YOUR
SOURCE
OF
TECHNICAL
&
SCIENTIFIC
INNOVATIONS

IABSRI

Integrated Activity-Based Simulation Research, Incorporated
1919 South Grand Blvd., Suite 412, Saint Louis, Missouri 63104-1573
Email: kofinsoyameye@earthlink.net, or kofinsoyameye@iabsri.net
Website: http://www.iabsri.net
Member of EDGE Innovation Network:
http://edge-innovation.com/current-member-section-landing/find-members/member-directory.html?filter=I

IABSRI's RESPONSE TO NIST's REQUEST FOR INFORMATION (RFI) ON CYBERSECURITY FRAMEWORK

SUBMITTED BY

DR. KOFI NYAMEKYE, PRESIDENT & CEO, IABSRI

ON

OCTOBER 10, 2014

COMMENTS ON CYBERSECURITY FRAMEWORK AND POTENTIAL APPROACHES TO RAISE AWARENESS FOR IMPROVING THE IMPLEMENTATION OF THE CYBERSECURITY FRAMEWORK

The traditional manufacturing production companies, such as the foundry or metal casting company, die casting company, injection molding company, etc., make their revenues only through running efficient shop floor PRIMARY ACTIVITIES (or functions), e.g., injection molding, machining, permanent mold casting, etc. Such manufacturing production companies are members of the supplier value chains of the major automobile manufacturing production companies in United States (U.S.). Also, they are typically small and medium-sized manufacturing production companies. Please see Figure 1 for Porter's generic value chain model which depicts the PRIMARY ACTIVITIES (or functions) and the SUPPORT ACTIVITIES [Porter 1985]. Figure 2 also shows Porter's generic value system model or supply chain model for a single enterprise and diversified enterprise (such as one of the major U.S. automobile manufacturing production companies). More importantly, such enterprises strongly believe that the PRIMARY ACTIVITIES (or functions), that do not directly add value to their customers' products, are considered wastes and should be completely eliminated. In fact, the Cybersecurity functions or activities in the *Framework Core*: *IDENTIFY*, *PROTECT*, *DETECT*, *RESPOND*, *RECOVER*, are extremely ***foreign activities*** to many of such manufacturing production facilities. We don't even yet know if we can correctly call them SUPPORT ACTIVITIES.

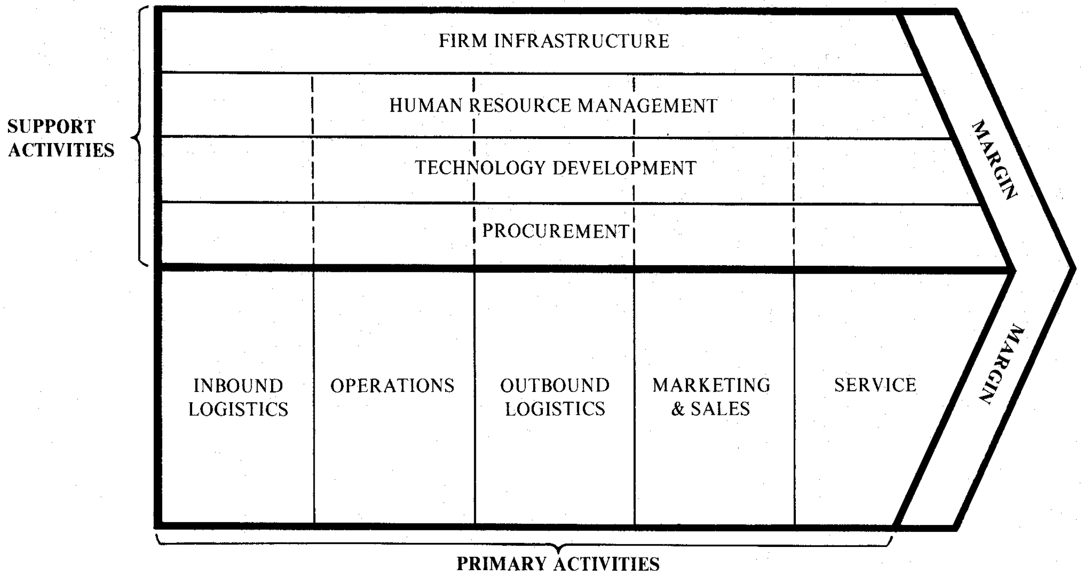

Figure 1. Value Chain [Porter 1985.]

