How to Develop More Secure Software: Practices from Thirty Organizations
Transcript

Part 1: Building Security in Maturity Model (BSIMM): An Update

Julia Allen: 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 Julia Allen. I'm a senior researcher at CERT working on operational resilience and software assurance. Today I'm pleased to welcome back two people to our podcast series. Gary McGraw has joined us, the chief technology officer for Cigital, and also Sammy Migues the principle consultant and director of Knowledge Management, also with Cigital.

Today, Gary, Sammy and I will be discussing their continuing efforts on a maturity model for building security into software throughout the life cycle. We have an update based on a prior podcast we did back in March of '09. And this one, today, is based on analyzing real world experiences from now 30 organizations in seven market sectors.

So welcome back, Gary. Glad to have you with us.

Gary McGraw: Hey, thanks. Great to be here, Julia.

Julia Allen: Hey, and Sammy, thanks so much for making the time.

Sammy Migues: Hi. We really appreciate you having us back. We like talking about this stuff.

Julia Allen: Yeah, I know. You guys have been very prolific and out beating the bushes and getting the word out. So I'm glad that we have a chance to kick this around today. So Gary, just by way of a little bit of background, some of our listeners may not be familiar with what we call BSIMM, the Building Security In Maturity Model. Could you just kind of set the stage in terms of purpose and audience?

Gary McGraw: Absolutely. So the BSIMM project came about as a study of real-world software security initiatives. And the idea is to contrast what's actually happening out there in the real world with what you might call faith-based software security of the sort you might read about in my book, *Software Security*. So there are a lot of people that had been talking about how people might want to approach software security or how people should approach software security. And that was certainly necessary a decade ago, 15 years ago.

But over the last five years or so, a lot of firms have begun to plan out and then execute pretty large-scale software security initiatives. And for the BSIMM project, we simply went and studied those actual initiatives and described what we see. So I guess you might think about it as a descriptive model of real software security as opposed to a prescriptive model that's trying to tell you what to do.

We're very much interested in describing what's happening out there and then you can use those data to help determine what to do yourself. So it's very scientific, very descriptive, very much about measurement and going out and looking and seeing what we see.

Julia Allen: Okay. Gary, who would be the ideal audience for BSIMM? Who might pick it up and put it into use?

Gary McGraw: Well, the BSIMM itself is available for free for anybody to use under the Creative Commons License. And you can get it from the website BSIMM2.com, that's B-S-I-M-M-2.com, and you can just download it and use it however you want.

Of course, the people that are going to get the most use out of a BSIMM would be people that are leading a software security group or a software security initiative in a corporation. So in fact, we had 30 firms in the study, as you mentioned before. And the people that we talked to when we were gathering the data for the BSIMM included, every time, the leader of the software security group who was in charge of the initiative in a corporation.

Julia Allen: Okay. And before we get into some of the players that you've been working with, could you say just a little bit about the structure of the model?

Gary McGraw: Absolutely. So we started out with something that we call the software security framework. And you can think of that as an archaeology grid. What I said before about going out and describing what it is that we saw out there, we wanted to be able to put things into various squares. Archaeology grid is like pieces of string and little tent pegs stuck in the ground. And we would pick up an activity that we would notice and we'd say, "Oh, this one goes in the training square," or "This one goes in the code review square.”

So there are, in the software security framework, 12 practices. And those practices help to just organize the activities that we actually found. Now what's interesting is, we describe 109 activities in the model, which we have observed over 30 firms. It's the union of all activities over all 30 firms.

And the interesting thing is, those 109 activities don't divide very evenly into the 12 practices because like I said before, this is an observation-based model. So we weren't going out and trying to validate what our approach to software security is or our own philosophy. By contrast, we were trying to figure out what's actually going on out there in the world in these large firms and describe it according to that framework.

