Building Security In Maturity Model (BSIMM) – Practices from Seventy Eight Organizations

Part 1: Target Audience, Structure, Addition of Healthcare Vertical

Lisa Young: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division 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 Lisa Young. I'm a member of CERT's Cyber Risk and Resilience Management team. Today, I'm pleased to welcome back Gary McGraw, CTO of Cigital. Today, Gary and I will be discussing their continuing efforts on a maturity model for building security into software throughout the lifecycle.

Today's podcast is an update based on a prior podcast we did back in 2010 -- hard to believe so much time has passed -- and is based on the real world experience of 78 organizations in 9 market sectors. So, Gary thank you so much for being here. And thanks for making the time to talk to us again.

Gary McGraw: Absolutely, it's my pleasure to be here. Thanks for having me on.

Lisa Young: So, for our listeners who may not be familiar with the BSIMM, the Building Security in Maturity Model, and its purpose, can you just give us a brief idea of what it is?

Gary McGraw: You bet. So, you can learn about the BSIMM on the BSIMM website. It's bsimm.com. The BSIMM is a measurement tool for software security initiatives. That is, when an organization that has lots of developers is trying to figure out how to change their culture in order to build more secure software, the BSIMM is extremely helpful along those lines.

We started the BSIMM project about 8 years ago, and we started by gathering data from 9 firms. Now, with the 6th iteration of the model, BSIMM6, we've actually described the work of 78 firms. We've measured a whole lot more firms than that, but we pay very close attention to data freshness and data correctness. So, some firms that we've measured are no longer part of the project.

The 78 firms build lots and lots of software and, in fact, have 287,000 developers. So, describing the work of a whole lot of people, not just a few. Let me just list what some of those companies are among the 7878. And I'm going to do this quick in alphabetical order.

So, there's Adobe, AETNA,ANDA, Autodesk, Bank of America, Black Knight Financial Services, Bank of Montreal Financial Group, Box, Capital One, Cisco, Citigroup, Comerica Bank, Cryptography Research, DTCC, Elavon, EMC, Epsilon, Experian, Fanny Mae, Fidelity, F-Secure, HP Fortify, HSBC, Intel, JPMorgan Chase, Lenovo, LinkedIn, Marks and Spencer, McKesson, NetApp, NetSuite, Neustar, Nokia, NVIDIA, PayPal, Pearson Learning Technologies, Qualcomm, Rackspace, Salesforce, Siemens, Sony Mobile, Symantec, The Advisory Board, the Home Depot, Trainline.com, TomTom, U.S. Bank, Vanguard, VISA, VMWare, Wells Fargo, and Zephyr Health. So, that gives you some idea of the breadth. We have lots and lots of companies where we've gone out and gathered real data. And then we built a model to describe those data, which can then be used to measure how a software security initiative is going.

Lisa Young: Well, that's awesome so that actually answers my next question, which is who is the intended audience for the BSIMM? And it sounds like there's quite a number of people who could benefit from this type of observational model.

Gary McGraw: Yeah, what happens in the real world is software security turns out to be the job of lots of people in an organization. First of all, there's a central core group that we've always observed in all of those 78 firms, which we call the SSG. That's short for Software Security Group. And then there are all the developers. There are all the people in QA. There are the product managers. There are the senior executives. There's even the CEO and the CTO. So, all of these groups participate in a software security initiative.

Lisa Young: So, all these groups participate in a software security initiative. And then can you say more about how the model is organized and scoped?

Gary McGraw: You bet. So, based on the data that we gathered from the field, we have identified a 112 activities that are divided into 12 practices and described very carefully by the model. And what we do when we do a measurement is we go out, and we have in-person interviews that are pretty extensive. And then we try to determine whether or not a firm that we're measuring is carrying out each of those activities.

We don't ask about those activities in a checklist fashion. Instead, we ask open-ended questions. And we gather lots of data which we then put into our BSIMM framework. So, there's a software security framework that describes 12 practices. And it includes things like code review as a practice, penetration testing as a practice, training as a practice, attack modeling is a practice. So, that gives you some idea.

