Surprise! We're Regulated!

Compliance rules affect most organizations. How do they impact yours? What can you do to comply?

By Bob Hayes and Marleah Blades

In the July issue of *Security Technology & Design*, we discussed the growing mountain of security legislation, regulations and guidelines and what you can do to influence the creation and passage of new rules ("The New Rules of Security," p.24). But what of the rules already in place? How can you keep track of them, how might they impact you, and what can your organization do to comply cost-efficiently?

The answers to these questions will vary based on the nature and culture of the organization, but all effective solutions share one vital element: a unified, enterprise approach to risk.

Be Aware

When the Security Executive Council (SEC) was launched as the CSO Executive Council in 2005, its research showed that legislative and regulatory compliance was one of the top three issues for senior security executives. Since then, security leaders' concern about compliance and regulation has grown in tandem with the wave of legislation.

Elizabeth Lancaster Carver, member services and projects manager for the council, says: "What concerns security executives the most is the challenge to be compliant with each law without wasting precious human or capital resources due to varying requirements for similar controls. That is to say, access control requirements for C-TPAT, federal sentencing guidelines and PCI could all apply to one company, yet the controls vary significantly, and the challenge is to implement one control that will meet the requirements for all three." The SEC members pictured on the cover of this month's issue have all struggled with compliance, and they all recognize the immense challenges that often stand in the way.

The increase in security-specific regulation has been accompanied by an increase in non-security regulation that contains security components. To get an idea of the depth and breadth of this increase, visit the Security Executive Council's library of laws, regulations, voluntary guidelines and standards at www.csoexecutivecouncil.com/public/lrvc.html/?sourceCode=std. This library is updated constantly and continues to grow at a rapid pace.

Whereas many CSOs are aware of the security-specific rules coming down the pike, they may not be as familiar with the security aspects of non-security rules, and in some cases they are completely unaware of the impact such rules might have on their organizations.

You can increase your own awareness of new laws and regulations in one or all of the following ways: One way is to increase your participation in industry groups and associations, which keep tabs on such issues for their membership and sometimes offer tools and advice on how to comply.

A second option is to use tools specifically intended for security executives, regardless of industry. For instance, as mentioned in last month's article, the Security Executive Council has created a tool to help member organizations identify, track and comply with security-significant laws, regulations and guidelines. "One of the main ways we found members using the tool is to bring in their colleagues who are also dealing with regulations and compliance to work on the project together," says Kathleen Kotwica, the council's vice president of research and product development. "Although the tool is specific to security requirements and controls per member requirements, we have had requests to extend it to the entire regulation. We are currently trying to load as many regulations and guidelines as possible, including by industry. This allows our members, for example, to examine if a standard currently used in the organization also fulfills the requirements of another regulation and where the gaps are."

A third way to increase your awareness is to read industry publications like *ST&D*, which is partnering with the Security Executive Council to publish regular updates on compliance issues and expert commentary on laws that may impact you in our monthly Compliance Scorecard column.

The fourth option is to use internal company resources to ensure not only that you know about rules that will impact or are impacting your organization specifically, but also that you are involved in the planning and implementation of compliance strategies. To accomplish this level of awareness, you must be part of a corporate team that examines and approaches risk as one unit, with overall business goals in mind. If your company has no such team in place, even your own personal awareness will not be able to save you from the potential consequences.

Some of the nation's top CSOs met at a recent International ISMA conference. Pictured from left to right are Paul Herring, Wm. Wrigley Jr. Co.; Bill Duggan, Kellogg Company; Joe Murphy, Motorola Inc.; Pat Laird, Exelon Corp.; Jim Hutton, Procter & Gamble; Chris Berg, Novartis; Mark Farrell, Comcast; David Quilter, CSO Emeritus Faculty; John Mallon, SC Johnson & Son Inc.; Jim Ashby, Boise Cascade; Tim Janes, Capital One; Nick Proctor, British American Tobacco; Steve Bernard, Sony Pictures Entertainment; Frank Rodman, Ziff Bros. Investments; Bob Hayes, CXO Media/IDG; Terry Luddy, Medtronic Inc.; Don Hubbard, Pricewaterhouse Coopers LLC; Lynn Mattice, Boston Scientific Corp.; David Burrill, CSO Emeritus Faculty; Bob Brand, Cox Enterprises; Lou Alexander, Philip Morris Intl.; and Don Bitner, AMGEN