Julia Allen: Excellent. So since you're headed in that direction, let's talk a little bit about who you've been working with. When we first talked back in '09, it was based on nine firms. And now you've worked with 30 organizations and broadened your market sectors, and obviously collected a lot of additional observed practice about what these folks are doing in their software security initiatives. So who have you been working with and how have they participated in evolving the model?

Gary McGraw: So the data is absolutely critical to the model and so the 30 firms were very, very much important to our work. We couldn't have done it without talking to these 30 firms. I do want to mention one thing about the number. The first study that we talked about was a study of nine firms. And it was very useful because it was observational. It was based on real data. But now that we have 30 firms in the study, we can actually do statistical analysis of the data that we have gathered.

And we can tell you much more certainly what's going on out there in the world from a software security perspective -- what works, what's common, what's not common. And we actually validated the model that we originally built by collecting more data.

So of the 30 firms, 20 of them will allow us to say who they are, which we're very happy about. And they are, without any further ado: Adobe, Aon, Bank of America, Capital One, The Depository Trust and Clearing Corporation (also known as DTCC) EMC, Google, Intel, Intuit, Microsoft, Nokia, Qualcomm, Sallie Mae, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, VMware, and Wells Fargo.

So you can see, it's quite a big list of companies and representative of many different verticals, including financial services, independent software vendors, technology firms, healthcare, insurance, energy, and media

Julia Allen: Well with that kind of a dataset and that kind of organizational participation behind you, as you said, you can start doing analysis. But it seems to me you're getting to a very robust set of observed practice that we can all benefit from.

Gary McGraw: Yeah. And you know one of the neatest things about the project has been the sense of community that's developed among and between the participants. So as you can imagine, people who run software security initiatives are busy people. And they're busy working professionally to solve this very hard problem that we're all interested in, software assurance, how do you do that.

One of the cool things that's happened is they've all met each other, these guys. And so now we have a moderated mailing list for people to discuss questions that come up and things that other people have worked on and asked for good advice. And in fact, we're going to have a conference in the fall in Washington, D.C. in the November timeframe for those participants to get together and to meet each other.

Part 2: Key Activities; Most Commonly Observed Activities

Julia Allen: Excellent. So Sammy, I think it's time for you to get involved in our conversation. So based on your work with the model and talking to organizations, what have you found are the key or most important practices to set up a successful initiative?

Sammy Migues: Well, so I'm going to differentiate the use of the word “practices” there because we use practices as one of the terms for the software for the BSIMM itself -- in other words, the 12 practices into which we have the activities, as opposed to the “activity” that we see in the organizations.

So some of the most common activities that we see that help organizations actually become successful have been based around having an actual software security group (SSG) itself. In other words, they have put somebody in charge and they have started an initiative and they have actual focus on getting software security improvement across the enterprise.

This has been key to success in all 30 firms that we've seen. And this is not just our observation. This is what they have told us specifically, "This is how we got it done." So that seems to be a really big part of it.

A second part of it is actually having enough of a software security group to go around. Now what we've seen as an average is about one percent. That is to say about one software security group person dedicated to helping developers get software security right per 100 developers.

So 500 developers should be, if you're following the averages, about five people in your software security group. And that seems to be the average that is holding true, not only from the original nine firms, but that has held true across the 30 firms. And it's not exactly one percent in every firm but that is the average that is holding. So it seems to be a pretty good number of people to work with.

And we've got to keep in mind also that this ranges across, as Gary mentioned earlier, some very sizable organizations where we have an SSG size that's about 22 people. So these numbers have run from very small SSGs, one or two people, to very large SSGs that have, nearly 100 people in them. So it's an interesting take away from the study so far.

So that's one part of it. The second part of it is the SSG structure itself. And that is it is typically at the higher levels of the organization. We have people who are running software security groups that are no more than, let's just say, three or four hops away from executive management, from the CEOs themselves. So they have the ears of the people who can really put resources against the problem. And this is key to success in a lot of areas. But it's certainly key to success in software security.

