Governing Energy

Cyber Governance—Now!

Volume 7 Number 9—May 7, 2018

In 2011 as part of a research program regarding the new SEMS based Operations Management Systems the oil and gas sector was deploying, it appeared that one of the missing components at the time was an Asset Integrity Management Governance Model. Readers may remember that during that period there were three major management failures resulting in death, billions in property losses and significant environmental damage:

- BP Deepwater Horizon aka Macondo—commencing April 20, 2010
- San Bruno Pipeline Explosion—commencing September 9, 2010
- Fukushima Daiichi Nuclear Incident—commencing March 11, 2011

In October of that year we put forth our White Paper, *Asset/Equipment Integrity Governance: Operations–Enterprise Alignment: A Case for Board Oversight*.[i] The purpose of this asset focused model was, "extending traditional thinking into field operations.

The Sarbanes Oxley Act of 2002 required "transparency," but its implementation appears to be mostly financial in nature. Issues around fraud were top of mind post Enron et.al. so, this is somewhat logical.

Overlooked in traditional governance models were the Assets. In other word, the firm's Balance Sheet.

Governance models are risk mitigation in nature. Their goal is to assure the organizations functions in accordance with regulations, ethics, good citizenship, etc. across all activities including that of its ecosystem.

Cyber Exposures

According to one recent study, “Although companies are detecting (cyber) breaches faster, security teams are still only finding 64 percent of them.[ii] This same article puts forth a five-step program to achieve cyber resiliency. They appear to have decidedly ‘technology’ bent to them.

- Build a strong foundation
- Pressure test resilience like an attacker
- Employ breakthrough technologies
- Be proactive and use threat hunting
- Evolve the role of CISO[iii]

Some of these actions are traits of a High Reliability Organization, i.e., Resiliency. However, absent is the involvement of those charged with organizational governance—the Board of Directors. If the threat (as articulated in the referred piece) is that high, why isn’t the Board actively involved?

Arguments that the Board delegates authority and responsibility on these operational problems are mute given the potential impact on the organizations of failures—potentially as great as the three disasters mentioned above. Time for action!

One Organization’s Action Plan

Recently the US Department of Defense elevated its U.S. Cyber Command to a *Combatant Command* stating in part, "The cyber domain will define the next century of warfare." By making this change, the commanding officer of Cybercom will now report directly to the Secretary of Defense. [iv]

By putting Cybercom on par with the nine other combatant commands the defense department acknowledges, “a new warfighting domain has come of age.” This is recognition that an effective cyber defense is just as critical to national defense as other *traditional* military forces!

We continue to believe that cyber security is now a Board level issue. It seems the Department of Defense agrees with us. Where does the commercial sector responsible for national Critical Infrastructure sit on this fence?

How Important to Your Organization is Cyber Defense?

Free Economic Value Proposition Matrix version 2.0 (realize the value of your investment)
Also, checkout our YouTube Channel

Additional details are available from the author.

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 six books and has written extensively about the field of operations. Shemwell is the Managing Director of The Rapid Response Institute, a firm that focuses on providing its customers with solutions enabling Operational Excellence and regulatory compliance management. He has studied cultural interactions for more than 30 years—his dissertation; *Cross Cultural Negotiations Between Japanese and American Businessmen: A Systems Analysis (Exploratory Study)* is an early peer reviewed manuscript addressing the systemic structure of societal relationships.

End Notes

[i] http://therrinstitute.com/wp-content/uploads/2017/10/asset_integrity_governance_-ver_1.1.pdf

[ii] https://www.securitymagazine.com/articles/88926-study-finds-87-percent-of-focused-cyberattacks-are-prevented

[iii] Ibid.

[iv] https://www.globalsecurity.org/security/library/news/2018/05/sec-180503-afps01.htm?_m=3n%2e002a%2e2282%2elf0ao0731u%2e23mu