An Experience-Based Maturity Model for Software Security
Transcript

Part 1: Motivation and Target Audience; Drawing from Observed Practices

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 security governance and software assurance. Today I'm very pleased to welcome three people to our podcast series – this is a first: Gary McGraw, who is the Chief Technology Officer for Cigital, Brian Chess, Chief Scientist and Co-founder of Fortify Software and Sammy Migues, Principal Consultant and Director of Knowledge Management for Cigital. Today we'll be discussing their efforts to develop a maturity model for building security into software throughout the development life cycle based on analyzing real world experiences from a number of organizations that they've been working with. So first, I'd like to welcome everyone so you all can recognize their voices. So Gary, great to have you.

Gary McGraw: Great to be here, Julia. I suppose I could pretend I'm Brian.

Julia Allen: That'll confuse everybody for sure. So Brian, how are you doing?

Brian Chess: Doing well. Gary, you behave.

Julia Allen: And Sammy?

Sammy Migues: Hi Julia. Thanks for having us all here. We really appreciate it.

Julia Allen: Okay, well this will be fun. So why don't we start with Gary, just to kind of direct traffic a little bit. Obviously you've all launched on this effort for some very compelling reasons. So why do you believe we need a maturity model for software security and why now?

Gary McGraw: Well, software security has been in practice for about 10 years now. And we've been trying out a lot of good ideas. It turns out that there are a number of organizations that have been carrying out software security for this decade. And there are plenty of things to learn by studying real programs that already exist.

So we have plenty of methodologies in software security that are, you might consider them religions. There's the Cigital Touchpoints, Microsoft's SDL, OWASP's CLASP. But we thought it would be a good time to study successful programs and we chose nine of them out of the thirty-three that we know about, and figure out what exactly they're doing. Our plan was to create a yardstick that you can use to measure your own software security initiative that will allow you to understand where you stand next to your peers, and among your peers, and help you to plan large-scale evolution of your software security program.

The main constraint that we had was we swore up and down we were only going to use real data. So though we have a lot of great ideas about software security, and we've certainly all three been practicing it for many, many years – collectively probably over 60 years – we stuck to that constraint, which is if we didn't observe something in the data, it wasn't allowed to be part of the model.

So the yardstick is a very much real yardstick that we've got. And we're pretty excited about the results.

Julia Allen: Well that's great. We'll get into some of the experience base. But I think that makes it a lot more compelling for potential users. So speaking of that, Sammy, who do you feel are the best or most intended audience or users for the model?

Sammy Migues: Well, we'd like to see a couple of different groups pick up the yardstick as it were. Probably the first group is the executives. We want to see the CIOs, the CISOs who are responsible for software security initiatives. We want to see those guys pick up this yardstick and drive it into their organizations. Now not necessarily as a stick, so we don't mean to be too literal there. I mean they can drive the yardstick into the organization as a carrot too. “So here's some things that if you're pursuing I can give you some resources for because they make sense.”

And then of course, there's the software security groups themselves. So we'd like to see an SSG that's in existence in an organization pick this up and say "Here are some activities I could be doing because there are other organizations out there, really good ones, really big ones, who are doing these sorts of things.

And if there are some things here that I'm not doing, I should probably think about that.” And start looking around, herd all the cats, because there's probably going to be some pockets of goodness around the organization where somebody's doing a little security here or a little security here. And start bringing that in under one umbrella, under the BSIMM, and start sort of harmonizing those activities and pushing it back into the organization. So I would see those two groups really focusing on using the BSIMM.

Julia Allen: It's always good to have a yardstick or a benchmark or something that's been vetted to compare your current practices against and then be able to kind of place yourself somewhere on that spectrum.

Sammy Migues: Absolutely. And understand that as you've probably heard, that these are things that people are doing. There's no made up stuff here.

Julia Allen: So that's a great segue. So Brian, both Gary and Sammy said a little bit about the genesis of the model. But can you tell our listeners a little bit more how you came to develop it and who you drew experience data from?

Brian Chess: Sure, I'd be happy to. This is probably the project that's going to get me the closest I'm ever going to come to doing anthropology. The way we built the model was by interviewing the executives at nine companies. These are the executives who are in charge of the software security initiative.

So we picked four financial services companies and three independent software companies and two technology companies. In all, we did about – oh boy, let's see, about 18 hours worth of interviews with these nine executives. And tried to understand what their practices are and what activities they're actually carrying out in their organizations in order to build secure software.

So seven of the nine companies have been gracious enough to allow us to use their names. So let me rattle them off for you. So we talked to executives at Adobe, EMC, Google, Microsoft, Qualcomm, Wells Fargo, the Depository Trust and Clearing Corporation, more properly probably known as DTCC. And then two more companies who would prefer to remain anonymous.

Julia Allen: And hopefully as the model becomes more familiar, the word gets out, that more organizations will be beating a path to your door to contribute their practices as well.

Gary McGraw: That's the plan. And we've seen that already evidenced that people are psyched to get involved already.

Part 2: Structure and Scope; Where to Start

Julia Allen: So Gary, tell us a little bit about – to make this more tangible for our listeners – a little bit about the structure and scope of the model.