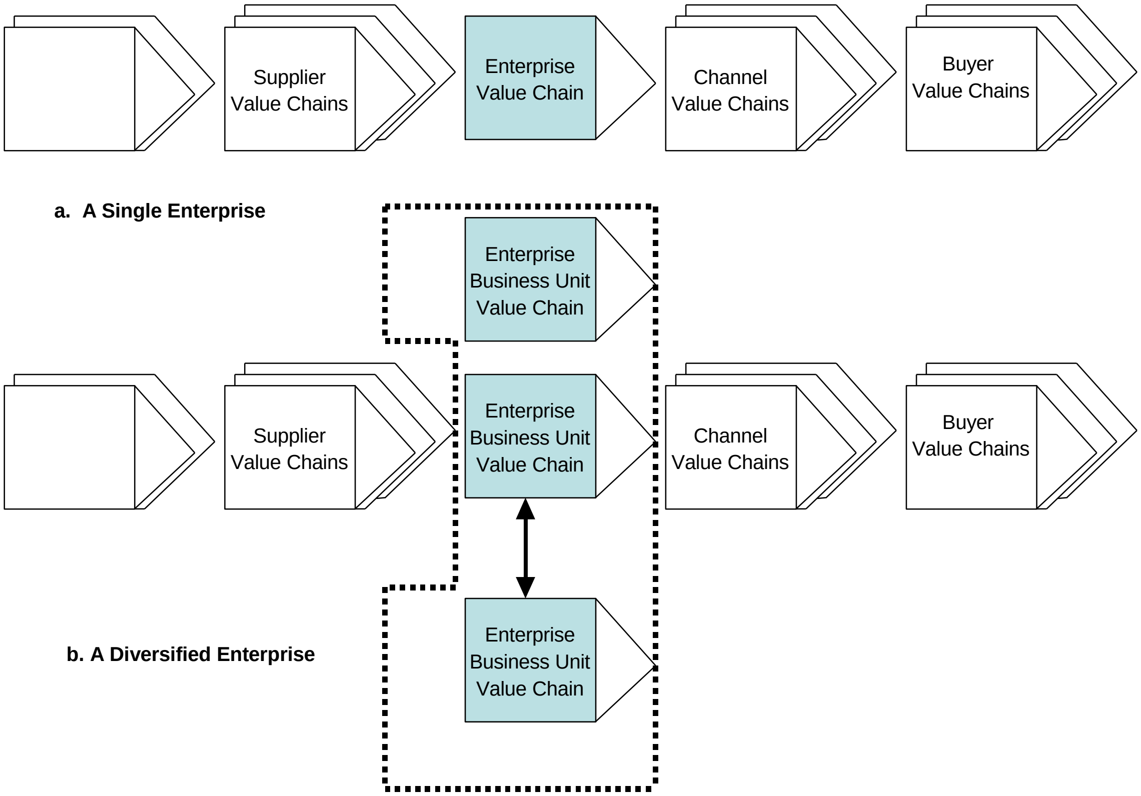

Figure 2. The Value System Model [Porter 1985.]; a. For a Single Enterprise; b. For a Diversified Enterprise.

Except for a few PRIMARY ACTIVITIES, such as entering quality control data on a specific machine into a *shop floor* PC, most of such small and medium-sized manufacturing production systems don't consider IT functions as helpful to adding value to their products. ***This is just the culture of such organizations***! Of course financial planning, human resource management, accounting, etc., are also SUPPORT ACTIVITIES – *office functions* – which mostly use IT systems such as PCs or servers for such activities. Thus, the CEOs of such companies are extremely hesitant to accept the new Cybersecurity functions which they may not see as SUPPORT ACTIVITIES.

Thus, unless we can convince the CEOs of such companies to consider the new Cybersecurity functions -- in the *Framework Core* -- as SUPPORT ACTIVITIES -- for the shop floor and the office, *the Cybersecurity Framework will not fly with such companies*!