The Impact of a Non-Unified Approach

Often, corporations consider laws and regulations to be primarily the concern of only one business function. For instance, the Health Insurance Portability and Accountability Act (HIPAA) is often considered only an HR or IT law; Sarbanes-Oxley (SOX) a financial law; and the Foreign Corrupt Practices Act (FCPA) a sales or supply chain law. But each of these laws has an important security component. In such cases, security is often the last notified or the last brought into the planning and compliance process — if it is brought in at all. When the security department is not deeply involved in or consulted about a company's implementation of these laws, the impact can be significant.

The most likely problem to come out in this situation is a collective impression that someone else is taking care of the security concerns, when in fact, no one is. Then, when the company is one day caught in breach of the security portion of the rule, everyone turns around and points the finger of blame at the security department, even though security was never included in compliance planning.

The biggest concern at the corporate level is SOX, and the biggest concern at the security level is whatever the top industry guideline is – CIP for electric utilities, PCI or GLB for financial institutions, or HIPAA for healthcare or insurance, for example.

The same results can come about if the overall compliance effort is inclusive but disorganized, or if the planning process engenders turf wars among the heads of different departments. And don't forget, the security department is not always the victim here. When legislation is security-specific, it is just as important for security to include other impacted players in the planning process, or the result will essentially be the same: organizational failure to consider all the aspects of compliance.

If you think this is not a problem in your organization and that such disorganization and lack of unity cannot be widespread, consider this. At the SecureWorld Expo events being held across the country, the Security Executive Council has been teaming with *ST&D* to hold focus groups on regulatory compliance and Unified Risk Oversight. At all of these focus groups, two questions are asked: 1. What is the number-one regulation of concern for your corporation; and 2. What is the number-one regulation of concern for your security department? Invariably, the biggest concern at the corporate level is SOX, and the biggest concern at the security level is whatever the top industry guideline is — CIP for electric utilities, PCI or GLB for financial institutions, or HIPAA for healthcare or insurance, for example.

At the corporate level, SOX is burning up everyone's energy and attention, and this seems to be leading to a lack of focus on other concerns. In the same way, security departments are so focused on industry regulations that the corporation's main business concern is not of top interest to them. This appears to speak to a widespread lack of unity.

Unified Risk Oversight

The only way to effectively comply with the mountain of legislation, regulation and voluntary guidelines — let alone to ensure cost-effectiveness in compliance — is to approach it in the context of Unified Risk Oversight.

Unified Risk Oversight is a method of approaching risk whereby the corporate risk is identified by a team of executives or managers who represent the company's various business units, then managed with the best interests of the business and its goals in mind. By "corporate risk," we mean not just the compiled risks of individual business units, but the new risk picture created when different departments' risk considerations are brought together and compared, combined and prioritized.

A quick note here on terminology: Unified Risk Oversight does sound similar to another popular term, enterprise risk management; however, there is one crucial difference: oversight. While ERM identifies all risks that may impact the corporation at the board level, Unified Risk Oversight is about who or what entity is watching over it all. It calls for one centralized overseer, a component not necessarily an integral part of enterprise risk management.

When risk is managed by the URO method, all decisions to transfer, avoid, mitigate or accept risk are made in full consideration of their impact on all business units. Of course, this means not every decision will reflect what you may feel is the best option for security, but every decision will take security into account and seek to provide the best possible outcome for the business as a whole.

If you look at the impact of non-compliance as a huge risk to the organization (a viewpoint borne out in the headlines on a regular basis), then enterprise regulatory compliance efforts fit precisely into the Unified Risk Oversight framework.

Cutting Costs by Joining Forces

If there is not such a framework in place, the most important part of creating one is getting senior management buy-in. In many organizations it is not a hard sell; in fact, many of the businesses that already use URO use it because the CEO drove the change from the top down. However, where URO is not already a management concern, you will need to make it one, and money is a good place to start.