Gary McGraw: Well, we built a software security framework before we got started with the interviews. And the framework was a way to help us frame the conversation around all of these 110 activities. The framework has 12 practices in it. And I'll just give you a couple of examples. One practice is training, another practice is architecture analysis, another one is strategy and metrics.

Those are divided into four major domains. And basically the 110 activities that we identified – all of which were observed in the real world – are captured and described in the model. And in fact, if you get into the heart of the model itself, if you download the document and check it out – and we're going to release the whole thing under the Creative Commons so you could use it any way you see fit. You can find that each one of the 110 activities is described in a paragraph that includes the objective, the activity, and two or three examples for each activity.

Now all of the examples that are in the document are real examples. So not only do we give you some ideas of what activities are successful – or successful companies are carrying out – we also give you some stories about how they were carried out in particular. That doesn't mean that's how you should do it but it does mean that this is something that's very much real world.

Julia Allen: So I would expect, in looking through it, that I'll see some practices that I'm familiar with: about secure coding practices and using static analysis tools and maybe doing some assurance case or attack pattern work. Were there some things that were surprising? Or did you find in talking with the nine organizations that it mostly validated what you already knew?

Gary McGraw: There were things that were surprising. And we've actually written a series of articles for InformIT that describe the results in different ways. One of the articles that we wrote was about ten surprising things that we learned while we were working on this material.

I think one of the things that surprised me the most, though Brian and Sammy may differ a little, was the fact that everybody used fuzz tools. And we knew that fuzzing tools were something that people could use in their penetration testing and in their security testing efforts. But we really didn't anticipate that everybody would be doing fuzzing. And not only that, doing fuzzing in a very sophisticated manner that took advantage of things like their own internal class structure and APIs.

Julia Allen: That's pretty interesting. So just moving along, Brian, let's say that I wanted to take a look at this, try it out, take it for a test run, either on a current project or something that I've got in the pipeline. So just as a first steps type of advice, who should lead the charge on looking at and adopting the model? And where do you think is the best place to start?

Brian Chess: Well let me say, it's not appropriate to try and apply BSIMM to an individual software project. It's really about building a software security initiative for an entire organization.

Julia Allen: That's a good clarification, thanks.

Brian Chess: Sort of the bottom bar from our point of view about what you have to have in order to get started is you've got to have enough executive buy-in in an organization that you can form a software security group. If you haven't dedicated any people to the task of making sure the software is secure, you're probably not ready for BSIMM yet. But hopefully you are ready to create that software security group. So I think number one activity is enough buy-in to say it's time for some people to go and solve the problem.

Now at the organizations we're looking at, they've been at this on average for about four and a half years. So they're well into creating a software security initiative. I'd say one of the most interesting outcomes that I just didn't know was going to come out of the interviews we conducted was that the size of that software security group tends to average around one percent of the size of the software development group.

Now I would say one of the problems people have always had trouble with is how do I know I'm spending the right amount of money or effort on security? And now we at least can tell you how much some of the leading organizations are dedicating in terms of people power to the effort.

Julia Allen: And do you find some places where the software security group recommends that their development project's a place to start, or does it really kind of depend?

Brian Chess: So, we do see organizations come in from different angles. The financial services folks tend to be a little stronger when it comes to policy and compliance issues, whereas the software vendors tend to get better attesting faster. So there's no single right place to start. And BSIMM doesn't tell you how you have to come at things. So it's not a cookbook.

But there are a lot of good ideas in there including 10 practices that everybody who we talked to are carrying out. And that includes things like training. It includes some technology components. It includes having that software security group get good at carrying out an activity before that activity is rolled out and carried out by the entire organization.

Part 3: Setting Expectations; Making the Business Case

Julia Allen: Well Sammy, what results can I expect? And when might I start to see some benefit or payback from this investment?

Sammy Migues: Well, that's an easy question and a really hard question. So the easy answer is, you're going to get a yardstick, as we've said before, for the common good. You're going to get something that everyone in your initiative, everyone in your software security group, can rally around and something that's easily understood and hopefully easily consumed, pushed out into your organization. So that's really the easy answer to your question.

The harder answer is when will a particular activity get better? And again, that's going to be really tough. So what's going to happen is, you're going to look at these items and you're going to say, "Well, there are some things here that just don't apply to me." And then you're going to say, "Here are some things that do apply, and I'm going to prioritize them this way."

What we're claiming, what we're saying, is that when those things get applied, they're going to get better. As Brian said, certain organizations have decided to focus more on compliance things, other organizations have focused more on testing things. The point is that when you do a variety of these things, all the rolled up benefits are all going to aid each other. So it just helps itself roll along.

The point is you're going to pick something that's right for your culture, you're going to work on it, and now you're going to have a framework for actually doing that.

Julia Allen: What we've found in our Capability Maturity Model Integration (CMMI) work is in putting together an oversight group or a software engineering process group like what you described for the SSG, you try and look for some low hanging fruit. You try and look for some quick wins. Because if you're able to demonstrate something early in the adoption process, it starts to help build some momentum. So do you find with the organizations you talked to a similar approach when they're getting started?

