack because it was not satisfied with vendor's services).

104 *See, e.g.*, Schnuck Markets, Inc. v. First Data Merchant Data Servs. Corp., No. 4:13-CV-2226, 2015 WL 224993, at *2, 8 (E.D. Mo. Jan. 15, 2015) (indemnification clause required grocery store that was target of cyber attack to indemnify transaction processing servicers for costs of fraud monitoring, card replacement, and fraud losses up to $500,000 as a result of data breach).

105 *See, e.g.*, *Baidu, Inc.*, 760 F. Supp. 2d 312, 320 (S.D.N.Y. 2010) ("While [company asserting claims against security provider for cyber attack] gave up, in agreeing to the Limitation of Liability clause, any claims for ordinary negligence or breach of contract based

When contracting with employees within the company, such as IT personnel, to protect sensitive data, it would be prudent to consider the responsibilities of those in-house IT personnel in their employment contracts, and how they compare to contracts with outside vendors.[106] When entering into contracts that relate to everyday business operations, the following matters are worth consideration:

- How will the parties proceed with business in the event of a data breach affecting operations (*e.g., force majeure*)?
- Who bears the risk of loss where sensitive data is compromised (*e.g.*, limits on liability, indemnification clause)?
- What are the company's contingency plans to meet demand/ contract terms?

§ 28.05. CyberSecurity Training/Planning/Remediation.

As a general matter, the lack of training, preparation, and awareness are major causes of data loss. Some studies have shown that four out of five losses caused by employee negligence. The loss of usernames/passwords and loss of hardware are major issues. Awareness and training are significant tools in combating cybersecurity risks. Companies in the energy industry should strive to have their own, individualized plan for cybersecurity training, planning, and remediation. However, the following general ideas highlight some of the major issues involved when conducting cybersecurity training or creating a data loss response plan.

---

on ordinary negligence, it did not waive its claims for gross negligence or recklessness."); *Schnuck Markets, Inc.*, No. 4:13-CV-2226, 2015 WL 224993, at *7 (E.D. Mo. Jan. 15, 2015) (omission of "data compromise losses" from limitation of liability clause evidenced parties' intent not to include data breaches in clause).

106 *See, e.g.*, Music Group Macao Commercial Offshore Limited v. Foote, No. 14-cv-03078, 2015 WL 2170121, at *3 (N.D. Cal. May 8, 2015) (addressing discovery dispute related to music company's claims against its own IT consultant for failure to prevent cyber attack, and concluding "that Defendant is entitled to discovery of the employment agreements of the relevant IT employees with the information protected by the constitutional right to privacy redacted" because "if Plaintiff specifically hired other individuals for the purposes of ensuring cyber security and preventing attacks, that could be relevant to show that Defendant was not negligent, that his acts did not cause the cyber attack, or both").

[1] — A Cybersecurity Plan.

A data loss or cyber attack will be a significant and costly event to any company. Although no plan is perfect, companies can take steps to help prevent a loss, and avoid these costs. Properly protecting your company will ensure that cyber-thieves do not view your organization as a "low-hanging" fruit. In addition, when a loss of data or cyber intrusion occurs, a fast response is critical. Having a plan in place allows for a fast and coordinated response.

[2] — Before Creating a Cybersecurity Plan.

Companies should identify critical data that must be protected/would be valuable to others. The focus should also be on the company's weak points with regard to critical data, and the reasons why it should be protected. In addition, companies should consider how the data is kept throughout its lifecycle, which includes: collection; usage; short-term and long-term storage; and destruction.

[3] — Creating a Cybersecurity Plan.

A plan should have specific step-by-step procedures for dealing with data loss or cyber attack event. A plan should account for state-specific response provisions for critical states related to the business. Companies should strive to develop standards to the strictest applicable laws to ensure compliance. In addition, it is important to set-up data collection/back-up practices early. This may include monitoring your own network, which can require consent. Furthermore, companies should back-up data and critical files in an additional secure location.

There are several legal issues to consider as well. Companies should ensure that in-house counsel and outside legal counsel are familiar with cybersecurity issues, and specifically with the cybersecurity issues related to your industry. The involvement of an attorney at an early stage is critical because of potential liability issues and shifting legal requirements. It is also important that counsel have necessary contacts with forensic teams.