It's very important to note that we didn't build a set of activities and prescribe the way we think software security should be done. Instead, what we did is gathered data from firms that are actually carrying out and doing software security all the time. And we used those data to drive the model. So, the model is very much, like you said, observational and linked to real data from the real world.

Lisa Young: Well, and certainly those organizations that you mentioned are seen to be high performers in the industry. So, observing what they do then would help someone else maybe get better at doing software security.

Gary McGraw: That's exactly right. And we've even seen that happen between verticals, if you will. We've measured a whole lot of financial services organizations. In fact, we've measured 33 of the 78 firms are from financial services. And we've measured a whole bunch of independent software vendors in our population.

There are 27 of the 78 firms are big software vendors. And the work of those firms actually helps to inform those verticals that are just getting started with software security, for example, healthcare. And BSIMM6 covers healthcare for the first time. So, that's pretty cool because the leaders can show others what to do, and how to do it, and how to measure it.

Lisa Young: Well, I think that's really significant, too, because there's already a ton of compliance regulations, standards, guidelines, all kinds of things. But can you say, since this is the first time healthcare organizations have been part of the BSIMM data set, can you talk about the significance of that and possibly why compliance regulations like HIPAA haven't helped them improve in this area?

Gary McGraw: Sure. Regulation and compliance is very tricky. And it's important to talk about. And in fact, one of the practices, one of the 12 practices in the BSIMM, is about compliance and policy. So, you should understand that we recognize the importance of that sort of thing. What often happens in compliance regimens is that a compliance regimen will tell you what to do. Or, they'll describe what a goal state should be. But they won't describe how to do that. And so, the how is really important. And that's where the BSIMM really is helpful.

There are many firms in the BSIMM study that are constrained by lots and lots of different regulations, For example, in financial services you have DOCC, the FFIEC. You've got Basel III. You've got SOX, Sarbanes- Oxley, GLBA 2. There's all sorts of stuff that applies to financial services firms. And the same goes for healthcare. Now, one of the problems in healthcare regulation has to do with HIPAA. And that is that HIPAA is really mostly about patient data privacy. That's an important matter. But software security also covers things like how secure your medical devices are.

So, because HIPAA caused a lot of firms to pay lots of attention to patient data privacy, it sucked up all the oxygen in the room, meaning that healthcare firms didn't have any oxygen left to work on things like security engineering, and building secure and safe medical devices, and so on. And it's important to realize that those aspects of healthcare security are, in some senses, even more important. I mean look, if you're a patient, you don't care if your data gets leaked if you're dead.

Lisa Young: Right. No, that's very important. And I appreciate that. I actually really like the governance domain because it includes this compliance and policy. But it seems to me, as I look at it, it's more of a rationalization of making compliance as efficient as possible in the software lifecycle.

Gary McGraw: That's right, because if you have lots of compliance regimens and regulatory issues that you have to deal with, if you unify those and you create a security engineering methodology that aligns with those, then you can do the work you need to do and have all of that stuff that you need for compliance come off as the side effect.

Lisa Young: Right. Compliance is a byproduct of doing the right things. I like that.

Gary McGraw: Yep. Yep.

Part 2: Getting Started

Lisa Young: So, my background is in risk management. So, for me, when I look at the new version of BSIMM, I thought this really could fit in with such a nice view of risk management across the organization. And it's funny because I know a lot of people don't actually think of software as a security function. But it truly is in large organizations and independent software vendors.

Gary McGraw: Yeah, software is working its way into every aspect of business and every aspect of things that we use every day, our electric grid, our cars, all the consumer devices we have. Even the supposedly not technical devices that we have are getting software in them. And as software leaks into everything, sort of soaks the ground of everything in modern society, it's really important that we understand the security ramifications of that. If there's software in your thermostat, can your thermostat be attacked? And if a bad person takes over your thermostat, what can they do to you? And these are very important concerns that the BSIMM addresses head on.

Lisa Young: Well, that's really interesting, especially because now, like you said, the thermostat. We hear so much about software in this whole Internet of Things category every time we turn on the news.

Gary McGraw: Yeah, and in fact, the Consumer Electronics Association, which is now called the Consumer Technology Association as of I think last week, who just held the big show in Las Vegas, believes that security is really important for consumer grade devices. And they're taking a very close look at the BSIMM for their membership, which is really cool.