Sammy Migues: Well, so a lot of these got started years ago. But I'd say the answer is yes. You'll find that some, got started on the old vulnerability testing organizations of years ago. Some got started out of network security. Some grew perhaps even out of training or development organizations. And so they got really good at that stuff and started doing other things later.

And I think you'll find the same thing will happen now with people who are just getting started. They'll find some things they're really good at. They'll do more of that and they'll keep adding other things one at a time.

Julia Allen: Well Gary, as we come to our close, here's the – it probably used to be $64,000 question, but maybe now it's $640,000 question. Or we may be talking billions and trillions, the way things are going these days.

Gary McGraw: I think it's more trillion by this point.

Julia Allen: Right. So given all the demands that a business is attempting to address, and always limited resources, how have you been successful making the business case for efforts of this sort, for a building security in maturity model? How do you go about that?

Gary McGraw: So there are two specific answers to this question. The first is, everybody wants to know how their effort compares to everyone else's. And the BSIMM provides a very clear yardstick and a set of benchmarks for understanding where you stand among your peers, which is particularly interesting.

Every executive wants to know if they're spending enough, if they're looking like the Joneses, if they're keeping up with the Joneses, and where they're falling behind and where they're leading. The BSIMM can tell you that.

But we also designed the BSIMM with the notion of objectives and goals directly in mind. And in fact, on one of the pages is devoted entirely to goals. So you can have a conversation with upper-level management and ask if they would like to, say, make informed risk management decisions. Or figure out what the right thing to do for everyone involved in the SSG is. Or reduce costs through repeatable processes. Or increase code quality. And these are all, of course, motherhood and apple pie business goals. And once you get people to buy in on wanting that goal then you can tell them how much the car costs.

So we structured things on purpose so that carrying out that conversation at the business level would drive from a business perspective the technical activities and not the other way around.

Julia Allen: Recognizing the market sector differences in some of the companies that you've worked with, you talk about users of the model, or anybody wanting to be able to compare their practices with someone else's. Were you able to get some good benchmark data on the cost and the returns as you collected these practices from your organizations?

Gary McGraw: The short answer is no.

Julia Allen: Okay. Well, hopefully, over time if we put some of these practices in place, we can start to do some benchmarking to get some hard data.

Gary McGraw: Well, let me address that a little bit more. I mean, what we found is everyone uses metrics. And everyone uses business-related metrics that include cost and cost savings and remediation costs and things like that. However, what we discovered, and this kind of surprised us as well, is that metrics are applicable in a particular business culture.

And so metrics that work for one of the nine organizations would never work for another of the nine organizations. Nevertheless, they all had their own metrics. So that's kind of an interesting result in its own right. It looks like more anthropology is needed.

Julia Allen: So Brian, how can I – just some logistical information – how can I access the model? Gary said it's going to be available under Creative Commons. So can you say a little bit about how you plan to roll it out?

Brian Chess: So we've set up a website and you can go to the website and explore the model in a sort of an interactive fashion. You can drill down on those domains and into the practices and look at all the activities within a domain. We're also distributing it as a PDF. So if you want to just grab that PDF and start copying and pasting into documents for your own initiative, then all you need to do is cite BSIMM, and away you go. So we hope that this information gets used to create a lot of initiatives.

Julia Allen: Well that's great. And we'll make sure to put all that information in the show notes. So from any of you, Gary, Brian, or Sammy, do you have any other sources you'd like to point our listeners to or any closing thoughts?

Sammy Migues: Well, I mean, there's the three InformIT articles. They describe the software security framework. They describe the interesting things, the surprising things that we found and they describe the things that we found that everybody does. People might want to start there. They're a little easier to consume than the entire BSIMM. But after that, really it's the BSIMM itself. And start walking through it slowly, read through the activities, kind of see yourself in the document, and get a feel for what it entails and doesn't entail. And that's really where you're going to start to understand what it really means.

Brian Chess: Let me say one more thing, Julia. We're hoping to expand the model. We think nine data points is a great start but we want to get some more in there. And we're going to be selective about how we do that. In other words, we're not going to let anybody self-audit. They can't treat this like a checklist and go down the list of 110 things and claim that they do every single one.

So if people find that useful for their own purposes, great. But when we incorporate more data into the model, we're going to do it exactly the same way that we did it with these first nine. We're going to conduct an interview and we're going to map organizations into the model.

Julia Allen: And can people get in touch with you through the website?

Brian Chess: Absolutely.

Julia Allen: Gary, anything in closing?

Gary McGraw: Sure. My last words are that we've been doing software security very much like alchemy was practiced. A lot of experts with lots of ideas about how to turn lead into gold. And the time for alchemy is over and the time for science has begun. So I believe that we're turning a corner in software security and starting to do data-driven activity, like the BSIMM and other things where we're actually collecting real data from the field and using that to make decisions is the way forward.

Julia Allen: Well, we've all aspired to trying to bring the engineering to software, and now software security, so this could be a big step in that direction. I want to thank you all so very, very much for your time and your expertise and your efforts today. And I look forward to spending a little more time myself with the model. So thanks very much.

Brian Chess: Thank you, Julia.