Companies should work to build necessary relationships before a data loss or cyber attack occurs. Consider getting to know applicable regulators and law enforcement before a breach occurs. It is also important to determine

which crisis response vendors to choose before an attack happens to avoid making the decision on the fly.

[4] — Training.

An important step after adopting a cybersecurity plan is to conduct employee training. Training should include initial training along with periodic refreshers to ensure preparedness. Testing should be completed to verify the company's readiness for a data loss or cyber attack.

[5] — Model Plan (Adapted from DOJ Guidance).

As one example, the Department of Justice's recent cybersecurity guidance sets forth a model cybersecurity plan that companies can adapt for the specific needs within their business and industry.[107] This guidance lays out the following steps for responding to a cybersecurity attack or data breach.

Step 1 — Assess and understand the breach or threat. Is it an intentional attack or computer error? What is the scope of the problem?[108]

Step 2 — Minimize damage from the data loss or cyber attack.[109]

Step 3 — Collect critical information. This process may involve a forensic team to assess the breach and help collect data. Detailed notes should be kept on the process.[110]

Step 4 — Proceed with notification procedures, including internally, law enforcement, regulators, and customers/third parties. After notification, focus should be on continued legal compliance.[111]

---

107 Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents, Version 1.0 (April 30, 2015).

108 *See id*. at 6-7.

109 *See id*. at 7-8.

110 *See id*. at 8-10.

111 *See id*. at 10-12.

[6] — Information Sharing.

In addition to dealing with a cybersecurity attack or data breach event within your own company, those in the energy industry should be aware of benefits of information sharing networks. First, alerting similarly situated companies will allow them to prepare for potential attacks, and help protect the industry as a whole. In addition, participation in information sharing networks may also give companies a forum to share tactics related to responding to data loss or cyber attack if another company has experienced a similar problem.

§ 28.06. Insurance Coverage.

Insurance can play a vital role in an organization's overall strategy to address, mitigate, and maximize protection against the legal and other exposures flowing from data breaches and other serious cybersecurity, privacy, and data protection-related incidents.

[1] — Potential Coverage Under "Legacy" Policies.

There may be significant potential coverage for cybersecurity and data privacy-related incidents under an organization's traditional insurance policies, including its Directors' and Officers' Liability, Professional Liability, Fiduciary Liability, Crime, Commercial Property and Commercial General Liability (CGL) policies. For example, there is potential coverage for data breach-related liability under CGL Coverage B "personal and advertising injury" coverage. The current ISO standard form policy states that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury,'" which is defined to include "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." ISO Form CG 00 01 04 13 (2012), Section I, Coverage B, Section 1.a., Section 14.e. Courts have upheld coverage for data breaches and other claims alleging violations of privacy rights in a variety of settings.

Likewise, an organization may have significant potential coverage under its Commercial Property policies for first-party property damage and business income loss.

In response to decisions upholding coverage for cybersecurity and data privacy-related risks under traditional lines of insurance coverage, however, the insurance industry has added various limitations and exclusions to traditional lines of coverage.

By way of example, Insurance Services Office (ISO), the insurance industry organization that develops standard insurance policy language, recently introduced a new series of cybersecurity and data breach exclusionary endorsements to its standard-form CGL policies, which became effective in May 2014. One of the endorsements, entitled "Exclusion - Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability - Limited Bodily Injury Exception Not Included," adds the following exclusion to the primary CGL policy:

> This insurance does not apply to:
>
> **p. Access or Disclosure of Confidential or Personal Information and Data-related Liability**
>
> Damages arising out of:
>
> **(1)** Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of non public information; or
>
> **(2)** The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.
>
> This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph **(1)** or **(2)** above.

In connection with its filing of the endorsements, ISO stated that "when this endorsement is attached, it will result in a reduction of coverage . . . ."

Likewise, it is common for energy sector property programs to contain one of the following three "electronic data" exclusions, or other broad electronic data-related exclusions.

Institute Cyber Attack Exclusion Clause CL380

1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by, or contributed to by, or arising from, the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

Terrorism Form T3 LMA3030 Exclusion 9 (Extract)

This Policy does not insure against loss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code."

