A CMI/SkyView Partners Business Brief White Paper:

The Hidden Cost of Security Compliance

By John Vanderwall,
Chairman and CEO SkyView Partners, Inc.

In Cooperation With
SKYVIEW
PARTNERS, INC

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

I found myself in an interesting conversation with a friend of mine recently. He's in IT management for a division of a large storage area network provider. When I asked about his job he quickly lamented that he didn't like his job at the moment because he was too often caught up doing "busy" work and wasn't able to take on projects that would have the potential to affect his company's bottom-line.

When I asked about security compliance, he rolled his eyes. His view was simply that compliance was yet another burden that IT had to deal with that took away from the bottom- line impact that they so desperately wanted to affect. Let's look at the burden and cost of compliance.

Standards, regulations, laws, legislation …. You would have to have buried your head deeply in sand not to have even a passing understanding of the simple fact that "compliance" has become a recurring theme in the day to day operations of business. Compliance covers a host of areas, but for the purpose of this discussion we will limit ourselves to the topic of "security compliance", most specifically as it relates to security on your computing platforms. Don't worry. This isn't going to be a technical discussion. This discussion is about something that every executive should think about … the bottom-line.

So where exactly, does security compliance begin? Security compliance starts with evaluating one's "house." In other words, it starts with examining where the deficiencies lie, determining what risk they present and what needs to be done to address these risks. Next come the auditors' visits. Depending on the size of the company you may also have to deal with an internal audit group prior to working with an external audit group. And depending on the vertical industry to which your organization belongs, you may be dealing with multiple audits from multiple auditing firms. Regardless of the number of audits performed each year, when auditors get involved, the requests for data for analysis start to roll in.

Having co-founded a company and worked in the security compliance space for more than 10 years, it's been a fascinating journey helping companies attain and maintain security compliance on their systems.

The issue is that most companies tend to look at security compliance as an "event." They think if they can make it through this event just one time, they will be okay. The funny thing is that the next year, those auditors are back, asking for the same data – again - doing the same analysis - again - and writing up their opinions - again. I've often remarked that compliance is the "gift that keeps on giving". It happens at least every year, like clockwork and you hope that what the auditors sees this year is just a little better than what they saw last year, or you will have to explain a lot to investors, shareholders, executive committees and the board of directors.

It's in the simple fact that most companies think of security compliance as an event that the hidden costs stack up. When auditors ask for data, executives refer them to the IT group and the scramble begins.

Seemingly innocent requests for data cause a lot of work for people in IT, as they develop reports, analyze output and explain results.   Explanations lead to more requests and more reports and more analysis. To the executive this cost is hidden. IT is doing the work, developing the reports and explaining the results. It's not like there's an obvious cash outlay because numerous temporary workers have been hired to address the auditors' requests. What is hidden is the fact that IT is busily preparing information for auditors which means they are NOT working on those things or are delaying delivery of projects that may have a very positive effect on the bottom-line. It's the opportunity cost that is hidden when you deal with security compliance. Rather than developing that new web portal that might result in increased business volume or working on back office thru-put for increasing order flow, the IT group is examining systems, producing reports, explaining processes, testing processes and spending a lot of time with the auditors. What we've seen is that the process of compliance is largely manual and prone to error and inaccuracy. So while the hidden cost of compliance is lost opportunity, the loss is exacerbated by the manual nature of the compliance reporting. Steps often need to be repeated – not just because the auditor is asking again but to verify that the results were accurate. So as an executive you have to ask: What else could IT be doing other than producing compliance reports and explaining processes? Is there anything we can do to solve the compliance reporting issue or should we just ignore the issue of compliance and focus on bottom-line projects?

The answers to these questions aren't as easy as they might seem. First of all, I'm not advocating the idea that compliance is something to be ignored. The implications of ignoring compliance can be catastrophic. Read the newspaper and see the results of what happens when people don't pay attention to compliance - security breaches, lost data and fraud all resulting in millions of dollars spent fighting to restore your good name and customer/investor confidence as well as the fines assessed from various agencies. It's important that IT focuses on bottom-line projects and deal with compliance at the same time. To do that, the best answer to the issue of compliance is in the old adage "work smarter, not harder". Failing to realize that compliance is something that is here to stay and must be dealt with consistently will quickly put you in the category of working harder and not smarter, as you scramble each year to address security compliance. To be smart about security compliance, let's look at what compliance is really concerned about.

