Getting Real about Security Governance
Transcript

Part 1: An Evolution Toward Practicality

Stephanie Losi: Welcome to CERT's podcast series: Security for Business Leaders. 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.

Show notes for today's conversation are available at the podcast website.

My name is Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon, working with the CERT Program. Today I am pleased to introduce Julia Allen, a senior researcher with CERT in the areas of security governance and executive outreach. We'll be discussing how to implement a governance-based information security program. So, Julia, how has your security governance research progressed since we last talked about why leaders should care about security?

Julia Allen: Well, Stephanie, first of all I'm real happy to be talking with you today to give everyone an update on how our work has moved along. And the original research that we did on governing for enterprise security that culminated in our research report in June of 2005 and that we talked about in our last podcast, really set the stage for how to think about security from a governance perspective. There are many, many governance concerns and corporate-level oversight issues that executives, business leaders, boards of directors, members have to consider. And so what we did in that original research was put security into that context: how to think about it using the governance principles and constructs of enterprise governance, corporate governance, information technology governance, tried to get security interpreted and use some of the same terminology – put it into the same mix of governance concerns.

And what's transpired since that time is we've actually been able to observe and research and better understand how some organizations are actually enjoying some success in putting governance-based security programs in place. And so what we've attempted to do in our Governing for Enterprise Security Implementation Guide series is to start to describe a governance framework and some more prescriptive steps that leaders can take to actually put such a program in place.

Stephanie Losi: Okay and so how would you characterize that? You say you created a framework. Now, what is it, and what does it do for leaders?

Julia Allen: Well, the way I would characterize it is as a set of activities, a set of roles and responsibilities, and a set of results or outcomes or artifacts – the tangible objects that get created when you put such a program in place. So, in terms of activities, we've actually laid out a sequence. For example: establishing your structure, assigning roles and responsibilities, laying out your top-level policies, inventorying, creating an inventory of your most critical digital or information assets. So there's a set of activities in sequence that we recommend – in other words, a recommended order.

And then, and I would say probably one of the most fundamental pieces of the implementation guide, is clear distinction of roles and responsibilities. I mean, we fully recognize that not all of these roles will exist in every organization, but they're notional enough, like: the role of the board risk committee and the role of the chief security or chief information security officer; if there's

a chief risk officer; the role of legal or general counsel; the roles that business unit managers or executives need to play. So we've laid out activities, roles, and responsibilities. And then, for each activity, what the results are that are produced by that activity. For example, you'd expect [for] an activity that is targeted towards developing top-level policies that you would actually end up with a set of robust policy statements. If you're doing an inventory of your information assets, you would actually have a way of capturing that inventory, so we attempt to describe that as well.

So it's certainly a place to start. It's a framework against which to make conscious decisions of, "Well, should I include or exclude this activity? Should I do it in this order? Should I combine roles, or should I better distinguish or differentiate roles?" So in that sense I think it is a framework and gives leaders an opportunity to say, "Well, is this what we want to do, or should we do it slightly differently?"

Stephanie Losi: All right, that sounds great. What led you initially to believe that implementation-level guidance of this sort was necessary? You had written a paper earlier, I know, on governing for enterprise security, and so what got you from thinking, you know, in that vein – because that was a much more general paper – to sort of thinking in this more specific vein where, "Okay, we're going to actually provide, you know, some sort of general timeline and set of steps that people can take that they then can customize to their own needs?"

Julia Allen: Well, as you might expect for leaders that are ready to tackle this issue as an enterprise-level issue or a governance-level concern, when they read and had a chance to consider our original research results, it was – you know, it's kind of like, if you'll allow me: "Okay, I get it. Yes we have to do that. Yes. Okay. Now what do we do?" So it was really a process of interacting with some of our readers, giving presentations, talking to some organizations that are doing this particularly well, and finding out that certainly leaders don't need, kind of step one, step two, step three in excruciating detail, but they needed enough detail that they could begin to see what such a program would be like and have something that they could delegate to various individuals in their organization. Perhaps their chief information officer, obviously chief security officer, human resources, the folks who handle their public relations, because they're all players in putting such a program in place. So what we were told, the feedback that we received, is, "Give us something a little more tangible that we can act on."

Part 2: A Guide to Effective Governance

Stephanie Losi: And so when you were sort of reviewing these cases to sort of figure out, "Well, who has done a good job with this, what are the best approaches?" so that you could come up with your suggested order of steps, what did you learn? Would you say this is an optimal way, or is this a way that is most likely to work for the greatest number of organizations? How did you arrive at this, and are there certain things that maybe an organization should steer away from doing as well?

