SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Overcoming Challenges, Finding Unexpected Benefits in CFATS

Marleah Blades

Originally Published in Security Today

April 2010

Overcoming Challenges, Finding Unexpected Benefits In CFATS

The Chemical Facility Anti-Terrorism Standards are complex and fairly disruptive. Few would argue that. The risk-based performance standards guidance alone is nearly 200 pages long, and many companies have had to re-allocate or hire staff, facilitate training and certification, and contemplate ways to re-imagine corporate processes in order to control access to chemicals of interest.

However, when all is said and done, regulators and most of the regulated seem to agree that the standards should lead to the shoring up of potential vulnerabilities that, before CFATS, often went unaddressed.

When will all be said and done? It will probably be a while yet, since as of this writing more than 2000 top-screened organizations haven't yet received their tier letters from DHS, and even Tier 1 companies are still in the process of receiving approval for and implementing their site security plans (SSPs).

Whether you've only just discovered your company's risk tier or whether you're embarking on the final phases, it may be helpful for you to consider that there may be unnoticed benefits behind the challenges of CFATS. Members and faculty of the Security Executive Council recently shared their thoughts on some common CFATS compliance challenges and how they've overcome them, as well as some tips on where to look for those hidden benefits.

Who's the Boss? Who owns the CFATS compliance process? Who's responsible for managing it? It's a DHS program, so should it be global security? Risk management? Or should it be environmental health and safety, or someone else entirely?

Assigning responsibility for CFATS is one challenge many organizations face, says Chad Wehrman, senior security manager, stewardship and global enterprises for Procter & Gamble, a member of the Security Executive Council.

“It’s very helpful to know how you’re going to be involved at the early stages, so you can understand who has the ultimate authority and who the primary point of contact is,” Wehrman says. “What I would recommend is determining up front who is going to be responsible for compliance, leadership and ownership of the program.

“At P&G, we’ve worked through an internal process to determine that global security should play an active role, and we have identified others within the company who can answer the technical questions pertaining to the chemicals as we go through the process.”

Procter & Gamble manages compliance centrally from its headquarters. One staff member dedicates about 10 percent of their time to monitoring and tracking compliance stages at the company’s various regulated sites, and there are several security managers trained to perform security vulnerability assessments (SVAs) and develop SSPs.

Oilfield services company Baker Hughes takes a slightly different approach to managing compliance, according to Jose Olivarez, the company’s vice president of security, Western Hemisphere, also a Security Executive Council member.

In 2009, he hired a new team member specifically to address CFATS.

“This new global, physical and regulatory security manager leads our compliance efforts and is responsible for SVAs and methodology, and ensuring that the minimum security standards not only of CFATS but of Baker Hughes are met at any facility we have around the world,” Olivarez said.

Regardless of which functional unit holds primary responsibility for compliance, it’s crucial for the responsible function to bring in assistance and advisement from other business units, George Miserendino, owner of Triton Security Solutions and Security Executive Council faculty said member.

Miserendino has consulted with numerous companies working to achieve compliance. The former director of corporate security for Excel Energy, he has also worked with the Edison Electric Institute’s Security Committee on CFATS issues since the drafting of the standards. “The best way to

approach (the compliance process) is with a cross-functional team that consists of physical security, environment, safety, site operations, and maintenance," he said. "That's the best model I've seen."

Internal Communication and Time As part of CFATS, DHS has implemented an information protection regime called Chemical-terrorism Vulnerability Information (CVI), which limits what information can be shared about regulated companies and their compliance processes, and with whom.

While valuable, the limitations of CVI can make internal communication difficult if they're not handled early on, Wehrman said.

"We can't discuss specifics with anyone at any of the sites unless they've been through CVI certification," he said, so ensuring that all affected parties are certified before site visits begin is crucial for communication and saves time as well.

"We have to travel to each site and spend a day reviewing the facility prior to sitting down and completing any of the paperwork, because we have to understand the chemical, where it's housed, how it's protected, whether we need to add any safeguards, and whether we believe we'll be compliant with the current status," Wehrman said. "So the site visits are sometimes several days long, and we've found we have to have a team of people that will answer all the questions during the visit. Not just the security manager and the local security contact at the site; we need to have experts in IT, risk managers, environmental health and safety managers, and site chemical owners, and they need to be actively involved. So gathering the team together, scheduling the time and making sure everyone is CVI certified before we arrive can make a lot of difference in the efficiency of the site visit."

