Hackers Eye U.S. Oil and Gas **Infrastructure**

Almost every form of technology is connected to the internet, which allows for very advanced monitors and controls from a remote location. The downside of this interconnectivity is that critical infrastructure may be vulnerable to cyberattacks. Among the most critical infrastructure in the U.S. is within the energy industry, with power plants, pipelines and oil fields connected to systems that hackers may target. In a recent interview with Privcap, cybersecurity expert Tauseef Ghazi, a principal at RSM US LLP, discussed the nature of the threat, why too many middle-market companies are not prepared to deal with it, and where hackers have already made inroads.

Privcap: What threats do cyberattacks pose to U.S. infrastructure? Do you think this threat will increase in 2018?

Tauseef Ghazi, RSM: The threat will definitely increase in 2018. At the end of 2017, the Department of Homeland Security and the FBI issued a warning that was geared toward U.S. critical infrastructure and threats to it. That, plus what we've seen in Europe—around a power grid being compromised coupled with the increase in ransomware in 2017 will significantly increase the threats to cybersecurity in 2018.

Do you think the oil and gas industry is prepared in terms of cybersecurity?

Ghazi: Low oil prices put a burden on middle-market energy companies when it came to cybersecurity. Middle-market oil and gas companies are playing catch-up at this point.

Is there a risk in middle-market energy companies moving sensitive information to the cloud?

Ghazi: With oil prices as low, it was a natural transition to move information to the cloud and use commoditized services to manage your infrastructure. However, companies need to be conscious that when you move information to the cloud, you're not transferring the risk associated with that. The risk still stays with those companies. So, getting good processes around that is very important.

Tauseef Ghazi
National Leader,
Critical Infrastructure Security,
RSM

Do middle-market firms tend to have less protective oversight?

Ghazi: Yes. It's mostly due to lack of regulations. If you look at the oil and gas sector, there's not any specific cyber regulations within that sector. Power and utilities are a little different where there are specific regulations, but they're only focused on certain asset classes and their criticality to the bulk electric system. In addition, middle-market companies typically have not focused on building cyber programs within their management ranks and they are now just catching up to that.

What are the hackers doing now, exactly?

Ghazi: Industrial espionage is complex—it's not your average hacker that can do that. It requires a lot of time, investment and research. Currently, the threats are more like reconnaissance. They're not really attacking things, but doing reconnaissance to understand what those environments look like.

Is industrial espionage targeting intellectual property or is the goal to shut down critical infrastructure?

Ghazi: If the target is a power company then the goal would be to ultimately get to the bulk electric system and the power interconnects. If that is impacted then multiple industries, like the financial industry, healthcare etc. will all be impacted in the region. If you don't have power, you can't process banking transactions. In the healthcare industry, if you don't have power, you can't operate your hospitals.

How would an increase in cybersecurity regulations impact oil and gas?

Ghazi: An increase in cybersecurity regulations within the oil and gas industry would create a common set of controls and criteria that would allow for consistent implementation of those controls across the industry. Currently, we have a lot of standards, like the (International Electro-technical Commission (IEC) and the National Institute of standards and Technology (NIST) standard, that companies utilize. But the implementation of those vary from company to company. By having a common framework, it would establish a baseline of controls for all oil and gas companies.

What can you tell us about recommendations from the recent National Commission on Enhancing Cybersecurity report?

Ghazi: Most of those recommendations are pretty straightforward and most companies should implement those recommendations. The good news is that this White House administration currently has cybersecurity as a priority on their plan. The bad news is that we just haven't seen the details of that plan as yet. With the recent shake-up of the White House cybersecurity coordinator position, I think that that plan is somewhat coming into motion and we should be seeing some of that appear very soon. ■