Unified Risk Oversight saves money. For one, it can eliminate the gaps in compliance planning and implementation that allow breaches to occur — that is, it eliminates that collective idea that someone else has the ball. With Unified Risk Oversight, because all business units are involved in planning, all departments should be able to look at the compliance process and know exactly what is expected of them and of everyone

> By bringing together all business units to plan overall compliance strategy, you will avoid costly duplications of effort.

else. Now, this cost savings is technically theoretical — by being proactive, you are saving money that has not been lost yet. Security executives know this angle can sometimes be a tough sell in organizations that have not experienced catastrophic loss in the past. So there's another savings to point out as well.

By bringing together all business units to plan overall compliance strategy, you will avoid costly duplications of effort. If two departments are working to comply with different standards, all of which require a similar level of access control, for instance, and they are not talking to one another throughout the process, they are quite likely to miss valuable opportunities to leverage one system or process for the benefit of both. But when they are part of an oversight team discussing each standard from the beginning, they will see that with this single access control system or process, they can kill two birds with one stone, slicing the cost of compliance in half.

Four Steps to Achieve URO

Once you have received support from management and created a team of your peers from other business units, how can you use URO to manage compliance, and what might your process look like? The process for managing compliance through URO is actually quite simple.

1. See what regulations apply to your company. You can do this most effectively by using all three of the methods listed at the beginning of this article: checking with industry associations, using non-industry-specific tools, and conferring with the other members of your URO team, including the legal or government affairs department, to compile a complete list of applicable laws, regulations and guidelines.

2. Prioritize the rules and their concerns by exposure and risk. We recommend that security be the URO team leader whenever possible, because this step should be intuitive for them, whereas other groups are not familiar with assessing and prioritizing risk as a basis of their work. Unfortunately, many security departments have the well-deserved reputation of preferring to work alone, and if they cannot overcome that propensity, they are probably not a good choice as team leader. A loner philosophy just does not work well in cross-functional teams.

3. Identify the stakeholders and get them involved. In any given compliance initiative you will have numerous departments that will potentially be impacted. Make sure they all have a voice. Sometimes this group will include almost every staff group and every business function — corporate security, IT security, legal, compliance, business conduct and ethics, human resources, the business units themselves, environmental and safety. In order to ensure you are including everyone who needs to be included, you will have to carefully review your organization, the rule in question, and your industry.

For an example of how URO might pan out in reference to an actual cross-functional law, consider its impact on the implementation of Title 18 of the U.S. Code, on federal sentencing guidelines. In this situation you will need to have business conduct and ethics and maybe HR monitoring a reporting hotline and audits; executive management overseeing notification of the audit committee and the board; legal and security dealing with investigations; perhaps communications interfacing with the public; shareholder services monitoring progress; and if the issue at hand is a regulatory problem, you will have government affairs heavily involved.

That's a lot of departments to work with and consider, but without input from each, you will be missing a critical element of compliance or enforcement and putting the business at risk of significant loss.

4. Rely on ST&D and the Security Executive Council to keep you informed. Check back each month for a new Compliance Scorecard and for regular legislative and regulatory coverage that draws on the experience of council members and faculty, leaders of world-class security programs, to help you find the most effective path to compliance.

This article is based on the collective knowledge of Security Executive Council members, faculty and staff who are committed to sharing their experience in world-class security programs for the benefit of others and the security profession. For information about the Security Executive Council, visit www.csoexecutivecouncil.com/?sourceCode=std.

The council's list of legislation, regulations, and guidelines is lengthy but incomplete. If you submit to the council a law, regulation or guideline with a security component that is not currently on the list, they will provide you a free $50 metric tool for your participation. For information, visit www.csoexecutivecouncil.com/public/lrvc.html/?sourceCode=std. **ST&D**

Bob Hayes is Managing Director of the Security Executive Council, a cross–industry professional organization of security executives devoted to advancing strategic security leadership solution. He also serves as chief security officer of CXO Media Inc. and its parent company, International Data Group. Mr. Hayes has more than 25 years of experience developing security programs and providing security services. Prior to joining CXO, he spent eight years as the CSO at Georgia Pacific and nine years as security operations manager at 3M.

Marleah Blades is senior editor for the Security Executive Council. Before joining the council she served six years as managing editor of Security Technology & Design magazine.