Governing Energy

Cyber Operations

Volume 4 Number 20—October 20, 2015

During the late 1990s, we needed to address infrastructure concerns vis-à-vis Y2K exposure of real time systems. Concerns that the lights would go out at midnight drove a high level of effort to assure that would not happen.[i]

Today we face a more insidious cyber exposure. More than a decade ago we raised the issue of *Security Integration* (cyber and physical security).[ii] Following what many believed was a Y2K hoax; these issues did not appear to be timely "in the day."

Earlier this year, we learned that hackers could take over an automobile.[iii] Concerns about airliners were expressed as well.[iv]

Process industries have invested heavily in real time systems, the so called digital oilfield, remote operations and other cyber system solutions often using Internet or Cloud infrastructure. As commented herein previously, the upstream oil and gas sector has dramatically changed its safety processes following Deepwater Horizon incident in 2010.[v]

Likewise, the nuclear power sector made changes following Fukushima.[vi] Both heavily depend on new information management solutions. Other sectors have employed "Smart" devices and infrastructure or grid networks.

In the era of the industrial *Internet of Things*, any number of opportunities for hackers exists. Moreover, are firms whose IT departments have hitherto been focused on back office ERP systems prepared to address this potential onslaught?

Historically, organizations have developed cross-functional teams to address a myriad of business problems.[vii] Perhaps now is the time to stand up a permanent team composed of IT professionals, Operations and Risk Management experts? Such a team, working with cyber security experts would provide organizations with a "best practices" capability to resist attacks on producing assets.

It is important the organizations develop a culture that embraces the new *Internet of Things* world yet understands its strength and vulnerabilities. Such a culture should have a High Reliability mindset towards hackers, both from outside the organization and its supply chain as well as inside.

Is your organization prepared to reap the value from cyber enabled operations?

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 five 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. 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 social relationships.

End Notes

[i] Shemwell, Scott M. (2011). Bug Lore—Lessons for the Online Economy! Essays on Business and Information II: *Maximizing Business Performance*. (pp. 181-235) New York: Xlibris.

[ii] http://www.energycentral.com/gridtandd/communicationsandsecurity/articles/957/Security-Integration

[iii] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[iv] http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

[v] http://www.bsee.gov/Regulations-and-Guidance/Safety-and-Environmental-Management-Systems---SEMS/Fact-Sheet/

[vi] http://fukushimaupdate.com/

[vii] http://www.inc.com/encyclopedia/cross-functional-teams.html