Governing Energy

Cyber T

Volume 3 Number 4—February 17, 2014

Almost a decade ago this author put forth the concept of a Chief Security Officer, an individual responsible for both physical and cyber security of the global enterprise.[i] One of the points made in support of that position was the long-standing dispersed information management that was integrated with plant operations.

In another piece of that era, an economic risk framework was put forth that incorporated quantitative as well as qualitative data and information into a decision support model. *Aspects of such a model might include:*

- *An assessment of the relative exposure and identification of vulnerability entrance points*
- *Stochastic modeling of event possibilities and the development of sensitivities to possibilities that can then be quantified as a range*
- *Predictive modeling of a set of possible eventualities and their impact on the organization*

Such a model can be built using available software tools incorporating the specific data and information to which an individual firm may expect to be exposed. Finally, modeling the once-in-a-lifetime cataclysmic event that only the most pessimistic expect and developing response plans to Armageddon is possible, and, importantly, is being done in the power industry today.[ii]

The threat to control systems is not new. *In early 2000, an employee from an Australian software manufacturer was fired, and when he was turned down for a job with the local government, he retaliated using wireless technology illegally acquired from his former employer to release millions of gallons of raw sewage*.[iii]

Flash forward ten years and Cyber Terrorism has been taken to a new level. This is not to say nothing has been done, but that the challenges rise at a meteoric rate.

Historically, there has been an “air gap” between control systems and other IT systems on Mobil Offshore Drilling Units (MODUs). In other words a physical barrier or disconnect. However, poor system management procedures and a growing hunger for data may compromise this barrier.[iv]

Poor IT governance has led to significant damage from cyber-attacks. It appears that the retailer, Target cybersecurity team raised concerns prior to cyber-attack last year. Perhaps lost in the volume of warning received, yet it is apparent that the company’s payment network did not have sufficient isolation from the rest of the firm’s IT systems.[v]

So we raise the question once again. Is it time for a CSO reporting directly to the CEO? Much like the focus of enterprise risk management, this would focus, fund and measure the firm's exposures to physical and cyber terrorism. This individual would also be responsible to assure *zonal isolation* for IT networks.

Does your firm's governance model assure the isolation of control systems?

About the Author

Dr. Scott M. Shemwell has over 30 years technical and executive management experience primarily in the energy sector. He is the author of two books and has written extensively about the field of operations management. Shemwell is the Managing Director of The Rapid Response Institute, a firm that focuses on providing its customers with solutions enabling operations excellence and regulatory compliance management.

End Notes

[i] http://www.energycentral.com/gridtandd/communicationsandsecurity/articles/957/Security-Integration
[ii] Shemwell, Scott M. (2004, April) Integrated Physical and Cyber Security: A High Value Proposition for the Power Industry. Author.
[iii] Ibid.
[iv] http://www.digitalenergyjournal.com/n/Cyberattacks_to_drill_rigs_understanding_the_threats/1eccd4a9.aspx
[v] http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304703804579381520736715690.html