Most of such companies are not even familiar with the concept of ***information sharing***, which is a critical ingredient to managing Cybersecurity risks throughout the value system or supply chain and let alone know how to perform it. Compounding ***information sharing*** is the fact that some of such organizations don't have efficient production methods to achieve superior performance – *low inventory, superior quality, low cost and on-time delivery*. For example, many of such manufacturing production companies have job shops which are very poor manufacturing production systems [Black 1991; Nyamekye et al. 1996; Nyamekye 2000; Nyamekye et al. 2005; Nyamekye 2007]. By a job shop we mean that the production system has a functional layout – e.g., similar or identical CNC (Computer Numerical Control) milling machines are grouped together into one area on the shop floor; similar or identical CNC (Computer Numerical Control) turning machines are also grouped together into another area on the shop floor, etc. The controller of each CNC machine is a programmable logic controller (PLC). Each controller becomes an *attack surface* for the Cyber terrorist. Thus, in addition to the poor performance of a job shop, implementing the Cybersecurity functions in a job shop would in fact increase the production costs of the shop floor operations.

Consequently, implementation of the Cybersecurity Framework in such manufacturing production systems, will require an integrated approach. Firstly, NIST ***should*** educate such companies that the Cybersecurity Framework will provide the SUPPORT ACTIVITIES, e.g., TECHNOLOGY DEVELOPMENT, to enhance the PRIMARY ACTIVITIES, e.g., operations, such as the manufacturing activities on the shop floor. One specific enhancement of the PRIMARY ACTIVITY, is the ***elimination of downtime*** of a CNC machine due to a malware attack of the PLC which controls the CNC machine operations. Operator's safety enhancement on the shop floor, is another benefit of implementing the Cybersecurity Framework. We will shortly discuss operator's safety.

Secondly, NIST ***should*** educate them that the implementation of the Cybersecurity Framework will naturally help them to think about transforming their manufacturing production systems into *net-centric* companies which will naturally help them to achieve superior performance -- *low inventory, superior quality, low cost and on-time delivery, and more importantly,* ***information sharing****, not only between their upstream and downstream PRIMARY ACTIVITIES, but also* ***information sharing*** *among the value chain members, to* **better manage the Cybersecurity risks** *throughout the value systems of which they are members, Figure 2.* Such an educational program will naturally create *awareness* of the Cybersecurity Framework. Implementing the ***new battlefield management*** concepts to transform such companies into *net-centric ecosystems*, is an example of one approach to become a *net-centric* enterprise [Alberts et al. 2003; Garstka et al. 2004; Alberts et al. 2006; Nyamekye 2010; ELICIT]. We will shortly discuss ELICIT. Many of such companies are extremely patriotic companies. They will be extremely happy to embrace the idea of using the new battlefield management concepts, that have been successfully implemented in Iraq [Knowledge@Wharton 2006] and Afghanistan, to achieve performance far superior to using the traditional lean production methods that do not even capture ***information sharing*** [ELICIT] and more importantly the dynamic nature of value systems that causes ***bull-whip effect*** [National Research Council 2000] – inventory imbalances -- in the value systems.

A direct excerpt, from the Website of the Department of Defense Command and Control Research Program (DODCCRP), explains ELICIT (Experimental Laboratory for Investigating Collaboration, Information-sharing, and Trust) as follows: *The U.S. DoD (OASD/NII) Command and Control Research Program (CCRP) sponsored the design and development of the ELICIT platform for experimentation and classroom activities focused on information, cognitive, and social domain phenomena.*

*The purpose of ELICIT-related experimentation, teaching, and analysis is to investigate the cognitive and social impacts of C2 approach and organizational structure (e.g. information sharing, trust, shared awareness, and **task performance**)* [http://www.dodccrp.org/html4/elicit.html]. We can use ELICIT to achieve ***information sharing and collaboration*** among the value chain members in the value system.

Many of the shop floor operations can be extremely dangerous to the shop floor workers if something accidentally goes wrong with the CNC machines. For example, certain parts require high speed machining. Thus, if a Cyber terrorist is successful to infect the controller of a CNC machine with a malware, which can then control the machining operations, such as: "*open the clamp that holds the work piece during the machining operations," such a deliberate action of the malware can cause the part to fly like a missile and instantly kill a shop floor worker. Consequently, bringing such an awareness to such manufacturing production companies, will further strengthen the implementation of the Cybersecurity Framework*!

REFERENCES

Alberts, S. D., and R. E. Hayes. 2003. *Power to the edge*. CCRP Publication Series.

