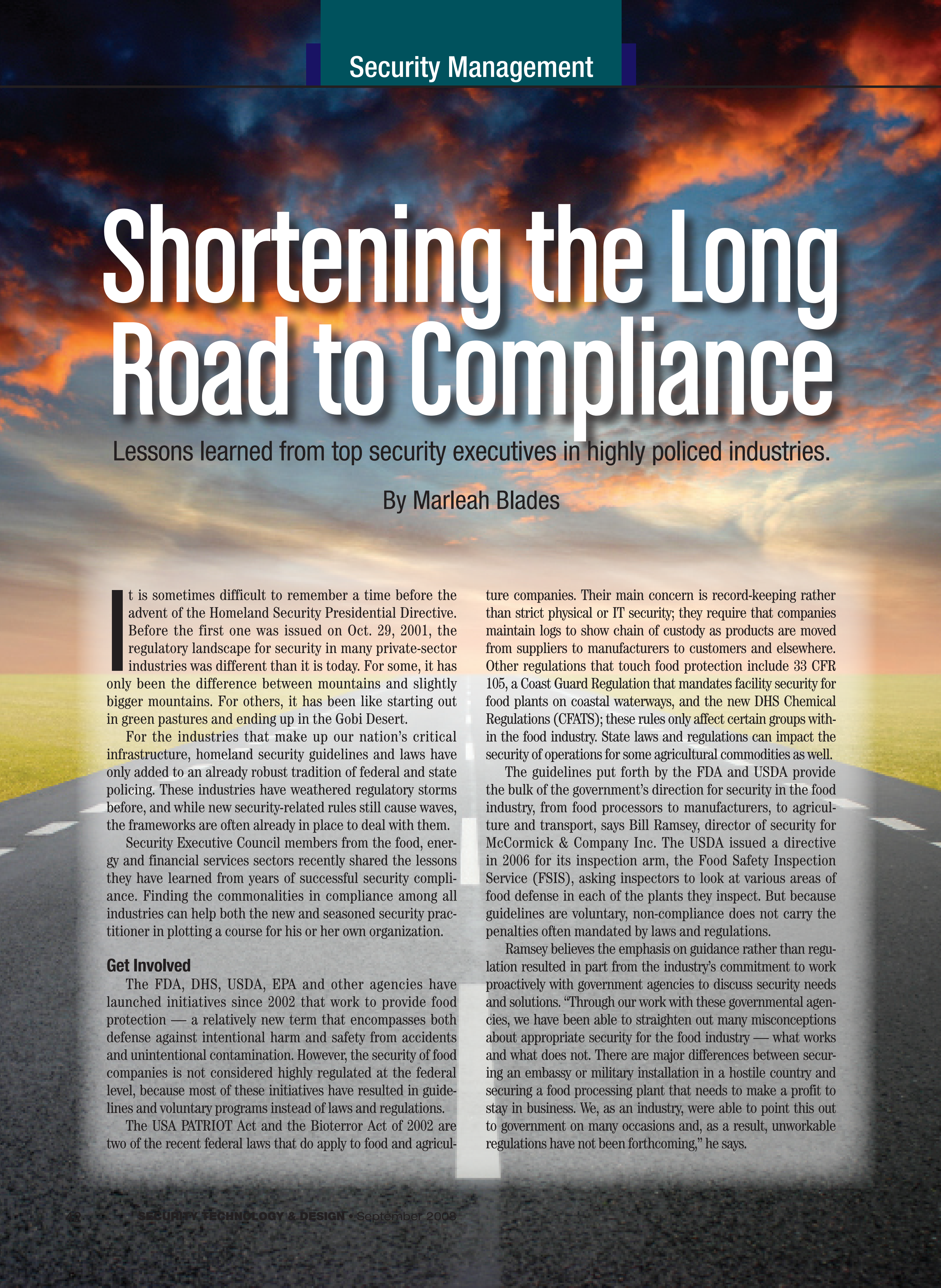

Shortening the Long Road to Compliance

Lessons learned from top security executives in highly policed industries.

By Marleah Blades

It is sometimes difficult to remember a time before the advent of the Homeland Security Presidential Directive. Before the first one was issued on Oct. 29, 2001, the regulatory landscape for security in many private-sector industries was different than it is today. For some, it has only been the difference between mountains and slightly bigger mountains. For others, it has been like starting out in green pastures and ending up in the Gobi Desert.