Lisa Young: Oh, that's awesome. Well, so based on your work with the model and talking to all these different types of organizations, have you found any key or most important practices to set up a successful software initiative?

Gary McGraw: Well, we do take a look at all of the hundred and twelve individual activities. And we have identified some activities that are commonly found in most BSIMM firms. So, there are 12 particular activities that we call the core activities of the BSIMM. And we see those in just about 70 of the 78 firms. So, there are things that are very much like the hygiene, if you will. But those 12 are spread across the 12 practices. And so, you can't really say in order to approach software security you should start with a particular individual practice, for example, training.

Instead, what we find is that firms that are approaching this in a mature fashion are doing it in a well- rounded way so that they take some activities out of each of the twelve practices, and they put them into service. If you have a BSIMM measurement, you can compare yourself to the BSIMM population. And then you can use data to drive your initiative, which is really very cool.

Lisa Young: So, I like that approach a lot. And sometimes I hear people say, "*Well, a hundred and twelve activities, that sounds like a lot*." But I have to say a hundred and twelve efficient activities sounds like a plan.

Gary McGraw: That's exactly right. And having a plan is a lot better than just listening to whatever some vendor just said. Let me give you a particular example.

Lisa Young: Okay.

Gary McGraw: There's been a lot of focus in the press, and in the hype cycle about bug bounty systems. And in fact, bug bounties are something that we have observed with the BSIMM. But you should note that we've only observed bug bounty systems in 3 or 4 firms out of 78, actually out of way more than 78. As I said before, we've measured about a 120 firms using the BSIMM. And we've made a whole bunch of progress. We've measured many, many firms since we released BSIMM6. So, the BSIMM model is always growing. And we always use the data to drive the model.

But back to my point, things like bug bounties may be a good idea for some aspect of your software security initiative. But it is not the case that that's what you should do first. And it is not the case that many firms that do software security all do bug bounties. They don't. And so, you can use something like the BSIMM and the BSIMM data to describe the real state of software security in terms of observed activities and huge populations, or large populations of firms.

Lisa Young: So, sure that makes sense because out of the 78 firms that are in this particular version, if only 3 or 4 are doing bug bounties, it might indicate to an organization to make that a lower priority. What was the practice you said before? Like 70 of 78 are doing it. Something like that might be a more important place for people to get started or to see if they're doing something like that.

Gary McGraw: That's exactly right.

Lisa Young: Okay. So, you can help use it to prioritize all of the activities that you do in the software security group. So, that's actually a really important way of deciding what buckets of money get spent on what activities.

Gary McGraw: Yeah, let me give you some examples of really fairly easy and very, very common activities just so we can put a fine point on it. One is provide awareness training. That's T 1.1. Another is create security standards. That's SR 1.1. Or, when it comes to architecture analysis, perform simple security feature review, or in code review, use automated tools along with manual review. So, those are some very pithy descriptions of these activities. I should note that if you look at the BSIMM -- and you can download it for free. It's released under the creative commons for free for everyone off the website at B-S-I- M-M dot com.

If you download it, you can read very clear, paragraph-length descriptions of each of the activities, which are based on real examples from the real world, from the firms that we've measured. So, what makes the BSIMM really interesting, from a science perspective, is it provides a set of facts, and a set of measurements, and a measurement tool that you can use to compare and contrast your own approach to software security in your firm against what everybody else on the planet is doing.

Lisa Young: Sure, and I like it because what I found in looking through all of your materials is that it's really nicely organized and easy for a lay person, who might be managing a software security group, but maybe they're not -- don't have a software background to be able to say, "Are we doing these types of things," strategy and metrics, compliance and policy, training, standards and requirements. I really like that it's organized in plain English for -- even though I have a technical background, it's not in software. So, if I were to manage a software project or software security group, this would really be helpful for me.

Gary McGraw: It's really important to understand what others are actually doing and use that to drive the model. So, we drove the model based on data. And the fact is the data, in some sense, self-organized. So, that's why it's easy to understand because it's extremely logical based on a huge pile of actual, real world data that we collected from a bunch of firms that were happy to help their peers, and a bunch of leaders in the space who believed that having a collective data set like this is really the way to go and is important.

