

Master the Compliance Sale

Sellers of information security technology benefit from compliance momentum, but it's still an asset-focused sale

By David Stelzl, CISSP

How many projects have you sold this year based on some federal regulation?

Compliance has created awareness, but it's the need to safeguard assets that closes the deal. For the last seven years, leading technology companies have consistently told technology resellers the security market would explode with compliance opportunities. But only deals that focus on relevant risks to data and that demonstrate the reality of pending threats, result in new business opportunity. Leveraging compliance goes a long way, but finding the high impact connections to asset owners is what justifies spending money.

Law and Order

There's momentum in the compliance industry. You may not see it, but laws are changing and new regulations will soon be enforced. PCI regulations are undergoing an overhaul, and a newly formed standards council will establish gold standards. (New members include Walmart, Bank of America and Microsoft.)

Laws like California's SB 1386, which regulates how companies must report the theft of personal information, are spreading to other states, serving as catalysts for legislation like Virginia's recently passed cyber-security bill. Proposed bills like AB 779 impose basic data-protection standards on companies that retain customers' credit- and debit-card information, forcing companies to cover the costs of reporting breaches and issuing new cards. Just ask banks that had to shell out hundreds of thousands of dollars in the wake of TJX's breach of 45 million customers' data.

Don't fall into the trap of believing regulatory compliance has no value to the security sales opportunity. The reverse is true. However, it is not the IT staff that is impacted, and therefore the IT staff is not the buyer. Focus on three key areas with data owners and you will likely gain new traction in your sales process:

- Due care requirements
- Information life-cycle management
- Security policy

Due Care

I frequently hear salespeople discuss due diligence—but not due care—when promoting information security. There’s a huge difference: Due diligence may be simply defined as an assessment process. Due care, by contrast, is more closely aligned with liability. You can assess all you want, but until you’ve taken reasonable steps to secure data, you haven’t demonstrated due care.

Due care is the data owner’s ultimate responsibility—not the administrator’s. Legally, the administrator serves as a custodian, but the data owner must ensure it’s truly secure. While these individuals usually have nontechnical backgrounds, auditors consider them the responsible, liable parties. This means taking reasonable steps to secure data.

During the sales process, it can be difficult to untangle all of the business requirements related to systems and data. Instead, move the conversation to due care. You’ll need to determine: Is the data reasonably safe? Has the company enacted adequate access-control measures like encryption? Is the IT department capable of restoring data and maintaining accurate reporting and archiving?

These concepts apply regardless of which regulation we’re reviewing. Most require similar security steps on the infrastructure side.

Information Life-Cycle Management

Information life-cycle has more to do with security than with different types of media. Information is created through various applications (email, IM, database entry, spreadsheet, Word document), at which point it becomes a new digital asset.

While a physical asset may be stored in a specific location, digital assets present a paradigm shift. Sure, there are data centers around the country with biometrics to protect against unauthorized entry, cameras, guards and other protective measures. But data doesn’t “live” in the data center anymore. In reality, live data is everywhere – in the air, on PDAs, Laptops, and traveling through Internet email around the globe.

Stolen information can travel around the world faster than any stolen merchandise and resale to run-of-the-mill criminals and organized crime occurs in seconds via chat sessions and portals.

Security Policy

Policy drives the architecture and limits a company’s liability—and as a legal document, company officers must sign off on it. At each stage of the information life-cycle, new security issues come into play, and following regulations is paramount. Almost every regulation calls for some policy changes. What used to be “extras” have graduated to necessities.

When data is created, for example, it must be classified based on how it will be treated throughout its life-cycle. Storage may be necessary, including the ability to recall data like email. Transmission over insecure networks should be prohibited, and storage on portable devices may require restrictions (at a minimum, encryption). Archival for a specified number of years is often mandated, and at some point policies call for data destruction.

If the technology specified in the policy standards is not compatible with the technology you're selling, you may find yourself out of a job. But if you're the one specifying the standards, it will be easy to focus on the appropriate products and services your company offers.

In most cases, regulations don't specify infrastructure, so your goal is to provide a level of due care with respect to the client's data. Even if your clients have never had any formal policies in place, chances are they will be required to create them in the future. Consider adding this offering if your company has never listed it on the menu.

You, Trusted Advisor

Stop looking for products that meet regulations. Instead, start looking at the assets: the data that must be protected.

Chart reasonable steps based on best-practice security guidelines. Examine data types and their life-cycle requirements. Get involved in policy changes to ensure your technology focus areas are covered. You can then become a long-term security advisor. Selling security is not about technology, it's the asset that matters.

David Stelzl, CISSP, author of *The House & the Cloud* and the owner and founder of Charlotte, NC-based Stelzl Visionary Learning Concepts, Inc., a company that offers keynotes, workshops, and professional coaching to high-tech solutions providers.. For more information, email SecureAssets@stelzl.us or visit www.stelzl.us.