Compliance versus Buy-In
Transcript

Stephanie Losi: Welcome to the CERT Executive Podcast Series. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Before we begin, I'd like to let you know that show notes and other supporting materials for today's conversation are available at the podcast website, please take a few minutes to look them over.

My name is Stephanie Losi, I am a journalist and graduate student at Carnegie Mellon working with the CERT program. I am pleased to introduce Julia Allen, a senior researcher at CERT who works on security governance and executive outreach. Today we'll be talking about the difference between compliance and true buy-in.

What I want to say is that what we see now a lot of the time it seems more like compliance, where the companies are scrambling to meet the deadlines, because of course Sarbanes-Oxley had several deadlines in the past couple of years, that companies had to meet. But how can we get from complying with the law to really changing processes and practices so that across the board there's an increased security mentality and culture of security throughout the company, rather than just a set of compliance practices that have to be in place by this particular date.

Julia Allen: It's very, very interesting when you take a look at, I'll give you one example, some of the forums that I've participated in, listening to executives, particularly audit executives, talk about organizations that have been able to comply with Sarbanes-Oxley for little to no additional cost, and organizations that have spent millions of dollars both in terms of reassessing and updating their own internal controls and then all the commensurate internal and external audit costs that have gone with validating that those controls are in place. And what the difference seems to be is that organizations that have embraced this notion of having a set of standard processes, standard operating procedures, kind of a standard way of doing business, this is what our objectives are, these are what our critical success factors are, these are the processes that we've put in place to accomplish that, and then having that documented and be something that's regularly reviewed and updated. Those organizations seem to have an easier time with this flurry of regulatory activity than those that are maybe "Well, now I've got to comply with Sarbanes-Oxley, and a couple of years ago it was Gramm Leach Bliley, and oh, you know, I understand that now we're holding some medical information so I may be subject to HIPAA," and etcetera, etcetera. And they try and treat each one of those regulations as a point event or a single event, as opposed to taking a look at what are we in business to do, what data are we trying to protect, what processes do we have in place to protect it, and typically those organizations that can get through this a little more easily are able to just map or trace the new regulatory requirements to their standard business practice, and by making a few changes, a few variations get through that compliance activity as yes, an additional thing to do but not the central focus.

Stephanie Losi: Okay, so let's take the perspective of let's say we're a company that has not been in that position, let's say there's a company that has spent millions of dollars on compliance or any significant amount really, how can they can get from

that point to the point that the company that really adopted the standard of best practices is currently at. What steps do they need to take?

Julia Allen: Well, that's a really good question and I think what they need to do is learn from their peers, do some benchmarking, find out how other organizations have gotten-- it's certainly not a quick-fix, I mean these organizations that have kind of this very explicit traceability between their business objectives, their success factors, their processes, policies, procedures and have that kind of as an integrated whole, that's been years in the making, but I'm sure there are ways you can get there more efficiently than trying to start from scratch. So I would say to organizations that find themselves kind of being whipsawed by all this regulatory activity is to really concentrate on what's core to the business, what are the key, you know, let's stay with security, what are the key information assets, what are the key processes, what are the key services that I'm offering, and what are the key risks, and then build a set of perhaps a modest set of core business process definitions and some standards and some policies and some practices. If you talk to folks that have been through Sarbanes-Oxley year one and just completing up year two, those that seem to have come out of the activity with a positive response are using Sarbanes-Oxley as an opportunity to really improve their internal controls, to do a lot of data capture, to do a lot of process definition, so that they don't have to repeat all of the individual actions in future years that they use to get to this point, so they're actually using it to almost serve as a catalyst or as a jumpstart to get to these standard sets of process definitions and policies and procedures as part of their compliance activity, so they can almost use what they're going through now to help them get to a more stable place.

Stephanie Losi: Great, and then once they have these policies and procedures and best practices all written into their organizational framework, how do you push that out to every employee to ensure that there is a true culture of security and that everyone is buying in and understands why we are doing this, and that the answer is not "Well it's because it's the law now," but the answer is "Because this is the right thing to do and the right way to do business and it's actually going to produce a return for us."

Julia Allen: You know, it's an interesting question for exactly what we're talking about, but it's kind of an age-old question for any kind of organizational change that you want to bring about, I'm doing one set of activities and I see an opportunity to get into a new market but to get into that new market I have to have all these new competencies, how do I actually get people to change, and changing human behavior is probably one of the toughest issues to deal with because people, you know, generally if they've been successful doing things in a particular way they continue to do--

Stephanie Losi: Well why change, right.

Julia Allen: They continue to do things that way. So some of the most successful approaches that we have found is that you really have to define what the benefit is, in other words if I'm in human resources and I have to help implement some of these improvements or perhaps build up some training capability to do education training and awareness with the staff so that they understand when they touch this particular customer database they have to-- they're going to be subject to additional authorization and authentication and access control requirements and they can't take particular data out of the physical facility or if they're going to have to access

remotely they have to go through a virtual private network, etcetera, etcetera. If people understand, if employees understand why this is important to the business, in addition to how their role, the particular role that they play, supports what the business is trying to accomplish, that starts to create some cultural momentum. One of the other approaches that we've found effective is if you take one set of controls or processes with one small group in the company and you work with them in a very intensive manner, and they start to produce in very short time some immediate beneficial results that are made visible, maybe put up on the company intranet, in other words you start with some small successes and let that serve as a catalyst for others to say "But wait, I want to be doing that too," you know, "I see that just made their job," or "they were able to get this job done in a week and it used to take two weeks, where do I get some of that?" So you start to create some pull for the improvement just based on people's natural motivations.

Stephanie Losi: All right, well thank you very much Julia, I think this has been a really interesting and illuminating conversation for me in terms of, you know, how do you get from compliance to buy-in, because it's definitely a question that I had in my mind.

Julia Allen: You're very welcome Stephanie, look forward to talking with you further.

Stephanie Losi: Thank you.