Lisa Young: I agree. So, you mentioned earlier this notion of a software security group. And I noticed also that there's a complement called a software security satellite. Can you say a little bit about that and what that looks like in these organizations that you've observed?

Gary McGraw: I sure can. So, software security -- when you're trying to control the work of two hundred and eighty-seven thousand developers -- requires a bunch of people working on software security full-time. And in fact, if you add up all the SSG members in BSIMM6, we're talking about a 1,084 SSG members.

The satellite is a set of people who are doing software security activities but who are not directly part of the software security group or line managed by the software security group. Instead, the satellite are people that might be in a product group, or in a QA group, or in a requirements management group. And in our BSIMM6 population, there are 2,111 satellite members. So, if you add up the SSG and the satellite, we're talking about 3,200 or so people that are doing software security full-time. And the BSIMM6 model describes the work of those 3,200 people.

Lisa Young: So, that's an interesting concept. So, the software security group, then, has more of a direct responsibility. And the satellites are interested parties and people who think it's the right thing to do, more like a volunteer army.

Gary McGraw: Well, I don't know if they're volunteers necessarily. That would be a nice way of putting it. Sometimes, they're co-opted volunteers.

Lisa Young: Okay.

Gary McGraw: But they're certainly a distributed army that is distributed throughout the entire firm. And what we've seen is a direct correlation between maturity, high maturity, and the existence of a satellite. And so, what we see unfold over time is a software security group will take on some activities, will understand how to put those to use inside of their firm, and then will get others to carry out activities as they mature so that they're spread throughout the firm.

Lisa Young: Okay.

Gary McGraw: And we see that over and over again. That's what the satellite is for.

Lisa Young: So, it's to radiate those practices, then, in the larger influence circle.

Gary McGraw: Yes, but I do want to state this for the record. We have never seen a firm without a software security group. But we've seen many firms without a satellite. So, you could never start with a satellite and then later add an SSG.

Part 3: Avoid Getting Eaten by Marauding Lions

Lisa Young: Okay, so that's a really good -- so then one or two good areas for people to start using the model then might be to set up a software security group, and what else? I assume they have to have some kind of sponsorship from senior leaders or management?

Gary McGraw: Yeah, that's something that we've also observed. In fact, there are two failure conditions for software security initiatives that I've seen over my 20 working in this space. One is there's a fantastic ground swell from development to do software security, but there's no executive support. And so, what happens is this ground swell of developers who want to do Sec DevOps, or whatever you want to call it today, hit the mire of middle management and just flame out.

The other failure condition is the pointy- haired executives on high declare everything will be secure. And everybody in development just looks up and says, "Oh, those people, flavor of the day. Great, it happens to be security this time." The way to avoid both of those failure conditions is to identify a software security group and identify somebody to run that software security group who has both authority and responsibility and the resources necessary to do this work.

Lisa Young: Okay. Well, that brings me to a question that we've asked on every podcast we've ever had. But how do I make that business case justification? What would be a good starting point for me to rally an executive manager to my cause?

Gary McGraw: Wow, you know what is funny? The best business cases I've ever seen, and I've been involved in about 20 of these cases, involve getting a baseline BSIMM score and then taking that to the board and saying, "Here are my peers. And here's us." And the board says, "Ooh, you mean everybody else in this population is ahead of us, and we're the slowest zebra? Isn't that bad?" And you say, "Yes, the slowest zebra, generally speaking, gets killed by the marauding lions."

Lisa Young: There you go.

Gary McGraw: And then the board says, "Oh well, gosh, what are we going to do to address this problem?" And you say, "I'm glad you ask." And you pull out your plan, and off you go, software security.

Lisa Young: Excellent. And so, that's the advantage…

Gary McGraw: And I've been personally involved in many, many of those activities at firms getting started. But yeah, having a measurement is unbelievably powerful.

Lisa Young: So, just downloading the BSIMM, going through your own practices, seeing how you compare to the firms in the observation, and making that case to boards to say, "Wait a minute, we don't want to get eaten by the marauding lions."