Julia Allen: Well, what we observed is there are clearly organizations who are doing this well, and there are organizations who are committed to do it but may be kind of at the beginning stages and struggling. And there are organizations that think they have a robust program in place that really don't, because it's really not sustainable or it might be locally optimized but it's not sustained at a consistent level across the organization.

So what we observed, particularly for the organizations that are doing it well – and I think this would be true pretty much for any organization that wanted to undertake this initiative – is that there is an aspect in the culture. There is an appreciation of security roles and responsibilities. When a piece of customer [data] or other type of business sensitive information is handled, people

understand that they need to be conscientious about protecting that. There is segregation of duties, where perhaps someone updates the information but they're not the same person who archives it or backs it up or supports an internal audit. So there's an appreciation that you need to separate roles and responsibilities so that you don't have conflict of interest.

So I think there are some elements of what we call effective security governance and ineffective security governance that we described in our materials, where the effective practices – and, of course, it's always a matter of degree how much you roll out, because it really depends on what's most important to the mission or goals of the organization. So I would say there certainly are some tried-and-true approaches that would work very effectively across most types of organizations, but it's probably a matter of degree in terms of how much they actually invest in full-blown implementation.

Stephanie Losi: Okay. And then again, are there certain steps that are must have versus discretionary? Are there some things that some organizations might say, "Well, we only have the resources to do X number of things or X portions of this project"? What are the things they really need to have?

Julia Allen: Well, probably some of the real core essentials are: We refer to tone at the top. There has to be – and I hate to use this because it seems like for every initiative that an organization takes on we keep talking about senior management support – but what it really comes down to is attention span. Where is the organization going to pay attention? So if you're going to do this, every organization that does this has to have in place some commitment structure where the senior leadership and those in the organization understand that this is important for the well-being, the survival, and the thriving growth of the organization. So: tone at the top, establishing a structure, key roles and responsibilities, some top-level policies. And then an inventory of the assets to be protected, because then what you need to do is you need to have some risk assessment of the degree to which those assets are at risk, the threats and vulnerabilities that they might be exposed to, because then that forms the basis of what protection strategies that you need to put in place. Since you can't do everything, you need to have some basis for saying, "Okay, well, I'm going to do these five things, and I'll try to do the other one hundred if I can, but I know I've got to protect these five assets, like my customer database or like my transactional history." And so you need to have some notion of what you're trying to protect and to what degree you need to protect it. So I would say those four or five things are probably essential for any program.

Stephanie Losi: Okay. So, really, you know, any size business can do this, it's just a matter of doing it on the scale that they can really afford to do.

Julia Allen: Correct.

Stephanie Losi: That's great. Okay. So it sounds as well like a lot of different groups of people have to be involved in order to have a successful project, right? So how can the organization overcome the hurdles involved in this?

Julia Allen: Well, there's – as you mentioned, Stephanie, there are a number of roles that need to be involved. I've mentioned some of them. [There are] some that you may not typically think of like human relations, public relations, legal counsel. The asset owners – I mentioned having an inventory of your most critical assets. Well, who owns those assets? Who's responsible for them? Who's responsible for key customer relationship management systems or a key financial system? Because they have a role to play in the protection strategies. So you've got to get kind of all your ducks lined up.

We recommend that you form a cross-functional team that meets on a fairly regular basis to put issues on the table and work up mitigating strategies for tackling those issues. The fact [is] that there's really no standard set of benchmarks that you can go to help evaluate your own program to determine if you've got inadequate or sufficient level of security because it's still a fairly immature or new discipline for most organizations to undertake. So you kind of have to develop your own benchmarks or perhaps benchmark with your peer or lead competitor organizations.

Certainly one of the big challenges is the growing number of compliance and legal requirements that organizations are faced with that are different from, in the U.S., from state to state, and then when you're dealing globally, from country to country. So when you put this cross-functional team together, they're probably in the best position to come up with plans and strategies for tackling some of the barriers.

Part 3: Making Security a Mainstream Process

Stephanie Losi: All right. So let's say with a project this big something is likely to go wrong at some point along the way. How can a company really deal constructively with that? So that the project stays manageable, it doesn't get derailed, it continues on and they can kind of make this into, you know, a learning moment?

Julia Allen: So you're talking about if there's like a major security incident or some kind of natural disaster that disrupts the program? Is that what you're referring to?