Alberts, S.D., and R. E. Hayes. 2006. *The Future of Command and Control: Understanding Command and Contro*l. CCRP Publication Series.

Alberts, S.D., and R. E. Hayes. 2007. *PLANNING: COMPLEX ENDEAVORS*. CCRP Publication Series.

Arnholt, R., Book, G. and Cliffe, A. *New DoD Protections Against Counterfeit: Is Your Company Read?* http://www.crowell.com/files/New-DoD-Protections-Against-Counterfeit-Parts-Is-Your-Company-Ready.pdf (accessed August 28, 2013).

Black, J T. 1991. THE DESIGN OF THE FACTORY WITH A FUTURE, McGraw-Hill, Inc., New York, NY, 1991.

Borg, S. *Securing the Supply Chain for Electronic Equipment: A Strategy and Framework*. http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf (accessed August 28, 2013). The Internet Security Alliance.

Chang, K., H., Nyamekye, K., and Black, J T., "A Distributed Expert System for Manufacturing Cell Control," Chapter in Recent Development in Production Research, Vol. 6, pp. 861-867.

ELICIT (Experimental Laboratory for Investigating Collaboration, Information-sharing, and Trust), CCRP, http://www.dodccrp.org/html4/elicit.html (accessed October 10, 2014).

Garstka, J., and D. S. Alberts. 2004. *Network Centric Operations Conceptual Framework Version 2.0*. Washington, D.C.: Office of Assistant Secretary of Defense (Networks and Integration). June.

Hessman, T. 2012. *Cybersecurity on the Plant Floor: Manufacturers Go Wireless*, IndustryWeek, http://www.industryweek.com/information-technology/cybersecurity-plant-floor-manufacturers-go-wireless (accessed October 10, 2014), March 13, 2012.

Integra Asset Management. 2013. *Flowchart Depicting Integra Asset Management Tracking of Counterfeits and Malwares in OEMs Global Manufacturing Supply Chains*, Saint Louis, Missouri, August 2013.

Knowledge@Wharton, Leadership and Change. 2006. "Tip of the Spear: Leadership Lessons from the U.S.-led Armed Forces in the Middle East," Knowledge@Wharton, http://knowledge.wharton.upenn.edu/index.cfm?fa=viewfeature&id=1484 (accessed August 28, 2013), May 17, 2006.

Levin, C. 2012. Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts. http://www.levin.senate.gov/newsroom/press/release/senate-armed-services-committee-releases-report_on-counterfeit-electronic-parts#sthash.qFAJgIbJ.dpuf (accessed April 15, 2014).

Livingston, H. 2010. *Preventing and Detecting Counterfeit Electronic Components In the Supply Chain*. http://www.nhjes.org/2011_Joint_Conference/presentations/2B%20NHJES_Livingston_Henry_Oct6[2].pdf (accessed August 28, 2013). BAE Systems Electronic Systems.

Monden, Y. 1983. *Toyota Production System: Practical Approach to Production Management*, IIE Press, 1983.

National Research Council. 2000. *Surviving Supply Chain Integration: Strategies for Small Manufacturers*, National Academy Press, Washington, D.C., 2000.

National Research Council. 2005. Network Science, National Academy Press, Washington, D.C., 2005.

National Research Council. 2007. Strategy for an Army Center for Network Science, Technology, and Experimentation, National Academy Press, Washington, D.C., 2007.

NATO Network-Enabled Capability Command and Control Maturity Model (N2C2M2). 2010. CCRP Publication Series.

Net-Centric Checklist. 2004. Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, http://www.dod.mil/cio-nii/docs/NetCentric_Checklist_v2-1-3_.pdf (accessed May 30, 2004), Version 2.1.3, May 12, 2004.

National Institute of Standards and Technology. 2013. *Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework*. Gaithersburg, Maryland.

Nyamekye, K., J. A. Clendenin, and H. Burleson. 2004. "Information System Architecture for Wired Battlefield," 2004 Proceedings of Navy Marine Corps Intranet, June 2004 [CD Version].