Gary McGraw: It really helps. Yeah, there is one thing I want to say. Getting an official BSIMM measurement where we do the measurement is different than measuring yourself. You're welcome to measure yourself. But what we've found is that people who do that tend to be a little bit over optimistic and delusional about their capabilities. And when we do a measurement ourselves as the scientists who built the measurement tool, we get a much more objective measurement out of the system.

The other advantage of getting measured by us is that you get to join the BSIMM community. And in fact, the BSIMM community was something that I didn't anticipate when we started this project eight years ago. But once we got to BSIMM2, and we had 30 firms, I asked the firms, "What do you guys want out of this besides a measurement?" And they all said, "We'd like a moderated mailing list. And we'd like to have a conference where we can meet each other."

And so, we've been holding BSIMM conferences for the BSIMM community ever since. We just had the sixth one last November in Denver, outside of Denver, Colorado. And it was a very powerful conference indeed where BSIMM community members are presenting aspects of their own software security initiative to their peers. And they're talking about the challenges, the pitfalls, the successes, and the real truth of software security in a very powerful fashion.

Lisa Young: Well, I like that approach. And I like the distinction between measuring yourself against a model and having the professionals do it because I would assume, too, that this community would help one another support the cultural change that's necessary to actually undertake some kind of initiative like this.

Gary McGraw: That's right. The BSIMM community, since they've in some sense done it in their own organization, has lots of advice about how to interact with the executive team, how to interact with armies of developers, sneaky tricks to get developers to really help with software security instead of thinking of it as a burden and so on. And they've done, collectively, 100s if not 1000s of experiments in the real world. And so, the BSIMM knows what works.

Lisa Young: Wow, that's great. That's very powerful. But can you talk about, as a scientist and developer, what's next for BSIMM, what do you see on the horizon?

Gary McGraw: Well, we're continuing to expand the BSIMM at all times. We actually have measured well over a 100 firms now in the entire data pool. We only, as I said before, report on data that's extremely fresh for each iteration of the model. So, each time we release the model, there are minor adjustments driven by the data themselves. That's really important.

As a scientist, I love having real data. If I can look at real data and describe those data and analyze those data, that's a lot better than just sitting in my closet making stuff up in opinion land. And I think that because you got into security in some sense in possibly a different way than others may have, that measurement is something that's really missing in security.

The BSIMM shows a way forward for measurement and science in a field that's grown very, very fast. It's an adolescent field that, frankly, needs more science in it. And so, we're proud that the BSIMM escaped the test tube and became this thing that it is now. When we started it as a science project, I really didn't anticipate that this was going to happen. But it's going to continue to grow and expand. And we welcome other firms to join us. If you're interested in the BSIMM, just drop me some email or get in touch with the BSIMM team through the BSIMM website. And we'll get you involved.

Lisa Young: I think that's great, Gary. And I really appreciate that. One of the things that I was struck by, too, is the growth of the BSIMM.

Gary McGraw: But what happens is the activities themselves are ranked. The easy ones are level one activities. The ones that require some level one capability to be built on top of are level two activities. They're mid-level, mid-tier activities. And then level three is rocket science activities that are pretty rare, but they indicate a very mature approach to a particular practice. And we've seen more movement between levels than we have seen deletion of activities in the BSIMM.

We have added a few activities. I gave you an example of bug bounties. We've actually added that into the model. And we track that directly because we saw it begin to emerge. And so, the BSIMM, as a description of the space, really does adjust to describe the real world out there. And we tune it using advanced statistics in order to describe the world as clearly as we can and as accurately as we can.

Lisa Young: Excellent. Well, thank you so much. I just want to say thank you for being here, for taking the time to educate me on the BSIMM and our listeners, as well.

Gary McGraw: I've been doing software security for about 20 years. I wrote the book *Building Secure Software* in 1999 and 2000, believe it or not. So, it's been a long time. And I'm optimistic that we're making real tangible scientific progress in the field. And I think that that's rare among people that have been doing security for a long time. We know what to do. And not only do we know what to do, we know how to do it. And not only do we know how to do it, we know how to measure it. And so now, it's time to do it and to measure it.

Lisa Young: Excellent. Well, thank you so much again for being here, for talking to our listeners and me. And I appreciate your time.

Gary McGraw: Thank you, it's been great.