Stephanie Losi: Well, that could be one way. Something could go wrong and the company could have to deal with it, or something could go wrong even in the rollout process. As they're developing this overall governance structure or governance framework, some problem could come up. Maybe a division is uncooperative. So it really could be anything, but just what are some of the best ways for an organization to really deal constructively with problems that come up along the course of either implementing this project or once it's in place something happens and they then have to react?

Julia Allen: That's a good question, but I think it generally applies to any business process or any product and service that the organization is offering, not just the security program. So one of the tenets of this approach is that we suggest that security be mainstreamed. What I mean by that is that [it's] part of strategic and operational planning, part of normal management review. If the organization is using balanced scorecard to do quarterly performance measurement and if that's the basis for how executives get evaluated and get their annual bonuses, then you get security in the balanced scorecard.

So my point being is that when anything happens – and things will happen all the time inside and outside of the organization, – if there's a public disclosure of sensitive data and that shows up in some press release and the company has to scramble. All of their normal processes for business continuity, crisis communication, incident response for situations that they would be handling that are not related to security – a new merger and acquisition, a new product release, putting a product out and finding out that it's got defects and they have to recall the product. All of those kinds of processes that the organization has in place need to embrace and integrate security considerations as well. So that when a security event happens or when something causes the governance program to get derailed or maybe a key leader, a key champion, leaves the organization and now there's a vacuum because there's really no sponsor that's keeping everything going – then the normal business processes would kick in and you'd have to reassign roles and responsibilities, or you would have to get somebody front and center. You'd have to craft the key messages that are going to be delivered to the press and to employees to help them

understand what's going on. So obviously, as always, communication is key, but really the answer is: get security into the mainstream of how the organization does business and then just treat it as any other normal business practice.

Stephanie Losi: Okay. So you've really tried to, with this latest work, put things into a step-by-step process that people can follow. How possible do you think it is to really make that a repeatable process? Can it really be made from, you know, something that is going to be different for every organization [in]to something that really will work for most organizations if they follow it step by step by step by step?

Julia Allen: Well, we've observed that organizations that consider security essential to their success, you don't even find particular energy or attention being paid to security because it's just assumed. It's assumed like it's assumed that you'll fill out your timesheet or your effort report or whatever you use for your compensation basis. It's assumed that you'll ask for, if you're making a purchase request, that you'll ask for that in a standard way.

So, yes, I think the answer to your question is, it is possible to make it a repeatable process, and I think it is possible to have some aspects of it that are consistent across most organizations. And I think there will always be many aspects of it that are tailored to the specific organization based on their mission and what the critical assets are that they most need to protect.

Stephanie Losi: Great. And so from this point forward, now that you've done this work, how do you see governance evolving in the future?

Julia Allen: What we see happening is – and unfortunately I think we're going to see more laws and regulations and more government oversight, not just from the U.S., but from all the other countries that we all do business with – we're going to see more of that kind of attention until the business environment and the Internet-based business community demonstrates that they've got this problem handled to an acceptable level. So I think in the near future we're going to see more energy and attention and regulatory oversight.

And then I think as time goes on we're just going to see more cases where organizations are willing to talk about or able to talk about what they've done to put effective programs in place that other organizations who aren't quite that far along can actually use as examples. And how the future is going to evolve in terms of our work is we intend to put examples of results and outcomes and documents, policies, asset inventories, roles and responsibility definitions. So we intend to continue to populate our governance research space with example artifacts and other types of templates that organizations can use to help them get started.

Stephanie Losi: Great. So where can the listeners learn more?

Julia Allen: Well, my recommendation, and obviously you're talking to someone from CERT so this would be consistent with that, is that your listeners start at the governance portal on the CERT website, and there's a fairly rich set of resources, bibliographies, links to other sources and sites. And so to be able to use the – what we've attempted to do is we've attempted to pull as much as we know about the entire body of knowledge around governance and security into one place. And so it's useful as a point of departure, but there are many other organizations that have been actively participating in this arena for a while. The Information Systems Audit and Control Association has their IT Governance Institute, the Institute of Internal Auditors have done some excellent work here, as has the National Association of Corporate Directors for boards of directors. So, lots of good sources, lots of good sites, and most of those can be found on the CERT governance portal.

Stephanie Losi: Great. Thank you very much Julia. I have enjoyed our conversation, and as always I learned a lot.

Julia Allen: Well, I appreciate it, Stephanie. I look forward to talking to you again in the future.