Staying Safein Cyberspace:What You Must Do

Cyber Security Program spokesman stresses importance of shoring up chemical facilities' business and process systems

Tom Good, Chemical Sector Cyber Security Program spokesman By Joy LePree It's a dreadful feeling when you realize your home computer has succumbed to a virus. It's even more upsetting when you discover that your e-bay password has been "borrowed" and used to win a pricey item that was paid for courtesy of your stolen PayPal account information. Now, imagine similar, but larger scale, computer hacking and what it could do to a typical business. Think of the ramifications it could bring to a large chemical company where business and operations include propriety information and process secrets that are prime targets for theft. This makes it essential that the chemical industry, as a whole, enhance the security of computer systems that control traditional business processes as well as those that control plant operations. For this reason, the Chemical Sector Cyber Security Program was organized and created by an executive team from a handful of large chemical companies including Dow Chemical, DuPont, Rohm and Hass, Celanese, Albemarle, and Eastman Chemical in March 2002. Since then, it has expanded to include more than 20 major chemical companies from the U.S. and abroad and is operating under the Chemical Information Technology Council (ChemITC), a ChemStar Panel of the American Chemistry Council. The Chemical Sector Cyber Security Program is an industry-wide initiative that addresses cyber security in information systems and manufacturing control systems in the chemical sector. Tom Good is the steering team sponsor of the program's Manufacturing and Control Systems Security Team as well as a project engineer with DuPont Engineering's Electrical, Instruments, and Control Systems' section. In this interview, he provides an update on the program and offers advice to CHEM.INFO readers. Q: What is the Chemical Sector Cyber Security Program? A: As a whole, the program is really an initiative of bringing people from the chemical industry together to try to help each other operate our facilities in a safe and secure manner. As a group, we want to facilitate business continuity and information protection as well as reliable delivery of products and services. In the chemical industry, we buy and sell a lot of products amongst ourselves, and we need to be working together to leverage the success and knowledge of the companies across our industry. Q: On what aspects of cyber security does the program focus? A: Typically when you think about cyber security, you think of IT and the security measures you can take for desktop systems. But we focus on the whole gamut of where information technology is used in a company. That includes manufacturing and control systems, business systems, and the value chain systems that interact with our partners such as transportation. Today's industry is a very integrated operation where manufacturing, business, sales, and other systems interact with each other, so we wanted to address security in a collective manner across all those systems. Therefore, we have a broad mix of people with different backgrounds involved in the project. We need to leverage the

knowledge and skills that various people can bring to the table to be sure all areas of concern are adequately covered. Q: Why is a cyber security program important? A: Because of the interaction with various chemical companies and the types of products made and used, we need to be sure that our supplies and products don't have a disruption in business continuity. We, as an industry, are working together and trying to leverage the experience and successes to overall improve and make our industry more robust and less likely to be impacted by a cyber incident. Q: What are the risks of not having a cyber security program? A: Typically, security programs are focused around aspects of security such as confidentiality, integrity, and availability. When we talk about confidentiality, it's important that information is kept internal to a company. A big financial impact could occur if there's an incident regarding the loss of proprietary information. Integrity and availability, specifically when you get into manufacturing, have an even larger impact than confidentiality. That's why these two areas are the motivating and driving issues around security in manufacturing. We require 100 percent uptime of our process control systems. We need those to be functional 24/7, 365 days a year to safely operate our facilities and provide products within our manufacturing specifications. A cyber incident like a virus getting in and impacting the operation of one operator station could take that station off-line and make it unavailable to the operator to view what's happening in a process. Even on a scale as small as one operator station, it could have a major impact on a company. Q: How can chemical engineers start a cyber security program within their own facility or company? A: There's a general tendency to add things like anti-virus software and patching processes to a process control system. But what really needs to be done is to develop a whole cyber security management system. That system should deal with organizing for security, assessing the risks of systems and processes, and addressing those risks in an organized manner via policy and security controls. Once the appropriate controls and solutions are implemented in a facility, a monitoring and improvement phase should come next. It should include conducting audits to make sure the tools that were put in place are achieving the objectives and goals. I suggest that companies address security as a continuous process of system management, not just apply Band-Aid controls. Guidance is available through the public areas of the Chemical Sector Cyber Security Program including the elements of setting up a program, working within the culture of your company, and trying to develop, structure, and organize a team to address cyber security. My best piece of advice, however, is that chemical engineers and manufacturing process engineers need to work together with IT professionals at the company to improve security. It's not just an IT problem or a manufacturing problem, so trying to maintain two separate sets of practices, procedures, and programs isn't going to work. *Joy LePree is a contributing writer for CHEM.INFO. She has worked as a journalist for 14 years, covering a variety of issues and trends involving chemicals, processing, engineering, and maintenance.*