



B U S I N E S S R I S K L E A D E R S H I P

April 9, 2009 www.csoonline.com

Taking a Lesson in Federal Compliance from the Chemical Industry

Honeywell's Jon Harmon says the industry's response to CFATS provides a model for compliance with stringent federal security requirements.

By Jon Harmon, Honeywell Process Solutions

In many ways, the role of the CSO is directly tied to business profitability. By creating and enforcing policies that protect human, physical and intellectual assets, the CSO ensures the very integrity of the organization. This link to the bottom line, though, is about to become much stronger—and quite possibly much sooner than anticipated.

Events occurring in the U.S. chemical-manufacturing industry, specifically those relating to security guidelines being enforced by the federal government, are likely foreshadowing what's next in line for other industries.

In 2007, the Department of Homeland Security (DHS) introduced the Chemical Facility Anti-Terrorism Standards (CFATS), a rigorous program designed to protect high-risk chemical facilities from attacks. The legislation mandates that sites identified as "high-risk facilities" implement solutions, under the guidance of Risk-based Performance Standards (RBPS), to address gaps in safety and security. Under the new Congress, there will likely be additional issues addressed that may intensify the requirements, such as the need for inherently safer technologies (ISTs) and state and local interpretations related to enforcing compliance.

The penalties for non-compliance can range from hefty fines to total plant shutdowns. Under this scenario, the CSO of today's chemical plant has never had more responsibility riding on his/her shoulders.

The chemical industry is just one of the critical sectors impacted by DHS regulations. And it's very likely that CSOs across various industries - water treatment plants, port facilities, educational and banking facilities, etc.—are/will have to deal with federal compliance issues. With this in mind, it's critical for CSOs to begin evaluating their purchasing behaviors immediately and identifying technologies that create a holistic security solution under the possibility of future enforcement.

So how can a CSO truly prepare his organization for a "new normal" with stringent regulations?

What to Expect

For starters, CFATS was one of the first pieces of legislation that successfully motivated chemical facilities to develop site vulnerability assessments (SVA). The premise of an SVA is quite universal in that before a site's security systems can be bolstered, the site must first understand its existing weaknesses or gaps. SVAs are designed to find those existing gaps in everything from

physical security, cyber security and life-safety systems. Additionally, the SVA also prioritizes the shortcomings by determining which gaps could cause the greatest impact to the plant and surrounding community.

An SVA can take about a month or so to complete and the next step in CFATS compliance—the creation of the actual site security plan (SSP)—can take much more time. Creating an SSP requires substantial effort, focus and organizational support and often requires the assistance of expert consultants outside the organization to help understand and meet the regulation.

While CFATS is aimed specifically at facilities that use, transport, store or produce certain chemicals and other potentially hazardous materials, there are several requirements in the legislation that could be modeled for other industries. These include screening tools developed by DHS (TOP Screens), SVAs, SSPs and implementation of solutions.

Using Today's Technology for Compliance

Technology can play a key role in easing the burden of complying with federal regulations. In the case of the chemical industry and CFATS compliance, some facilities have elected to take an integrated approach to securing their facilities. This differs greatly from the traditional model where plant operations and security personnel operated independently of one another without much transparency.

For instance, integrating video surveillance and access control systems to a plant's process control system allows operators to visually validate incidents in the command and control room. This is beneficial because the operator can be quickly alerted if an intruder has breached a critical area of the plant. The operator can then take appropriate action, such as dispatching authorities, locking down further access or shutting down a potentially hazardous process in the affected area of the plant and alerting field personnel to move to a safe location. Conversely, this approach also is beneficial to plant security personnel. If a process involving volatile and hazardous materials spirals out of control, security personnel can better coordinate with first responders.

In a manufacturing setting, integrating security with process control and business systems offers a best-in-class solution that provides the most comprehensive protection. In addition to keeping track of assets, an ideal solution, when implemented effectively, will be able to:

- Identify and control who enters and exits the plant
- Track movement of facility occupants
- Control access to restricted areas
- Track and locate equipment, products and other resources
- Track location of onsite personnel in the event of an incident
- Protect process automation networks and systems from cyber threats
- Respond proactively to alarms and events
- Share data to generate costs savings

This integrated approach has long been considered as an effective means for securing critical infrastructure. The rise of regulations such as CFATS, however, has broadened its acceptance in the chemical industry. This is due in part to DHS language that specifically points out that merging an active security system with life-safety technology may facilitate a common set of operational procedures and prove a more cost-effective approach to overall facility security and security management.

This represents another area of CFATS that could potentially be broadly adopted across various vertical industries—bringing together security and operations technology on the same platform can lead to synergies that ultimately create a stronger security shield and greater collaboration between once-disparate departments.

The CSO's Evolving Role

Probably the most important thing for CSOs to remember in a climate heavily influenced by federal mandates is that they cannot help achieve compliance alone. The CSO must have an accurate picture of all the internal resources available to establish processes, form teams and identify solutions that drive compliance and help preserve or enhance the bottom line. Externally, this means CSOs will need to investigate technologies—including video surveillance, access control, perimeter detection and command and control—that can be integrated to a common platform for better domain awareness, improved reaction time and reduced operator training.

Taking these steps can help lead to an overall reduction in the cost of compliance, especially considering that the cost of poor planning - or worse yet, inaction - will almost certainly lead to hefty fines.

Jon Harmon is Global Director of Critical Infrastructure Protection for Honeywell Process Solutions