For the industries that make up our nation's critical infrastructure, homeland security guidelines and laws have only added to an already robust tradition of federal and state policing. These industries have weathered regulatory storms before, and while new security-related rules still cause waves, the frameworks are often already in place to deal with them.

Security Executive Council members from the food, energy and financial services sectors recently shared the lessons they have learned from years of successful security compliance. Finding the commonalities in compliance among all industries can help both the new and seasoned security practitioner in plotting a course for his or her own organization.

Get Involved

The FDA, DHS, USDA, EPA and other agencies have launched initiatives since 2002 that work to provide food protection — a relatively new term that encompasses both defense against intentional harm and safety from accidents and unintentional contamination. However, the security of food companies is not considered highly regulated at the federal level, because most of these initiatives have resulted in guidelines and voluntary programs instead of laws and regulations.

The USA PATRIOT Act and the Bioterror Act of 2002 are two of the recent federal laws that do apply to food and agriculture companies. Their main concern is record-keeping rather than strict physical or IT security; they require that companies maintain logs to show chain of custody as products are moved from suppliers to manufacturers to customers and elsewhere. Other regulations that touch food protection include 33 CFR 105, a Coast Guard Regulation that mandates facility security for food plants on coastal waterways, and the new DHS Chemical Regulations (CFATS); these rules only affect certain groups within the food industry. State laws and regulations can impact the security of operations for some agricultural commodities as well.

The guidelines put forth by the FDA and USDA provide the bulk of the government's direction for security in the food industry, from food processors to manufacturers, to agriculture and transport, says Bill Ramsey, director of security for McCormick & Company Inc. The USDA issued a directive in 2006 for its inspection arm, the Food Safety Inspection Service (FSIS), asking inspectors to look at various areas of food defense in each of the plants they inspect. But because guidelines are voluntary, non-compliance does not carry the penalties often mandated by laws and regulations.

Ramsey believes the emphasis on guidance rather than regulation resulted in part from the industry's commitment to work proactively with government agencies to discuss security needs and solutions. "Through our work with these governmental agencies, we have been able to straighten out many misconceptions about appropriate security for the food industry — what works and what does not. There are major differences between securing an embassy or military installation in a hostile country and securing a food processing plant that needs to make a profit to stay in business. We, as an industry, were able to point this out to government on many occasions and, as a result, unworkable regulations have not been forthcoming," he says.

Trade organizations and industry associations provide one of the best outlets for security professionals who recognize the need to collaborate with government for proactive security policies like these. They usually have government relations units that watch for talk of regulation, solicit information from members and the industry, and communicate the needs of the industry to the government. By remaining involved in these initiatives, security professionals in every field can ease their regulatory burden by ensuring that guidelines and regulations are reasonable and needed.

"The key ingredient for success in achieving compliance with myriad regulations is to establish working relationships with the major operational groups within the organization and to educate these folks on the regulations and the importance of compliance," Perman says.

Cover the Basics

Karl Perman, manager of corporate security programs for Exelon Corp., one of the nation's largest electric utilities, agrees that participation is key to the development of attainable regulation. Exelon Security team members are involved with the security sub-committees of both Edison Electric Institute and the American Gas Association and regularly meet to discuss the regulatory environment and best practices. "If we don't take on our own destiny by policing ourselves, someone else will write regulations for us," he says.

The energy industry has dealt with security regulation for some time and has longstanding rules under control. Perman says it is the emerging regulations that are consuming a lot of resources. Right now, that means the North American Electric Reliability Corporation (NERC) Reliability Standards for Critical Infrastructure Protection and cyber security. The compliance deadline for these standards is the end of the year. NERC's cyber security standards provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system. Says Perman: "They cover everything from physical security of critical cyber assets to background investigations for individuals accessing these assets — it's 'How You Do Security 101.' Exelon has a team of cross-functional people working on this. We have numerous security policies and procedures in place , and we're updating several of those based on these standards."

Despite these massive changes, Perman knows that Exelon is having an easier time meeting the compliance deadlines because the basic tenets of strong security are already in place. "If you haven't already completed the fundamentals on these, you've got big problems," he says. "If you've got the fundamentals, then at least you have started down the road to being compliant."

Across the board, executive and organizational support has also made compliance easier within Exelon. "The key ingredient for success in achieving compliance with myriad regulations is to establish working relationships with the major operational groups within the organization and to educate these folks on the regulations and the importance of compliance," Perman says. "A security compliance council is an excellent way to do this.

