protiviti®
Face the Future with Confidence

Energy and Utilities Industry Perspectives

Your monthly blog and industry news round-up

March 2017

Data Security Alarms Should Be Sounding for Oil and Gas

Oil and gas industry executives don't need to see a new Wikileaks story about secret CIA hacking tools or hear more about the electronic penetration of presidential campaigns to understand the seriousness of a potential digital hack to their operations.

But it's a large step from knowing a risk exists to being ready for it. Achieving confidence in the ability to manage such risk can involve substantial new investments and operational adjustments, even for an industry accustomed to meeting regulatory, operational and market challenges.

Protiviti's recently released **2017 Security and Privacy Survey** indicates that oil and gas companies are facing their cybersecurity challenges in ways similar to other industries. The survey's main findings include:

- Nearly one in five companies cannot confidently identify or locate their "crown jewels," or most valuable data assets, because they lack an effective enterprisewide data classification scheme and policies.
- How well companies manage their vendors' security practices marks a notable difference between top security performers and the rest.
- Companies with a high level of board engagement in information security issues rate considerably higher than those without such involvement in nearly all facets of information security best practices. These companies also report a higher level of confidence in their ability to prevent an opportunistic data breach.

These findings largely correspond to what we have seen among our own energy clients. One difference we have noticed, however, is that energy companies tend to have little to no formal documentation on testing of security incident response plans, compared to other industries. This could mean that energy executives have not substantiated a basis for the same level of breach-prevention preparedness as some other industries. I would argue that as a critical infrastructure, they should.

Although Protiviti energy clients indicate they are committed to security, we see about the same 38-percent level of compliance with implementation of the five core information security policies identified in the Protiviti survey: acceptable use, records retention/destruction, data encryption, information security, and social media policies.

In addition, energy companies, specifically those in exploration and production (E&P), have been hesitant to invest in tools to identify where their "crown jewels" are stored, apparently on the basis that many do not feel their company is much at risk because it does not retain much sensitive data. However, many common processes at E&P companies (i.e., escheat and royalty owner payments) do involve sensitive information protected by state privacy laws (e.g., individual tax ID numbers are actually Social Security numbers). Further, company confidential information, such as reservoir data, land acquisition data, and merger and acquisition activity, would be considered data that requires identification and protection. Very commonly, even where these processes are mostly manual, this information is digitized (e.g., scanned documents) or entered into a system. If the company does not know what data exists and where, it will have a difficult time protecting it.

Energy executives and boards would be wise to ask themselves some worst case scenario questions and know the answers now rather than having to discover them under fire later:

- If our data assets were compromised, could they be reconstructed, and how long would it take?
- If field operations were disrupted by an attack on the operational control system, how much revenue would be lost per week? Per month?
- If competitors or counter-parties were able to learn confidential details of our strategies and plans, where would our company be most vulnerable?

The bottom line is that what you don't know, such as where your critical data is, can, and eventually will, hurt you. With all issues of cybersecurity, it's only a matter of time.

Will Hiring Hackers Help Energy's Cybersecurity Efforts?

The chief cybersecurity engineer for a major industrial process company **advocated** not long ago that oil and gas companies hire hackers to improve their cybersecurity defenses. At an annual European-Middle East-Africa user group conference in The Hague last October, Eric Knapp urged attendees to drop their negative perceptions and put hackers to work on their teams.

Knapp's advice followed a presentation of survey findings stating that 82 percent of oil and gas industry respondents have experienced an increase in successful cyberattacks over the past 12 months. Executives of European petrochemical companies SARAS and SABIC estimated that cyberattacks cost businesses up to $400 billion per year.

Several weeks earlier, the World Energy Council (WEC) issued a **report** that, among other conclusions, found that the demand for cyber specialists is growing twice as fast as for all other IT jobs. The WEC cited research linking recent high-profile security breaches to a shortage of almost one million skilled cybersecurity professionals.

Our perspective:

The idea of leveraging "hackers" needs to be put into context. Many organizations have resources (internally or through consulting firms) who mimic the activity that various types of real hackers execute to illegally break into a company's IT infrastructure. These "white hat" penetration testers are excellent at testing infrastructures, applications, networks and databases. The use of trained personnel who act as hackers but have written agreements and rules of engagement can make a lot of sense for an organization and is worth considering.

However, cybersecurity, much like other strategic initiatives, cannot be addressed with technology resources or tools alone. It requires a joint effort among departments and employees of all levels. In the same way that police cannot solve all crimes by themselves (despite being the "experts"), cybersecurity professionals need the knowledge and assistance of everyone in the organization. Employees who have been educated on matters of cybersecurity become empowered and thus an extension of the security program.

Finding the similarities between cyber risks and existing risks (e.g., safety) can help translate this subject to nontechnical resources. Many of the lessons learned with regard to overall risk management through more traditional departments, such as internal audit or compliance, can be applied to cybersecurity. Sharing data points that are already being collected by these departments can add value to analyzing security threats. At an even higher level, sharing information across the industry in cyber intelligence groups (CIGs) can allow firms to collaborate on specific threats and solutions, and share data that can add value to their overall threat analyses.

Is hiring "hackers" the answer to the cybersecurity challenge? It's not quite that simple. White hat hackers certainly have a key skill set organizations need to face the growing threat of cyber crime, but the ultimate success of an organization lies in how well the leadership empowers the overall enterprise to combat cyber risks together.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contact

Tyler Chase
Managing Director
Leader, Energy and Utilities Industry Practice
+1.713.314.5036
tyler.chase@protiviti.com

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®