Nyamekye, K., Sierhuis, M., and Hoof, R. v. 2009. "Planning For Manned And Unmanned Entities In Net-Centric Environment: Missions and Means Framework, Multi-Agent Simulation," Proceedings of 14th ICCRTS: C2 Architectures and Technologies, Paper Number 098, http://www.dodccrp.org/events/14th_iccrts_2009/track_09.html (accessed January 21, 2014), June 2009.

Nyamekye, K., 2000. *New Tool for Business Process Reengineering: Activity-Based Simulation Offers Functionality that We've Never Experienced Before Until Now*, IIE SOLUTIONS. http://www.iabsri.net/300nyamekye.pdf (accessed August 28, 2013), March 2000, pp. 36-41.

Nyamekye, K., and Y.-K., An. 1996. *Using Rapid Modeling Technology in a Permanent Mold Casting Production Facility*, AFS Transactions, Volume 96, pp. 96-188, 1996.

Nyamekye, K., and J., A, Clendenin. 2006. *ICLOGISTICS JOINT BATTLESPACE INFOSPHERE (JBI)-GRID ARCHITECTURE*, July 2006.

Nyamekye, K., Sutterfield, S., Askeland, D. R., and Bain, R., and Cunningham, M. 2005.

Classification and Coding: The First Step In Designing Manufacturing Cells: An article from: Modern Casting [HTML] (Digital), November 1994, Reprinted and Published, by Amazon Dot Com, http://www.amazon.com/gp/product/B00092YG9A/ref=sr_11_1/104-7516179-4397551?ie=UTF8 (accessed August 28, 2013), July 28, 2005.

Nyamekye, K. 2010. *Methodology for Designing and Evaluating Reliability of the DoD Net-Centric Ecosystem*, ITEA Journal 2010; 31: 399–409.

Nyamekye, K. 2013. "IABSRI ARCHITECTURE FRAMEWORK FOR COMPLETE AND SECURED SUPPLY CHAIN TO MITIGATE COUNTERFEITS AND MALWARES," white paper, August 2013.

Nyamekye Research and Consulting. 2000. *Member: National Institute of Standards and Technology Manufacturing Simulation and Visualization Program*. http://www.mel.nist.gov/div826/msid/sima/item2000/06mclean.pdf (accessed August 28, 2013).

Nyamekye, K. 2010. IABSRI Multi-Threaded Missions and Means Framework, Army SBIR Phase-I Base Final Report, August 25, Contract Number: W911QX-10-C-004506.

Nyamekye, K. 2007. "Axiomatic Design Approach for Designing Re-Configurable C4ISR Systems," Proceedings of 12th ICCRTS: C2 TECHNOLOGIES & SYSTEMS, Paper Number I-220, http://www.dodccrp.org/events/12th_ICCRTS/CD/iccrts_main.html, (accessed July 30, 2007), June 2007.

Pathak, V. *Improving Supply Chain Robustness and Preventing Counterfeiting through Authenticated Product Labels*. http://www.cs.stevens.edu/~vpathak/pubs/checkorigin.pdf (accessed August 28, 2013).

Porter Michael E. 1985. Competitive Advantage: Creating and Sustaining SuperiorPerformance: With a New Introduction, The Free Press, A Division of Simon & Schuster Inc., New York NY, 1985.

Stahl, F. 1994. *LEAN 94-0: Manufacturing Change at the John Deere Harvester Works*, Report On the Visit of the Ad Hoc Lean Aircraft Initiative Team, McDonnell Douglas Aerospace Saint Louis, Missouri, November 1, 1994. http://dspace.mit.edu/bitstream/handle/1721.1/1652/94_04.pdf (accessed August 28, 2013).

Sankar, R. 2013. *Five Ways to Optimize Supply Chain Management: Improve Collaboration Between Manufacturing Supplier and Retailer for Demand Data Driven Forecasting and Inventory Management*, IndustryWeek, August 2013. http://penton.ebookhost.net/iw/arena/1/ebook/1/index.php?e=139&user_id=84990&flash=11.800 (accessed August 28, 2013).

Yan Q., Li, Y., and Deng, R. H. *Malware Protection on RFID-Enabled Supply Chain Management Systems in the EPCglobal Network*, IGI GLOBAL DISSEMINATOR OF KNOWLEDGE, DOI: 10.4018/978-1-4666-3685-9. ch010. http://www.igi-global.com/chapter/malware-protection-rfid-enabled-supply/75517 (accessed August 28, 2013).