Auditors are interested in process, documentation and best practices. The starting point for an auditor is a company's security policy. The security policy document tells the auditor the view of and rules for security as it's to be implemented throughout your company. Keep in mind that a company's overall security policy is high level and only becomes detailed as each computing platform is addressed. It's at this level that auditors become interested in the specific process and documentation that illustrates how a particular computing platform meets the objectives of the corporate security policy.

Once you're familiar with what the auditor is concerned about, working smarter dictates that the best approach is to determine what can be automated. The goal of your automation effort should be to define a process that produces accurate information in an easily repeatable format. Automating your security compliance process cuts the hidden cost associated with manual processes. No more “scrambling” to answer requests for data. No more time spent documenting your processes and continually reviewing that documentation. No more time spent reproducing information because a “manual error” was found. By examining compliance, automating what can be automated, you end up with several very positive results for your company. First you free up time for IT to focus on bottom-line projects. Second you improve your ability to respond to compliance requirements with accurate information and easily repeatable processes. Third, implementing the right security compliance automation solution, you end up with a valuable by-product. That by-product is a sound “security administration” discipline. Administering security, which is really the result of a sound security policy, can be time consuming work. It’s one thing to produce the information quickly, accurately and easily, it’s quite another to deal with those “out of compliance” issues, and develop a regular discipline of proactively examining key aspects of security and looking for anomalies. Your security compliance automation solution should point out exceptions and allow you to pinpoint and “fix” out of compliance issues quickly and easily, going beyond the ability to produce nice reports. The hidden cost of administering security and dealing with problems revealed during the compliance process is yet another problem that management must address.

The good news is that solutions for automating security compliance and security administration exist. What executives need to do now is stop and count the cost of compliance and security administration and recognize that investing in technology to solve this problem will not only free up talent in your IT staff to pursue creative bottom-line projects rather than mundane and highly necessary security compliance and security administration details, it will improve accuracy and efficiency. As executives, it’s important to not only look at the expenses associ- ated with IT, but to listen to and appreciate the process IT is going through. It’s easy to look at the IT group and say “it’s your job to deal with these information requests, just do it”. However, in today’s world of limited IT resources, it makes sense to stop and think about that innocent request of your IT group to “get the auditors the information they need”. Stop and ask yourself and your IT group some questions: What is the impact of security compliance on my precious IT resources? What opportunities am I missing because I haven’t given them the resource to work smarter and not harder? Is there a better, more effective way to do the work that a seemingly simple request entails? Are there added benefits from investing in re- sources to deal with security compliance? When you spend the time to have a good discussion with your IT group on just the subject of security compliance, you may find that the proper investment may impact your bottom-line in ways you didn’t imagine.

About the Author:

John has spent over twelve years in executive management positions in the computer security arena. In 2002, he, together with Carol Woodbury, founded SkyView Partners Inc. SkyView Partners Inc. is a security compliance software and consulting firm specializing in automating security compliance reporting and security administration. SkyView Partners Inc. has supplied solutions and consulting to many Fortune 1000 companies and many Small -to Medium-sized businesses. Numbered in its customer list are Scotiabank, CDW, Les Schwab, Sungard Public Sector, TD Financial, Costco, Pfizer and many others. In his spare time, John has created a non-profit organization, Expressive Business Strategies, that teaches practical business principles to the poor in developing countries. The goal is to give people a “hand up” not a “hand out” resulting in sustainable economic development for these emerging nations. To find out more about SkyView Partners, go to: www.skyviewpartners.com

Status Check -- by Kris Neely, CMI’s Chief Technology Officer

Security compliance has never been a hotter issue. Hackers steal billons worldwide each year. And that’s just the part we know about.