Wehrman also notes that there is other "pre-work" that can be done before the visit to save time and ease the process, including mapping and logistical questions regarding the facility.

Dealing with the Government Maintaining strong communication with DHS representatives during the compliance process is not always easy, but according to Miserendino, it is key to an efficient compliance process.

Regulated companies aren't the only ones under a heavy workload with CFATS. DHS is dedicating staff to analyzing top screens, evaluating and approving SVAs and SSPs, running help desk, and conducting regular audits and inspections. Sometimes communicating with the DHS field representatives poses a challenge.

"The important thing is ensuring we develop and foster a relationship with our contacts at DHS," Olivarez said. "We do so through one-on-one sessions, being leaders and participants in security sessions and panel discussions, and being actively involved in our industry to ensure our voices and those of fellow constituents are heard for the benefit of the entire industry and the program."

Persistence is key when communication is difficult, Miserendino said. He recommends calling DHS contacts several times to give them an opportunity to respond. If response still doesn't come, e-mail the CFATS Help Desk and request the name of the regional CFATS supervisor.

Hidden Benefits

As promised, if these and other common challenges can be overcome, CFATS-regulated sites may be able to turn their work on the compliance process into unexpected gain for their companies. There are many side benefits to CFATS compliance.

Regular drills and exercises. CFATS RBPS 11 stipulates that companies conduct regular training commensurate with their level of risk.

"I think that's one of the best parts of the risk based performance standards," Miserendino said. "We've been encouraging annual training, drills and exercises to validate the training, as well as having formal lessons-learned and incorporating those lessons into the procedures. It's the basis of continuous improvement."

Better background checks. RBPS 12, personnel surety, requires background checks and appropriate credentialing for staff, third parties and visitors.

"I think they'll get a better caliber of employee because they'll be doing rigorous background checks," Miserendino said, highlighting a solid business-enhancing byproduct to a basic security requirement.

Potential to improve future compliance efforts. Olivarez of Baker Hughes is using the CFATS compliance process as the jumping-off point for a new Regulatory Center of Excellence.

"I saw this coming down the road," Olivarez said. "The U.S. and our industry are beginning to be more and more regulated on different fronts, not just chemicals, but in transportation of hazardous materials and other areas of our business." The new manager Olivarez hired to head up CFATS compliance has a future-forward business plan of dealing with global compliance issues proactively for whatever comes next down the pike.

Internal checkup. As frustrating as CFATS compliance may be for some, it requires all regulated organizations to carefully evaluate their own processes and methods, which is something all companies should do from time to time.

"You never should get too comfortable," Olivarez said. "The intense scrutiny that you put your facilities through forces you to look at things through a magnifying glass. Items that we may not have considered problematic in the past have been identified with clarity, and it's helped us evaluate the fitness of our methodologies and approach to risk analysis."

Wehrman said he agrees with Olivarez.

"We had secure controls in place, but they may have been site specific instead of focusing in on a specific chemical that could be construed as a threat," he said. "And we can re-apply those learnings to additional facilities outside of the U.S. We can apply this standard to all our facilities globally."

Better seat at the table. "When you deal with these kinds of complex programs, you can't do it in a vacuum," Olivarez said. "and the synergies you find when you bring other functions into the fold helps you enhance your security programs. We've been able to demonstrate value-add back to the business because in a couple of sites we've been able work with site management to improve the operations and processes to reduce chemicals of interest.

"Now our professionals are not just talking about just security, but how we operate the business."

Special thanks to George Miserendino (solutions@tritonsecsol.com), who provided significant material support for this article.

Marleah Blades is former senior editor for the Security Executive Council, a problem-solving research and services organization that involves a wide range of risk management decision makers. Its community includes forward-thinking practitioners, agencies, universities, NGOs, innovative solution providers, media companies and industry groups. For more information about the Council, visit https://www.securityexecutivecouncil.com.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com