NOVEMBER 29, 2017

Legaltech news©

ONLINE

An ALM Publication

Energy Sector Vet Says Strong Info Management Means Better Security and Compliance

New FTI Consulting senior director Deana Uhl looks back on her work with cybersecurity and information governance in the energy sector.

BY IAN LOPEZ

In the energy sector, data breaches can be tremendously consequential. Breaches abound with the potential for physical disaster as well as inadvertently revealing lucrative information, so there's little room for cybersecurity follies.

Energy sector veteran Deana Uhl thinks many cyber issues can be addressed through strong information management strategies. But the benefits don't stop there. Uhl, who for over a decade led information governance and compliance programs at Marathon Oil Corp., says that stronger information management could also be key to addressing stringent international data regulations.

This November, Uhl was appointed as senior director of FTI Consulting Inc.'s technology segment, where she will focus on privacy, e-discovery, data security and compliance efforts for clients. Uhl spoke with LTN about her years in the energy sector and the major issues impacting it today.

Deana Uhl, senior director of FTI Consulting's technology segment.

Plugged In

LTN: What are some of the information governance and data privacy issues unique to the energy sector?

Deana Uhl: I think most things with the energy sector are not too unlike other areas. But energy companies deal with data privacy on a daily basis. We have an international footprint in multiple countries, we have multiple offices, and how we communicate and translate that information between different offices is key. There are also multiple records retention requirements when it comes to these companies.

So I wouldn't say it's unique, but they do have their challenges similar to those of other global footprint companies.

What's the most difficult data management challenge for the energy sector?

Data transfers. Especially over in some of the countries in the eastern area, you have a lot of data transfer requirements where that information cannot leave the country. And so coming up with those protocols on how you maintain and manage that information can be one of the biggest challenges, especially when you're having to meet e-discovery requirements and a variety of U.S. regulatory requirements.

Are there any particular countries whose data laws are difficult for compliance while trying to comply with U.S. laws?

Yeah, a lot of them over in the Middle East have a lot of data, like seismic data and other technical data, that can't leave the country. And so while you've generated that information, that information has to stay in that country, and you have to manage it under that country's laws.

Are there any information governance strategies where you see energy companies in particular falling short?

Not necessarily. But a lot of oil and gas companies are very old, they've been around for a long time, and so they have a lot of data that is out there.

With energy companies, you've got some that are purely an upstream company, and others are more integrated, like the Exxons and Chevrons, that have a midstream and downstream facility as well, and each one of those come with their own regulatory requirements.

Is it harder to get older companies to upgrade their systems or implement new strategies than newer ones?

What you get into with the older companies is focusing on a lot of the legacy data that's sitting out there. Some of these companies have data that goes all the way back to 50 years, whether it's physical or in an electronic format. We're generating more and more information, and how we're going to manage that going forward is a really big challenge for any company.

So how can energy companies begin improving their information management strategies?

One of the key recommendations I would have for any company is really to sit down and understand the crown jewels—the data set that is most valuable to your company that you need to have in order to be able to do business and focus on it.

I think that what a lot of companies focus on is different data locations and not the actual data set or what that most valuable thing is. So if you lost it and you couldn't retrieve it to respond to regulatory requirements or even just to file a financial [document], that really causes a lot of inefficiency at the company, but it also impacts being able to do your business.

Focus on the top five data sets that you really need to focus on, then find a way to proactively manage them so that they bring both cost efficiency and risk reduction to your company.

What has your experience been like with facilitating conversations between IT, leadership and legal on information governance strategies?

Most of the IT departments I've worked with were sitting down with those departments and trying to come up with strategies on how to better protect information. One of the bigger—I wouldn't really say it's a challenge—is working with the business unit, because they literally own the data. It's their data that they're generating on a daily basis. There are challenges with them whenever you start having conversations about where they can be storing that information and how they can be better managing and protecting it. A lot of it just comes down to education and making them aware. [Data management] is not what they do on a daily basis.

To me, it's a balance scale between [information governance and compliance]: If you can manage your information in a way that you can meet your compliance requirements, I would bet you money that you were also better managing your information from an efficiency standpoint, because you can find your data.

I always ask my people, how much time do you spend on a daily basis looking for something? You know that there's a document there that you really need to get your hands on. You saw it a year ago but you can't find it, so you spend an hour looking for it. How would it feel if you knew exactly where that information was going to be located and you could search for it and find it pretty quickly?

I think that's one of those areas where if you can bring efficiency and compliance, then it's a win-win for information governance.

Is an increased focus on breaches leading to more conversations between IT and business?

In some ways. It's always easy to walk in and kind of scare them with the scary stories. But it really translates back to efficiency, because there's going to be some business groups in a company where cybersecurity isn't their main focus. They think that's an IT problem. And to me, it really takes "three legs with a stool" to make information governance successful, and that includes IT, legal departments and the business unit. If they're all pulling together, that's going to make it easier on everybody.

What types of breaches are hitting energy companies specifically?

In my experience, there is an increase in attacks on energy systems, whether it's on the control systems, or where [hackers] are trying to get into the systems for intellectual property, information on M&A activity and financial information.

A lot of people focus on cybersecurity form [as] an external standpoint, but there's also the internal portion. There are employees who every day have their hands on very sensitive information. The majority of data breaches were because someone walked out the door with data they never should have had in the first place.

When you look at data governance, it's about preventing people from getting in the door, which is obviously a huge deal, but there's also that internal component. If someone didn't click on that email or have access to that data, then the data would have been protected better.

Ian Lopez *is the senior technology editor for ALM Media.*