Seeking Compliance Nirvana

Greg A. Nolann

Compliance. The mere mention of it brings to mind a harrowing list of questions and concerns. For example, who is complying and with what? With so many standards, laws, angles, intersections, overlaps, and consequences, who ultimately gets to determine if you are compliant or not? How do you determine what is in scope and what is not? And why do you instantly think of an audit when you hear the word *compliance*?

To see the tangled hairball that is compliance, just take a look at my company. It is on the hook for SOX (Sarbanes-Oxley Act of 2002), as we are a publicly traded company; for a number of banks for the PCI DSS (payment card industry data security standard), also known as Visa CISP (Cardholder Information Security Program); for HIPAA (Health Insurance Portability and Accountability Act); for CA 1786 (and all other states' disclosure laws); and for the European Union, its member countries, Japan, Korea, and a handful of other countries' privacy and data security laws (these alone could probably spawn an entire series of lessons and lectures!).

The two main compliance obligations, SOX and PCI, address similar goals but take approaches that are 180 degrees apart. SOX doesn't specify a standard; instead it says to use some other established methodology or set of practices. PCI, on the other hand, specifies exactly what you must do, who can do it, where it applies, and how to determine if you are compliant. There should be a happy place where both meet. Let's look at these two individually and point out some of their unique problems.

SOX

Sarbanes-Oxley—what a pain that was the first time around! SOX has a component that addresses the integrity of systems involved in reporting numbers to the street. It's this little part of SOX that causes so much pain, because depending on the interpretation, it can bring non-financial systems into the scope of a financial audit. Auditing computer systems, particularly systems that are not financial in nature, is an entirely different animal than auditing finances and financial systems, and the carpet-bombing approach often taken by large audit firms to pass the final audit does more harm than good.

Don't let SOX

AND PCI GET THE
BETTER OF YOU

By carpet bombing I mean an all-out approach where armies of auditors and their handlers (AKA project managers) are sent out into

the company to try to figure out first what's in scope and to what extent it's in scope, then to pester those teams (for months), mapping what they think is compliant and twisting their arms to get them to fit that model before the actual audit so that the audit results in a 100 percent compliant result. Having auditors (internal and external) and compliance project managers in your face for months at a time weakens morale and impacts the bottom line. Why not instead work through a single touch point that bears the brunt of these folks, and let people do their jobs?

This single touch point would be the only person allowed to interface with teams in both directions. This person would do the homework to determine the scope of the audit, identify the minimum personnel required to figure out how the system works, and then take that specific system knowledge and translate it into bits that the auditors can understand. This way, many months of endless meetings with more people than necessary in the room could be reduced to just a few weeks of disruption.

Another problem with SOX is the actual control grid. The legislators didn't specify a standard to follow; they left it up to the auditing firms. If this were just a financial systems audit, I'd say OK, no problem. It's not, though. You now have inexperienced consultants following some sort of checklist that may or may not be applicable, and specifying controls that may or may not be relevant. Yes, SOX is the domain of the CFO and its auditors, but the reality is that the systems it targets are the realm of the CIO. Why not instead let the CIO drive SOX compliance such that it satisfies requirements set forth by the CFO?

At the end of the day, it's about ensuring that the systems involved in the revenue stream are secure and properly accessed by appropriate personnel. Is it really that difficult to assess this? Isn't it more important to do the right long-term thing by identifying issues, finding solutions appropriate to the system/environment, get-

Continued on page 71

Continued from page 72

ting a timeline to address the issues, and putting in place longer-term cultural efforts (e.g., education, processes, policies) that will help avoid similar issues in the future?

PCI

Don't get me wrong, I'm all for protecting credit card data and processing systems. This is something that is common sense, but sadly, common sense is by no sense common. Because of this, the payment card industry—you know, that cartel of card companies such as Visa, MasterCard, and American Express—has taken it upon itself to mandate compliance with its data security standard.

The DSS is PCI's attempt to define what you can and cannot do if you are involved in credit card transactions. The standard touches on network security, cardholder data protection, vulnerability management programs, strong access control, network monitoring, and INFOSEC (information systems security) policies. If you have had any exposure to the notion of information security, you know there's more than one way to address these notions.

That being said, the PCI DSS is poorly written, defines very specific (and sometimes uneducated) technical controls, and is inconsistently applied. Auditors are forced to follow the letter of the law defined by the standard rather than the spirit of it, which would make more sense. The PCI has been so overbearing about what auditors have to do that the Big 4 accounting firms have pulled out of that line of business altogether.

The standard also seems written to be *buzzword compliant* and is modeled on Windows-based systems (umm, we're a Unix shop). Again, it's not about having auditors trained to find specific implementations that may or may not exist on a given platform but rather to have auditors trained to understand the issues that arise from a given system—what it does, how it does it, and how it addresses the standard. Are you looking for a device labeled as a firewall or firewall functionality? Are you looking for scanning the entire IP space or simply the network connected to the card processing systems? Are you looking for logfiles capturing very specific data for very specific events or rather verifying that in the event of an investigation, it is possible to have accountability of actions?

Another problem is that the banks that are supposed to enforce compliance of merchants for the card companies are themselves not compliant and don't really understand the problem. How can they approve compensating controls if they either have bigger problems once they receive our data or simply don't have the experience to understand a given technical nuance?

Fortunately, our systems are architected such that the critical bits are segmented off from the rest of the company, access controls are in place to get to them, and data is handled appropriately. It's good systems engineering that properly identifies the system's risks (inherent in the given application, its users, the data, and the processing), considers business and technology constraints, and puts it all together. This makes our PCI audit easier. After all, isn't this what it's all about? Our systems are not perfect—there's no such thing—but they keep the data safe.

NIRVANA

Ideally, there should be only one audit per year that validates a company's security requirements and can be used to satisfy any or all external stakeholders. These security requirements are established based in part on specific risks or threats against the company's business/systems and in part on relevant external compliance obligations. Systems identified as relevant to these external suitors get a calendar-based audit, while all the rest are reviewed every four (or so) quarters to ensure they are still doing the right thing and addressing potential new standards.

Passing an audit needn't be a headache. A well-oiled compliance machine is invisible to the product development teams. It all starts with the product development culture. Products are defined with risks in mind and how to address these risks. Architects put together systems that address users, their data, administrators, their access, and the interfaces over which all this occurs. Developers write fail-safe code and address the usual bits of input validation (among other things). Operations personnel deploy and manage the systems in a similar fashion.

Yes, compliance is more than an auditor pestering developers too many times per year, taking them away from their work. If done correctly, compliance is ingrained into employees' minds and is just a part of doing business. You can get there with lots of training and built-in checks and balances. To me, a world without auditors—especially the Big 4—is nirvana. ☺

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

GREG A. NOLANN is an engineering manager who has been playing in the security/compliance space since the mid-1980s. He's currently trying to reach security compliance nirvana at a Fortune 500 company. You can find him taking pictures or exploring urban jungles when not thinking about security policies, processes, or protecting user data.

© 2006 ACM 1542-7730/06/0900 \$5.00