Electronic Data Exclusion NMA2914

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

a) This Policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

ELECTRONIC DATA means facts, concepts and information converted to a form useable for communications, interpretation or processing by electronic and electromechanical data processing or electronically controlled equipment and includes programmes, software and other coded instructions for the processing and manipulation of data or the direction and manipulation of such equipment.

COMPUTER VIRUS means a set of corrupting, harmful or otherwise unauthorised instructions or code including a set of maliciously introduced unauthorised instructions or code, programmatic or otherwise, that propagate themselves through a computer system or network of whatsoever nature. COMPUTER VIRUS includes but is not limited to 'Trojan Horses', 'worms' and 'time or logic bombs'.

b) However, in the event that a peril listed below results from any of the matters described in paragraph a) above, this Policy, subject to all its terms, conditions and exclusions, will cover physical damage occurring during the Policy period to property insured by this Policy directly caused by such listed peril. Listed Perils:

- Fire

- Explosion

These and other newer exclusions to traditional lines of coverage provide another reason for organizations to carefully consider specialty cybersecurity insurance products.

[2] — Cybersecurity Insurance Policies

Cybersecurity insurance coverage can be extremely valuable, but choosing the right insurance product presents significant challenges. There is a diverse and growing array of products in the marketplace, each with its own insurer-drafted terms and conditions that vary dramatically from insurer to insurer — and even between policies underwritten by the same insurer. In addition, the specific needs of different industry sectors, and different organizations within those sectors, are far-reaching and diverse.

Although placing coverage in this dynamic space presents a challenge, it also presents a substantial opportunity. The cyber insurance market is

extremely competitive and cyber insurance policies are highly negotiable. This means that the terms of the insurers' off-the-shelf policy forms often can be significantly enhanced and customized to respond to the insured's particular circumstances. Frequently, very significant enhancements can be achieved for no increase in premium.

There are a number of established third-party coverages, *i.e.*, covering an organization's potential liability to third parties, and first-party coverages, *e.g.*, covering the organization's own digital assets and income loss, as summarized in the chart on the following page.

In addition to the established coverages, there are significant emerging markets providing coverage for:

- first-party losses involving physical asset damage following an electronic data-related incident;
- third-party bodily injury and property damage that may result from an electronic data-related incident; and
- reputational injury resulting from an incident that adversely impacts the public perception of the insured organization or its brand.

As privacy and electronic data-related exclusions continue to make their way into traditional property and liability insurance policies, and given that an organization's largest exposures may flow from reputational injury and brand tarnishment, these emerging coverages will be increasingly valuable.

Third Party Coverages

Type	*Description*
Privacy Liability	Generally covers third-party liability, including defense and judgments or settlements, arising from data breaches, such as the Target breach, and other failures to protect protected and confidential information
Network Security Liability	Generally covers third-party liability, including defense and judgments or settlements, arising from security threats to networks, *e.g.*, inability to access the insured's network because of DDoS attack or transmission of malicious code to a third-party network
Regulatory Liability	Generally covers amounts payable in connection with administrative or regulatory investigations and proceedings, including regulatory fines and penalties
PCI DSS Liability	Generally covers amounts payable in connection with Payment Card industry demands for assessments, including contractual files and penalties, for alleged non-compliance with PCI Data Security Standards
Media Liability	Generally covers third-party liability arising from infringement of copyright or other intellectual property rights and torts such as libel, slander, and defamation, which arise from media-related activities, *e.g.*, broadcasting and advertising

First Party Coverages

Crisis Management	Generally covers "crisis management" expenses that typically follow in the wake of a breach incident, *e.g.*, breach notification costs, credit monitoring, call center services, forensic investigations, and public relations efforts
Network Interruption	Generally covers the organization's income loss associated with the interruption of its business caused by the failure of computer systems/networks
Contingent Network Interruption	Generally covers the organization's income loss associated with the interruption of its business caused by the failure of computer systems/networks
Digital Assets	Generally covers the organization's costs associated with replacing, recreating, restoring, and repairing damaged or destroyed computer programs, software, and electronic data
Extortion	Generally covers losses associated with cyber extortion, *e.g.*, payment of an extortionist's demands to prevent to a cybersecurity or date privacy-related incident