What can Government Agencies Teach You About Compliance?

What can Government Agencies Teach You About Compliance?

by BY DAVID WILSON
Manager, Computer Security Incident Response Team, United States Securities and Exchange Commission

It's a long-standing free market cliche that no goverment agency can possibly be more effective than private sector. As John McDiarmid put it way back in 1939, "Government by its nature unfit for efficient conduct of business enterprises." (“Can Government Be Efficient in Business?” Annals of the American Academy of Political and Social Science, Volume 206). As a result of this long-held belief, most private businesses don’t look to government agencies as models for success about, well, much of anything. But, as a much older saying goes, there’s often an exception that tests the rule. Is it possible that private industry could learn some lessons from the way government agencies resolve their issues with information technology compliance rules? Let’s look at some data.

A recent study released by the IT Policy Compliance Group found that about 12 percent of government organizations have a very large number of compliance deficiencies, making them “laggards” in the study’s terminology. Laggards are defined in the study as entities that need to correct at least 16 but perhaps hundreds of deficiencies before they can come close to being compliant. A bare majority of government organizations – about 56 percent – have at least three but less than 16 deficiencies. And only 32 percent of government agencies have less than three deficiencies.

But hold on. There’s something a little strange about the numbers for the private sector. About 20 percent of those efficient businesses are laggards. And only 10 percent of them have less than three deficiencies. Leaving the vast majority – 70 percent – in that middle ground of more than 3 deficiencies, but less than 16.

What the heck is going on here? Well, obviously, businesses and government agencies each have a very different set of requirements. But few would argue that the compliance requirements for a private sector entity – driven these days largely by the Sarbanes-Oxley Act of 2002 – are more onerous or more complex than the IT compliance requirements for government agencies set forth in documents like the Federal Information Security Management Act of 2002 or the National Institute of Standards raft of computer security papers that make up the NIST 800 series. And you really haven’t lived until you’ve been simultaneously annually audited for six months at a stretch by the Inspector General, the General Accounting Office, and your own internal auditing team, each of which is pounding away at what they see as different deficiencies.

So although each sector has different specific requirements, the basic objectives – protection of IT resources, keeping entities in compliance with existing regulations while protecting the entity’s infrastructure – must, of necessity, dictate a great deal of common ground. In “Anna Karenina,” Tolstoy observed that happy families are all alike, but every unhappy family is unhappy in its own way. Likewise, while there are a lot of reasons for any entity – whether in the private or public sector – to be out of compliance, those that are leaders in compliance tend to have a few things in common.

For example, a recent study by Lord & Benoit, LLC, analyzed data from 148 companies with revenues under $100 million and found that 60 companies had poorly designed controls with regard to a segregation of duties or a lack of effective compensating controls. Translation: Managers frequently believe that something is happening a certain way, when what’s actually happening is very, very different. There are countless ways that this can occur, from a simple lack of any attempt at oversight on the part of managers to a lack of internal checks and balances that would identify lower-level employees who are submitting inaccurate reports to upper management. That same study found that 45 companies had material IT weaknesses attributed to lack of or failure to follow policy relating to access controls, change controls, and application controls.

There’s no question that government managers can fall in to the same sorts of traps. Now that we’ve identified the sorts of issues that can make either a public entity or a private entity “unhappy” with regard to compliance, let’s look at the sort of things that can keep everybody – both the regulator and the regulated – happy.

The IT Policy Compliance Group study offers some clear guidance as to what separates those who are laggards from those who are leaders.

First, to be successful, you’ve got to document all your business procedures, all your IT assets, and all your IT controls. This really is the foundation of everything else and you won’t be successful until these tasks are completed.

Next, combine all that new-found knowledge about your environment with automated systems for monitoring and reporting of IT controls, IT change management, and IT procedures. Not only is this extremely efficient, it eliminates problems like accidental or deliberate failures to report.

And finally, successful entities are noting their failures and changing their procedures to allow them to achieve compliance.

In general, the entities that are not in compliance are simply going about this in the wrong way. They’re not documenting the environment (or at least not starting with that sort of documentation). And they’re spending money incorrectly, bringing in people to monitor controls rather than making an investment in automation. Failure to adhere to these two basic principles opens the door to a million ways of noncompliance.

In contrast, the one thing that every successful entity does is this: The more frequently they measure their IT-based controls, policies, and audit results, the more they’re in compliance. In fact, every government shop – that’s a flat 100 percent – that does that sort of monitoring once a month is a compliance leader. And the laggards? Well, 80 percent of them are only doing monitoring once a year. Tolstoy was right; everybody is happy in the same way.

I would like to close by saying that the private sector actually has a significant advantage in terms of motivators for full compliance. Sure, we all want to be compliant because, well, it’s the right thing to do, but in addition, not following the rules exposes you to liability, to fines, and could even cost you your job. In the private sector, however, compliance can also be an excellent marketing tool.

Don’t believe me? A decade ago, when viruses attached to word processing documents were driving computer users crazy, not a single Internet Service Provider attempted to strip such malicious software from their servers. ISPs saw such expenditures as placing them at a competitive disadvantage; the theory was that the razor-thin margins in the industry couldn’t tolerate additional expenditures.

But a funny thing happened. As Internet access became more of a commodity, ISPs began trying to differentiate themselves by making just those sorts of investments in order to attract new customers, or to make their current customers less likely to look for a less expensive service. Today, it’s hard to find an ISP whose marketing materials don’t prominently mention anti-virus protection.

You can apply the same techniques to the quest for compliance. That is, compliance should not be thought of as a black hole of expenditure, but a way of setting yourself apart from the competition. Who would you rather do business with, a company that’s a little less expensive but isn’t tops at following all the safety rules, or a company that’s little more expensive but is following all the rules, all the time?

You incentives here are pretty obvious. Compliance doesn’t just keep save you money on lawyers and keep you from getting fined. At the end of day, compliance is just good for business.

The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed herein are those of the author and do not necessarily reflect the views of the Commission or of the author’s colleagues upon the staff of the Commission, any other federal agency, or the government of the United States of America.

Close Window