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
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.]
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


Knowledge@Wharton, Leadership and Change. 2006. “Tip of the Spear: Leadership Lessons