Also, it's been organized in a way that has allowed the software security group to put feet on the ground for very specific problems. In other words, we've seen software security groups organized directly around the kinds of problems the organization has had. So we'll see someone in charge of making code review happen. We'll see someone in charge of making sure that all of the requirements, nonfunctional requirements, that need to come from compliance and privacy and 800-pound gorilla partners and others really get fed into the software development process.

We'll see someone specifically in charge of making sure that, for example, pen (penetration) testing and other things are ensuring that bugs are being removed from code before they go into production. So that organizational ability towards solving problems or that organizational structure around very tightly focused objectives seems to be a way to go in a lot of organizations these days.

Julia Allen: Okay, I also notice looking through your materials that as a complement to the SSG, you've observed this construct of what you're calling a software security satellite. Can you say a little bit about that?

Sammy Migues: So that's another very key point. There aren't enough software security people to go around. It doesn't matter where you look. If you look at it on a microscopic level within a business unit or on a macroscopic level across the planet, there just aren't enough.

So having some grassroots efforts across an organization to help you get software security done appears to be critical to success. We refer to those people who don't report directly to the software security group but whose interests and proclivities lie in helping get software security done, the satellite.

And people should not be picky about where their satellite is. In other words, you will find some people in your business analysts, in your product managers, in test, in production, in ops (operations), in development, who really care about software security and want to help make it better.

You should recruit all of those folks however you can -- training, pizza and beer, whatever it takes, and get those folks on board and have them working towards software security with you. That seems to be a key to success.

Julia Allen: Excellent. Well, in addition to the software security group and the satellite, I know in one of yours and Gary's articles, you talk about other common practices that you've observed that seem to occur most frequently for organizations that have a software security initiative. And I don't want to go through all of those today, but could you maybe pick out a couple of your favorites?

Sammy Migues: Sure. So what we're talking about here is most common activities. What we have in the 30 firms is 15 of them. So in this current dataset we have 15 most common activities, which we define as activities that are being performed by at least 20 of the 30 firms.

And so we have, as it turns out, coverage across all 12 practices with those common activities, which is an interesting thing in and of itself. Now me, I'm kind of partial to pre-work and planning and strategy. So some of the ones I like are the ones in, for example, in strategy and metrics. There's a common practice of identifying gate locations and gathering the artifacts on how these gates work.

In other words, it is very common across the 30 firms for an SDLC (software development life cycle) to be documented and within that SDLC documented to have security gates documented and for people to actually be actively working these gates.

Now, there's another activity that talks about making the gates mandatory and that happens a little less frequently. But at least identifying the gates is a very important thing. In compliance and policy, another very common activity is knowing all your regulatory pressures and unifying approach -- which is to say, how do the software guys understand the kinds of requirements that are coming from other organizations or outside the firm that are nonfunctional, not just what it takes to make a piece of software go, but what it takes to make the piece of software acceptable to the people in the firm and the people outside the firm.

And I'll just give you a couple of other examples very quickly. For example, in training, providing awareness training for everyone and then say, security features and design, building and publishing security features -- which is to say, start pulling some of the common things out of the organization, making them secure in the first place, and then pushing them back to everyone so everyone isn't trying to reinvent the security wheel all the time.

Julia Allen: Well, you might expect that given that I'm coming from a CERT perspective that one of my favorites is to identify software defects found in operational monitoring and feed them back into development. I think often the ops side doesn't really help inform the development side. Can you or Gary comment a little bit on that on, in terms of what you've observed?

Sammy Migues: So what we've seen is a security operations focus in some of the 30 firms, where in addition to the typical ops folks, we'll see some folks in that organization or with that purview who are really more interested in security itself. And they're watching for anomalous behavior in apps (applications) that goes above and beyond what the typical ops folks might be looking for -- like “We're taking up too much bandwidth all of a sudden. What's wrong?” And they might not associate that with an attack right off.