"It is key to socialize and determine the feasibility of an idea prior to engaging the senior executives," he continues. "I have found that if operations leaders are with you, then it is easier to win over the other executives. Most executives know that if you are the security leader, then you will be pushing security and compliance initiatives. But if someone in operations starts saying that they need to focus on a compliance issue, then the other executives in the room listen."

Security professionals must know their business and their compliance issues to be able to sell them to other operational groups, and each security director much choose the most appropriate way of establishing relationships and garnering support.

Gather a Support Group

The financial services sector has held up under rigorous security and information protection regulation for decades. Security professionals at banks and other financial institutions have adapted to many drastic changes in their regulatory environment, from the Bank Protection Act of 1968 and the Bank Secrecy Act of 1970 to Gramm-Leach-Bliley and the Guidance on Authentication in Internet Banking Environments.

"I would say the amount of regulation we deal with as a publicly traded financial services company is a significant piece of our business," says Stanley Jarocki, vice president of Wells Fargo. "There are dozens of regulations at the federal, state and international levels that we have to look at every day, and that's not even including privacy."

In banking specifically, there are requirements for recording and monitoring legitimate transactions of a certain size and transactions that appear suspicious, freezing accounts or blocking money movement to certain countries, managing fraud risk, developing business continuity plans, and managing financial risk and liquidity.

One might expect to find frustration in a security executive in such an environment, but Jarocki sees a positive side to all this regulation. "A lot of it is just an amplification of doing good business. I think that's an important thing to remember," he says. "We would do it anyway, because we want to offer our clients something of value. We do it because it's part of a good client relationship and partnership, and it's also tied to regulation."

Jarocki sees a trend of financial services companies bringing compliance, risk management, security, and privacy under a single umbrella — and security often takes the lead. Even in organizations where one executive does not have responsibility for these areas, a team approach is extremely important, Jarocki says. An information security council, for example, should not involve just information security personnel. The issues of information security also deal with privacy and risk management — representatives with those responsibilities must be involved as well. Then, individual business units must be made aware of their own responsibility for maintaining security in the organization and should be encouraged to take ownership of their role in security.

Common Areas in Security Regulation

Participating in regulatory initiatives, maintaining security fundamentals, building effective relationships and developing cross-departmental teams have helped executives in some of the most highly policed industries ease their compliance burdens. Another way to facilitate compliance in any industry, whether heavily regulated or not, is to identify common elements among applicable guidelines and regulations. When an organization attempts to comply with regulations one at a time, it may end up duplicating efforts to address concerns that appear in more than one. By identifying commonalities ahead of time, the organization can deal with common issues at once, sometimes with a single process or solution, saving time and money.

The Security Executive Council maintains a large and growing list of laws, regulations, voluntary compliance guidelines and standards (LRVCS) that impact security. (To view the current list and propose new rules for inclusion, visit https://www.securityexecutivecouncil.com/public/lrvc). After extensive cataloging and research of these LRVCS, the council has identified more than a dozen major categories that most requirements or controls (options recommended by guidelines for voluntary compliance) fit under.

For example, if we look at a selection of laws and guidelines such as ISO 17799, NFPA 1600, NIST Special Publication 800-53 Minimum Security Controls (Low, Moderate and High Baselines), the NERC Critical Infrastructure Protection cyber security standards, and PCI, we can find nearly 100 requirements or controls that can be categorized as specific to business continuity management. Similarly, we can find common governance issues in the Maritime Transportation Act, SOX, the U.S. Federal Sentencing Guidelines, HIPAA and NFPA 1600, among others. Additionally, many of the laws and guidelines already evaluated include considerations for security awareness and training. It is unlikely that any single business would need to comply with all the laws and guidelines cited in these examples, but if an organization can find common elements between even two of the LRVCS that are relevant to it, the cost and time savings can be significant.

By evaluating these common areas in their own organizations, security executives and other security professionals could put themselves several steps ahead of new legislation waiting down the pike.

Whether regulatory compliance is your biggest concern or the last item on your priority list, guidelines and regulations with security implications will impact your organization. Heeding the advice of those who have already been there will make that long and winding road a little easier. To find out more about the Security Executive Council's LRVCS research, contact contact@secleader.com. ST&D

Marleah Blades is Senior Editor for the Security Executive Council (SEC). The SEC is a member organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of members' programs, making program development more efficient and establishing security as a recognized value center. For more information and inquiries on membership, visit www.securityexecutivecouncil.com/?sourceCode=std.