TEXAS LAWYER

An ALM Publication

texaslawyer.com | March 27, 2018

A Look at the Data Issues Energy Industry Counsel Face this Year

BY DEANA UHL

As one of the longest standing segments in the global economy, the energy industry is deeply rooted in its processes and conventions. Aside from environmental protection policies, it is not as regulated when compared with health care and financial services organizations. Without a regulatory strong arm forcing certain practices, the energy industry has felt less pressure to adjust to the emerging challenges of today's growing data volumes and new data privacy laws. Many operate in a culture that tends to be slow to adopt new approaches in the face of economic, legal and regulatory change.

Data Breach.

Due to the above and other industry factors, counsel at oil and gas companies are often sitting on large volumes of information, which can be problematic for many reasons. Data hoarding presents challenges across data protection initiatives, electronic discovery activities for litigation and investigations, and importantly, compliance with Europe's General Data Protection Regulation (GDPR) and other global data privacy legislation. Further, energy companies are ripe for data breaches, and tend to face higher costs per data breach than the average corporation.

The Ponemon Institute's 2017 Cost of a Data Breach study found that the cost of a breach in the energy and utilities industry is estimated at $7.4 million per incident, a figure that is holding steady from previous years, while the global average rate across all industries dropped 10 percent from 2016 to 2017. Many organizations would view these figures with alarm, but energy companies have a unique perspective on risk. The cost of a single breach is relatively low stakes in comparison to the amount of money even small oil and gas companies are accustomed to spending for exploratory drilling. GDPR and other privacy, security and data breach laws on the horizon, however, will have more teeth than what the industry has experienced to date.

GDPR

Enforcement of the GDPR will go into effect in May of this year, and will impact all companies with a footprint in Europe. The law is broad sweeping, and states that organizations in breach of its extensive

requirements may be fined up to four percent of annual global turnover, or €20 million (whichever is greater). International companies that deal in Europe need to comply with GDPR, whether they are storing information for employees, contractors, vendors or customers. Oil and gas companies will be impacted, and should be addressing GDPR head-on, assessing the full scope of regulated data that is housed within the company and what processes are already in place that may help or hinder compliance. Counsel must review requirements and applicability, and identify gaps and areas of risk across people, process and technology to develop a pragmatic roadmap and action plan.

There are many requirements that will require attention, and particularly for oil and gas companies, contract management is a key area that must be addressed. Privacy information, such as physical addresses and even Social Security Numbers, is often collected in oil and gas industry contracts, particularly those with individual contractors or private land owners for drilling sites. Organizations will be required to protect the privacy of that information and ensure it is not inappropriately shared or breached. Another consideration is the obligation for certain companies to appoint a Data Protection Officer (DPO). The 2017 *General Counsel Up-at-Night Report* from Morrison & Foerster and ALM Intelligence found that only 10 percent of respondents already have a DPO in place, while 74 percent indicated they do not have plans to appoint one to comply with GDPR.

Internal Threats

In recent years, the energy industry has started to address cybersecurity in response to external threats. However, internal threats, which are equally dangerous, have been less of a focus. The Ponemon study mentioned above found that more than 50 percent of data breaches were not caused by malicious or criminal attacks, but rather by internal system issues or human errors. Counsel must be aware of how internal leaks or information theft by employees will impact data protection and privacy efforts. Holistic information governance (IG) programs help ensure access management protocols and prevent sensitive information from walking out the front door. Data remediation initiatives are a key part of this and can include a variety of activities to bolster data protection.

Identifying what trade secrets the company has, understanding who has access to what data, and reasonably limiting access are important first steps. Policies should involve a sustainable tracking process for when employees change roles or locations, or leave the company and should include a mechanism to know what devices departing employees were using. Employee agreements and exit interviews are additional best practices. Defensible data disposal, wherein redundant, outdated and trivial (ROT) information is deleted from company archives and backups, will help reduce data volumes and the associated legal and regulatory risks of over-preserving as well as improve employee efficiency in the ability to locate and find trustworthy data.

There are of course justifiable reasons for why oil and gas companies default to data hoarding. Though attitudes are starting to change, some legacy preservation practices will remain. Whatever a company's decision is on what must be preserved and what can be disposed of, a sound IG program, rooted in privacy enablement and driven by counsel, will ensure the company can effectively protect sensitive data and comply with GDPR.

Deana Uhl *is a senior director in the FTI Technology practice and is based in Houston. Uhl provides consulting to corporate clients, with a focus on designing, implementing and enabling change management for information governance, data privacy, data security and e-discovery programs. Uhl has particular expertise in advising oil and gas companies on the processes and technology to effectively address legal and regulatory matters and improve information quality and life cycle management to support operational excellence.*