The security ops folks are a little more interested in why is this app misbehaving and is it an attack? And if it is an attack, what should we do right now? Should we block part of it? Should we take it down? What should we do? And then working with the development folks to figure out whether that was actually a software security defect and making sure that the defect gets fixed and makes its way into ops.

So it's just that extra focus, which may in fact take an extra person pulling things from ops to dev (development) and back into ops that seems to be a very common activity these days.

Part 3: Making the Business Case; Getting Started

Julia Allen: Excellent. Well, one of the reasons I picked that one too is I think it's a nice segue into my next question for Gary, which I ask you this every time, every time talk Gary. And I know it's one of our tougher issues. But making the business case for all of this work in the face of everything else an organization is doing. One of the ways I like to make that business case is the ops impact of a software defect and had you addressed that defect earlier in the life cycle, you would have saved a bunch of money and a bunch of time.

But from your vantage point, with all these organizations -- you've had the first version of BSIMM out in the field for a while and obviously adding to it with this next version and so many more players. Have you started to form an opinion or a view or an observation of the benefits and the cost savings or other aspects of business case that make using BSIMM compelling?

Gary McGraw: So, less than I would like is the honest answer. Everybody who has a software security initiative under way has already convinced the business that it's an important thing to do. And not only that, it has funding to create an SSG and find an executive to run the SSG and to really make a cultural change inside of development. So we have kind of a captive audience, so to speak.

But if you look at all 30 stories of the way these software security initiatives were engendered in all 30 firms, you never have the same story twice. I will tell you this though. We have had a couple of the firms that are involved in the study use BSIMM results to help them to justify way up the chain at the board level, the kind of expense and budget that they're requesting. And not only that, they've been able to then later go back and demonstrate that the things that they're spending money on are actually effective, and they are in fact impacting software security in the right direction. So that's quite a nice use of the BSIMM that we really didn't anticipate.

I think that what we're seeing in the field is a maturity where we're moving away from selling sheerly on fear, uncertainty, and doubt, which was the early days, to regulatory concerns, which was the middling days. And now it seems like people are understanding that the world is implicitly, if not explicitly, demanding security. And therefore, you need to think about product security from the get-go. I think that selling a software security initiative at Adobe right now, for example, is nigh on trivial because they're finding out what happens when you didn't pay attention to that for a while.

Gary McGraw: And the good news is that Adobe has made huge strides in software security and they're using the BSIMM to be able to measure the effectiveness of what it is that they're doing.

Julia Allen: And I would think, you made the point earlier about now that you have data from 30 firms you can perform various types of statistical analysis for both model validation but also teasing out the common practices, best practices, most frequently used practices. And I would think having that observation-based data would be a great argument for a business case, would you think?

Gary McGraw: It absolutely is. And not only that, we've published the data so they're available for anybody to use to make a business case around software security. And I think that some people are taking advantage of the data that we've published, and we'll continue to publish those data.

I think that one of the important things about software security is getting an understanding of what your customer wants out there, what your customer is expecting. And forward looking firms have already begun to understand the importance of building products that are secure or services that are secure in terms of financial services. And we've see this field grow over the last decade. It's been pretty amazing to watch. And I'm actually aware of about 70 firms that have software security initiatives under way now. And we've studied about half of them. So we're going to continue to gather data and continue to report that data.
We have a community that has been developing around the BSIMM. And the community has decided that it wants to work on this cost issue and effectiveness issue together. We all think it's going to be quite a challenge to try to figure out how to describe how effective, say, particular activities are or particular practices are when it comes to software security. But it's something that we've sort of put on the agenda for the fall, and something that we hope that we can collectively come up with data that can help people figure out how to even divide up their money pot when it comes to software security between various activities and think about effectiveness that way.

