

Mr. Compliance Officer, Tear Down These Walls

Source: [IT Business Edge](#) | Priority: [Fortifying Network Security](#) | Topic: [Network Security](#)

Date Published: 7/21/2008

Carl Weinschenk spoke with Steve McCalmont, CEO and Founder, [Avior Computing](#), which recently did a survey looking at how its customers handled compliance.

Weinschenk: What was the survey about and what did you find?

McCalmont: The purpose was twofold. First, from Avior's viewpoint, it was to get a better handle on the global [compliance] questions that are pressing CIOs and CSOs. There is a direct tie-in in many places between compliance and security. Security is one aspect of many in the world of compliance. We looked to try to get better market information, get a look at the overall maturity of the market. One of the requests we continually hear – we specialize in the financial service and insurance industries – is that they want to know how they are doing in reference to their peers and where those peers see the market. We set out to answer some pretty high-level questions. The biggest thing we gained from this is that it appears that most of the major corporations are heading in the right direction, but that they have a lot of work ahead of them — and that they know it. So everything is a drill down from that statement. All the data we required and wrote analysis on supports that.

Weinschenk: How do most companies deal with emerging regulations?

McCalmont: When a new regulatory requirement comes out, when a new standards body presents something, management wants to effectively look at it. They set up groups to go after it. An example of that is Sarbanes-Oxley. When it came out, everyone was in a panic. The way most tried to solve that problem is to set up a group, a team, a project. They went after it in a reactionary way. Gramm-Leach-Bliley, HIPAA, BASEL II, new ISO standards, [all] are the same thing. One of biggest things we want to figure out is what people do to break down silos [between compliance efforts]. If you are going to make major gains in efficiency and effectiveness in compliance and security, the only way to do it is to look across the entire environment. Not only your department and group, but also third-party suppliers and vendors. "We found that 43 percent of the

surveyed organizations treat each regulation or standard as a separate project. That tells me that we are fairly early in the overall maturity in this sector."

Weinschenk: It sounds very broad.

McCalmont: If you drew a Venn diagram, the top of it is governance. Under that is compliance, risk and then underneath those two are security components scattered throughout. The issue is to look at it as a whole and get the big picture to increase compliance and security and manage risks better. The Nirvana is to supply risk-adjusted compliance information about business units and partners to make good decisions for governance.

Weinschenk: What did the study find?

McCalmont: Basically, we found that 43 percent of the surveyed organizations treat each regulation or standard as a separate project. That tells me that we are fairly early in the overall maturity in this sector. If it was a mature market, there would be only perhaps a handful of organizations — maybe 5 percent — that would treat it this way. The opposite would be implementing a unified program. Twenty-eight percent said they have a unified program. To me, that is not enough. If you want to achieve high levels of security and compliance and moderate risks effectively — all adding up to good governance — that number has to be much larger. The vast majority, especially in financial services, need to view programs as a whole. That's very hard to do.

Weinschenk: Does a holistic approach lead to better results for the effort, or simply the same results for less money?

McCalmont: We don't have the survey results to show this, but our customer base has proven [that improves results] ... There is a huge amount of cost savings by automating a unified program. Incidentally, probably one of the biggest cost savings is the hidden costs. But I would say the single biggest cost is [that companies with a silo approach] tend to be less compliant and consequently can be less secure. Here's a side note: Being compliant with a regulation doesn't necessarily mean you are secure. That's proven every day.

Weinschenk: What is the big picture?

McCalmont: If we look at it as a total program, the questions are how to achieve a high level of security and compliance and effectively manage risk. The only way to do those three things effectively is to do it across the entire enterprise, including third-party vendors. A lot of organizations, when they look at compliance, risk and security, they just look at themselves. If they have a lot of sensitive data at third-party suppliers, they have to do same thing there and at vendors.

Weinschenk: But you say there still is a lot of immaturity.

McCalmont: When we talked about some of the automation tools people use, especially during the assessment process, it wasn't a surprise for us but kind of shocking still to find that 85 percent of respondents still use spreadsheets to manage the compliance assessment process. That, in and of itself, is a huge security risk. You have all of your vital information about compliance sitting in a spreadsheet and people are e-mailing it to all departments. That spreadsheet itself is not secure. Most modern compliance automation tools have a very very high level of security built in to prevent that kind of information from being improperly disclosed. While it is in a spreadsheet, it is too cumbersome and is impossible to keep secure. One of the things I mention in all talks I give is if you are doing an assessment with detailed compliance and security information, do not do it on a spreadsheet because that is a major violation of security right there. It tells you how immature the market is.