Yet many of the executives and CXX-level folks I meet with -- whistle past the graveyard, scoffing at the notion that their firm will be hacked, and that “hacking” is the sort of thing that happens to other companies – so why should our company spend budget on compliance?

Leaving Sarbanes-Oxley (SOX) aside, security compliance should be a key CXX-level discussion point because it does happen to firms everyday. A denial-of-service (DoS) attack here. A virus on someone’s laptop there. A password taped to someone’s cubicle wall.

In addition, like Chinese Water Torture, it isn’t the single drip of water that causes the pain, it’s the constant, unrelenting rhythm of hack/probe/deny/virus/fraud/etc/etc that wears down IT staff members, and reveals security flaws.

John Vanderwall has done a terrific job of pointing to just a few key issues that point to the larger issue of security compliance and, by extension, remediation. I compliment his, and SkyView Partner’s, clarity of vision in being able to articulate the hidden costs of security compliance for a CXX-level audience. CFOs and CEOs – take note!

In closing, just a suggestion: know when to ask for help. Security compliance is a complex, multi-layered discipline. At CMI, we know this topic. I’d sleep better knowing my technology business partner knew as much.

Be well,
Kris

Kris Neely CTO, CMI

Reality Check -- CFO Endorsement for CMI White Paper on Security Compliance

Compliance is often perceived as a bad word, something bureaucratic and time consuming. I always tell companies that the secret to efficiency is making sure that the processes and procedures that you undertake every day, the ones that you use to run the business, are in synch with the corporate processes that you need every month, quarter or year. Budgeting and forecasting is a clear example of this. If every year the company has to stop and spend a lot of time preparing a budget, then something is wrong -- and that is a hidden cost. A budget should be easily derived from your weekly or monthly forecasting process. Of course, the annual budget should get extra attention, to be sure, but it should not be burdensome.

This analogy applies to IT Security Compliance. Every day processes should be part of the security compliance framework of the company. When you are audited or have a vendor visiting, you are wise to double-check everything -- but it should not involve the company stopping to meet compliance needs. Time wasted is always a hidden cost.

So start with a simple question: “When a compliance audit is required, what is the tone of our IT department?” Do their shoulders slump? Do they complain about all the extra work it will entail? Or are they happy to get the chance to show their boss that everything is under control? If the answer is the former, then you need to look at why.

Here is a simple test. Go to your HR Department and get a list of all employees who have left your firm during the last calendar year. Take that list straight to IT and get them to check the status of those people’s e-mail accounts, network access status, building access, passwords still in place, and so on.

If this is not 100% correct, then not only do you have an obvious (and potentially huge) security problem, but you do not have the processes in place that are helping security compliance. That said, you can easily test other areas of Security Compliance such as where files are stored, are file authorizations up to date and so on.

If you find issues when carrying out a quick review, forget compliance. You should be worried that your business is being placed at unnecessary risk. Nevertheless, check your own tone, as well: Are you more worried about your business, or the audit?

I have often found that IT departments are not trained, or do not have the experience, in how to make day-to-day processes part of a larger, or on-going objective. In short, the IT Department’s staff are often too tactical, and not strategic. Or, it is not clear who is responsible for implementing or manifesting such change(s). For example, when an employee leaves, who is responsible for collecting their access badges – IT or HR? Who checks that this happened every time? And so on.

That said, I can tell you from personal experience that investing a few minutes in a process can reap immediate longer term benefits. In the example I gave above, a simple employee exit checklist, prepared by an IT employee and reviewed by a manager takes only a few minutes. The same logical approach can be applied to more complex areas of compliance. Looking at the overall process is essential to avoiding the burden of compliance, but it is also essential for the well-being of your business.

Security compliance is as essential topic and I recommend this White Paper heartily to any executive trying to run a tight, cost-effective ship.

Best,
Kevin

Mr. Kevin Weston, is the former CFO of Digital Domain Productions, as well as former VP Finance and Operations of LucasArts, and was CFO/SVP Finance and Operations at Eidos Interactive Inc.