Cybersecurity – The Issues

Michael St. Angelo, Chief Executive Officer
NeuraMetrics, Inc., Jacksonville Beach, FL

The White House issued a document in February 2003, titled *The National Strategy to Secure Cyberspace*. Specifically, the Actions and Recommendations section of this document calls for the development of best practices as part of the solution to secure cyberspace and in addition, this document states "……securing DCS, SCADA and PLC systems is a national priority". For the first time, the federal government has recognized the importance of process control to the national infrastructure and the need to focus on this importance in the light of the national awareness for homeland security. In fact, the Homeland Security Department has been delegated the responsibility of making the process industries pay attention to an area of concern that never was an area of concern……..until after September 11, 2001.

The government is trying to work with the process control industry to develop a strategic objective that makes sense. As we all know, the vertical segments within the process industries (Power Generating, Food, Pharmaceuticals, Chemicals & Petrochemicals, Water & Waste, Pulp & Paper, Mining & Minerals, and Textiles) are all very different and as far as public safety issues are concerned, all have important, but vastly different concerns. Although as important, the affects of a long term, significant, power outage is very different than a tainted food product, a tainted water supply or the loss of an oil refinery. A strategy is needed to deal with each type of disaster that could occur and a strategy is needed for disaster recovery from each.

The national strategy sets cybersecurity priorities:

- **A Cyberspace Security Response System**
- **A Cyberspace Security and Threat and Vulnerability Reduction Program**
- **Security Awareness and Training Programs**
- **Securing the Government's Cyberspace**
- **Cooperation between the people that are responsible for the National Security and International Cybersecurity**

This translates, for the process industries, into a three-pronged strategy:

- **To prevent cyber attacks against critical infrastructures**
- **Reduce vulnerability to cyber attacks**
- **Minimize damage and recovery time from cyber attacks that do occur.**

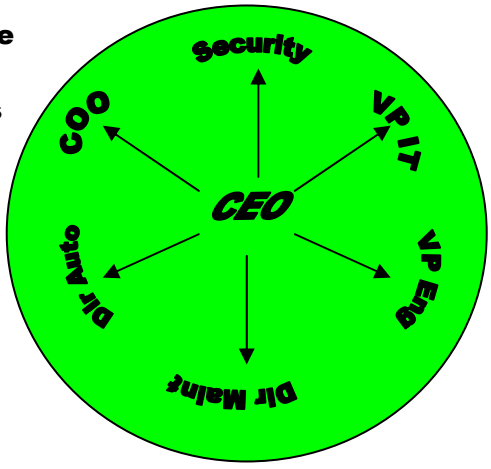
So far, we have viewed the problem from 30,000 ft. What we now need to do is begin to come down through the clouds. We need to begin to realize *how* each industry, as stated above, is very different, *how* each company in each industry stated above is different and finally, for the individual companies, *how* each plant in each individual company is different. This realization is complicated by the number of vendors that supply DCS, SCADA and PLC systems, the various types of products (control valves etc.) with which these systems interact, and the longevity these various systems have. Can a Foxboro 1st generation I/A system be secured from cyber attack using the same strategy as a Fisher Delta – V system or a Honeywell TDC 3000 system? The answer is no. However, there is some good news, for those who choose to view the glass as half full.

A huge portion of this problem is of a generic nature. The FBI, in studying the problem over the last ten years, found that in over 50% of the cyber attacks recorded (in the last ten years) the person spearheading the attack was someone having a trust relationship with the operation. That is, the culprit was, either, an employee, ex-employee, friend of an employee, etc. This suggests that, even in a terrorist attack, the chances are high that this "trust relationship" has to have been built to accomplish the attack.

This brings us to a new word on the scene; Cycurity™. Cycurity™ is the co-dependence of strategies that address both the cybersecurity world and the physical security world in industrial environments. The "industrial environments" in question are the physical environment as defined by the plant/individual company and the computer environment as defined by the vendor + individual company. Cycurity™ has the industry thinking in terms of CPTED (Crime Prevention Through Environmental Design) strategies and DRA (Degree of Responsibility Awareness) plans and OSP (Operations Security Plan) strategies. Today, collaborative security, another term not familiar to the industry is essential in manufacturing facilities.

Picture this: The head of (physical) security, the COO, the VP IT, the VP Engineering, the director of automation and the director of maintenance in a meeting where each has an equal role and an equal responsibility.

In most scenarios this is as foreign to the people involved as anything they have encountered in their entire career. In addition, there are issues that have been a "bone of contention" for years and may still be. Are DCS, and SCADA systems considered "computers" and are they available to the IT department for use or maintenance? Do IT people really understand the concept of "real time"? What should the



organization look like? Should Automation Department people report to IT Department people or visa versa? Is maintenance of a computer (process control or otherwise) considered "maintenance"? Etc. etc. etc. It is safe to say that in some companies these people would not attend such a meeting and if they were ordered to attend, would not contribute. And yet, this is exactly what is required to design an effective Cycurity™ Strategy. There are aspects of a Cycurity™ Strategy that could be considered a political football and that is a primary reason for using independent consultants to help in the design of the ultimate plan.

Collaborative security within an organization is absolutely essential…….but what about outside the organization? Yes, outside the organization there are entities that belong to the supply chain, have access to various parts of the control system, and therefore gain necessary information to keep the modern manufacturing operation (collaborative manufacturing) running. This access may be direct or indirect. Shipping departments "talk" inside and outside the manufacturing environment, Purchasing departments "talk" inside and outside the manufacturing environment, etc. This lays access to a company open for an attack from several different angles.

So what is the answer? There is no one answer to this problem which is growing in recognition by the day. Companies must examine their individual situation and begin planning from scratch. There are several methodologies available to choose from but each needs to be integrated into the company philosophy. The physical security plan, now in place, should be considered for up-grade, but the possibility of totally scrapping it in favor of an entirely new collaborative security plan should remain a viable option. The existing cyber plan, if there is one, must be examined for any new known flaws and the assigning procedures for passwords etc. must become much more sophisticated. OSL (Operational Security Levels) must be established and integrated into the operating parameters of the process control function. In the short term, an interim plan that takes advantage of existing strategies is a possibility but at the very least, biometrics should be considered now where they don't exist and the use of CCTV should be expanded to include areas from the corporate offices to the control room.

Michael St. Angelo is the CEO of NeuraMetrics, Inc. a consulting company dedicated to business improvement through the implementation of best practices and creative assessments. He has taught undergraduate courses in marketing and has held sales and marketing management positions with a process control company, an analyst firm, and was the Vice President of Sales and Marketing for a Boston based software company. Mike was a principle in The Lincoln Identification Company, a company that marketed fingerprint identification products to police agencies and he also held the position of Police Commissioner for three years in New Jersey where he was

instrumental in establishing building security checking procedures for the department. He can be reached at 904-46-9733

This article appeared in the Summer 2003 issue of the ISA Management Division Newsletter, an official publication of ISA -- The Instrumentation, Systems, and Automation Society.