Julia Allen: Great. Well, before I take us to our close, we've talked a little bit about where you think you're headed next for BSIMM. I did have one last question for Sammy. And that is, Sammy, for those who are just getting started or just thinking about this, do you have some observations or advice for getting started? Is there a set of practices that is a good or effective place to start that you would recommend for those who are just starting to dip their toe in the water?

Sammy Migues: Yeah. So I'm going to tackle that in two ways. The first way is from the program perspective. As I mentioned earlier, the first thing to do is just to put somebody in charge. And it has to be somebody who can actually get things done. I would not necessarily say that this is a developer or the lead developer. This is someone in the executive ranks who can actually make software security happen.

And the first thing I would recommend that that person do, and I'm sure we'll all have a different opinion on this, is to look around and see if there are any already existing pockets of goodness, as it were, in the organization. Is there anyone or any process that is already producing some software security goodness in some way? If so, take advantage of that in any way that you can.

A next part of it will be to figure out what's important to you with software security, as opposed to trying to do a little bit of everything you've ever heard of. There's going to be some privacy things, some compliance things, some top attacks or top vuls (vulnerabilities) that are important to you as opposed to all the generic stuff out in the space. Work with that to set up your software security program. And if you're going to get some automation, customize it for you. Don't use just off-the-shelf thing and take it as it sits.

The easiest way to get those sorts of things then is to use the BSIMM as a level set. So again, these are the things that you want to accomplish and you want to drive it to your business objectives. But if you use the BSIMM as a level set for what you have and what you need, then you can figure out exactly how to approach these individual things. And then if you're looking for some suggestions down at the actual activity level, then you can just fall back to the 20 most common activities.

Again, if they're most common against 30 organizations in multiple verticals across multiple sizes, then maybe they're most in common for you too. And that's probably a good place for you to start once you have an organization up and going.

Julia Allen: Excellent. Well thank you very much. So Gary, you started to lay the groundwork for where you're headed in the next period of time. Are there some other things you wanted to mention about what's next for BSIMM and some places, in addition to the BSIMM website, that you might like to point our listeners?

Gary McGraw: Sure. So the most important thing is for everybody to understand that the BSIMM is a continuing project, that we are actively seeking other firms who would like to be measured with the BSIMM and get involved in the project. And in fact, we've already measured a whole number of firms beyond the 30 so far, since I guess we released that in March was that?

Sammy Migues: Mm-hm.

Gary McGraw: And so if you're interested in participating in the BSIMM and becoming part of our community, by all means, get in touch with us and we'll try to get you factored into the initiative.

The other thing that's going on is some of the earliest measurements that we made in the BSIMM were made about, I don't know, 12, 15 months ago, a little bit over a year. And we're beginning to go back and re-measure firms that were already measured once. And it's very, very interesting.

So we're hoping to push the science in the way of being able to describe how people are improving their software security initiatives, which activities they're adopting, which ones may be falling by the wayside, how they are investing their limited resources to get software security done, and what the best in the world are doing when it comes to software security.

So that's another way that the BSIMM is growing And then as I said before, this community is beginning to emerge. We've built an advisory board for the BSIMM that includes Steve Lipner from Microsoft and Eric Baize from EMC and Jeff Cohen from Intel and Yana unpronounceable-last-name, I think it's Uselito [ph?] from Nokia, and Brad Arkin from Adobe. And together with those guys, we have been talking about enhancing the community, having a conference in the fall. We built a moderated mailing list. And we'll probably double the size of the BSIMM study for BSIMM3, which you should expect sometime early next year, I suppose. We'll talk to you again then, Julia.

Julia Allen: Excellent. Well Gary, thank you so very much for your time, for keeping me on your hit list as the new developments happen. I sure do appreciate it.

Gary McGraw: It's our pleasure. And we think that the people that listen to your podcasts are perfect targets for getting involved in the BSIMM.

Julia Allen: Excellent. And Sammy, thank you so much for your time and advice. I appreciate the opportunity to talk with you as well.

Sammy Migues: I thank you also, it was great being here.