

Software Security with Dr. Gary McGraw:

Listen to Podcasts: <http://www.imperva.com/resources/podcasts.asp>

Brian Contos: Welcome to the Imperva Security Podcast. I'm Brian Contos, Chief Security Strategist for Imperva.

Joining me today is Dr. Gary McGraw, CTO of Cigital, a software security and quality consulting firm with headquarters in Washington, DC. He is a globally recognized authority on software security and the author of eight bestselling books on this topic. His titles include "Java Security," "Building Security Software," "Exploiting Software," "Software Security," and "Exploiting Online Games," and he is the editor of "Addison-Wesley Software Security Series." Dr. McGraw has also written over 100 peer-reviewed scientific publications, authors a monthly security column for InformIT and is frequently quoted in the press.

Besides serving as a strategic counselor for top businesses and IT executives, Gary is on the advisory boards for Fortify Software and RavenWhite. His dual Ph.D. is in cognitive science and computer science from Indiana University where he serves on the dean's advisory council for the School of Informatics. Gary served on the IEEE computer society board of governors, produces the monthly "Silver Bullet Security Podcast" for "IEEE Security and Privacy Magazine" and produces the "Reality Check Security Podcast" for CSO Online.

Well, welcome to today's show, Gary.

Dr. Gary McGraw: Great to be here.

Brian Contos: So Gary, to kick things off, for somebody like you I know this is going to be a huge softball, but what are your perspectives on the current state of software security? I know this could probably be an entire book, but what are your high-level perspectives on where we stand when we're talking about software security?

Dr. Gary McGraw: Well, this may come as a big surprise. I've been doing security, as you know, for about 15 years or so, and yet I'm still optimistic about the progress that we've made and we continue to make in software security. So, back when I got interested in software security because of Java in 1996 - You know I wrote a book called "Java Security" with Ed Felten from Princeton, and it got me started thinking, why is it that these wizards screwed up Java from the security perspective? And where would you go to learn how to write something like Java from scratch in a secure manner?

The answer was nowhere. So, starting from nowhere to go to a whole shelf growing with all of the books that are available now on software security, to something like actual maturity models and science-based software security, we've made huge strides, and I'm really pleased about the progress that we're making.

Brian Contos: You said you're optimistic; we've been making progress. Are we better off today than we were 5, 10 years ago?

Dr. Gary McGraw: Well, that's a good question. One of the big challenges with software security is if you go and you ask developers, "Who is planning on having more software at the end of the quarter?" everybody raises their hands, without fail. Then, if you say, "All right, keep your hands up. Now, who's planning on having less bugs at the end of the quarter?" everybody raises their other hand [laughs], which means that they're all on crack, because there's no way to produce lots more code and fewer bugs. That's just not how it works, even if your defect density ratio is going down, which it is over time. You can look at Microsoft's code base, and their defect density ratio is dropping drastically, but the amount of code that they're building is going up even faster.

So, though we are making great progress in software security as a discipline, and we've learned the sorts of activities that we should put into the SDLC, and we understand the kind of knowledge we need to accumulate, and we understand the kinds of tools we need to use, we're building software so quickly on the planet right now that it seems like we're not making forward progress. That's our big challenge.

Brian Contos: Yeah, that's a good way of putting it in perspective. I guess one analogy or one way to think about that is that if you've got a very safe freeway and two very safe drivers, you probably are going to do pretty good, but if you have a million drivers, eventually something is going to happen, right?

Dr. Gary McGraw: Well, yeah. The law of large numbers kicks in, sure.

Brian Contos: When you and I were both at OWASP in Brasilia, I guess about a month or so ago, I was talking to some folks, and there's this gap that a lot of people have cited between the application developers and software programmers and then the security folks that have traditionally come up as system administrators, network engineers and from that into more of a generalized security role. There really hasn't been a lot of communication between these two groups. What are your perspectives on this? First of all, what do you think about it? Second of all, do you think it's important to get them to communicate more? And maybe, what's a way we can help address that?

Dr. Gary McGraw: So, I think that the distinction is a little bit artificial, but let me tell you how I look at it. There are developer guys and architects on one side, and on the other side are security people who do network security and network operation stuff on the other side. So, who's going to do software security? The answer is neither one of those groups. We shouldn't turn to either one of those groups to solve the problem. In fact, you need to create a new group if your organization is large enough, which is called the "Software Security Group" or SSG.

You know that we've been studying large-scale software security initiatives. I'm aware of 60 such initiatives going on in large corporations worldwide and some government institutions. By studying some of those 60 software security initiatives, one striking fact comes through: they all have a Software Security Group, which is responsible for carrying out the sorts of activities that you have to put into the SDLC we were alluding to before, and picking the tools, and then, generally speaking, teaching the developers how to do it right.

So, if you ask the standard network security person to teach the software guys how to build better software, that's a ridiculous thing to do because they don't even know what a compiler is sometimes. Not all of them, but generally speaking, that's just asking somebody that can't solve the problem to try, which is a recipe for failure.

Instead, you want to identify somebody to run the Software Security Group, and then staff it with people who have real software chops, but who've also come to understand security

over the years. I'll give you myself as an example. I'm a software guy, and I became a security guy in the mid-'90s because of Java. It made me wonder, why is it that software people have so little exposure to software security? One of the reasons was there were no books on it, and now, there are a whole bunch of books on it, and some are better than others.

We're taking away the excuses that developers have, "Gosh, I'd never had to learn anything about security." And developers, by and large, are understanding they do need to go and learn something about security. It's getting introduced into curricula, and the world is evolving in the right direction.

So, the way you posed the question is a little problematic: should it be the developers or should it be the security guys? The answer is neither one. It should be the Software Security Group, and we've seen that phenomenon all over the place in many initiatives.

Brian Contos: Yeah, that was going to be my next question. So intuitively, it makes a lot of sense to have a specialized group in this area, just like networking broke off and you had network ops, and then you had security people that were usually taking control of network security. Are you just seeing this in large government agencies and/or large enterprises? What can an SMB do or maybe just a small organization?

Dr. Gary McGraw: Yeah, that's a great question. There's some further data that I should mention, which is if you add up all your developers, even the people that you've outsourced development to, and you get a number, then the Software Security Group's size appears to be, in practice, one percent the size of developers. So that is, for every 100 developers you have, you should have one software security person. So, that number holds over our entire BSIMM study of 30 large organizations. Incidentally, there are zero government organizations in that study so far, but we're getting ready to change that. The Air Force is going to hop on board.

These companies are not all huge dev shops. One of them, Microsoft, has 30,000 developers, so they're a large development shop. [laughs] On the other hand, one of the smaller participants, DTCC, has about 400 developers, and so the size of their Software Security Group is much smaller than Microsoft's, if you apply the one percent rule.

So, "How small is an SMB?" is my question. And if it's smaller than 100, if it's say 50 guys writing code, then do you take the top half or the bottom half of a software security guy? [laughs]

The answer there may be to outsource some of that functionality, or to have it be somebody's part-time job. But, I will tell you this: management 101 states that if you want to get something done, you have to make it somebody's job, and you have to give them both the authority and the responsibility to get that job done.

It should come as no surprise if you have the developers pointing over to security, and the security guys pointing over to developers, and nobody standing between the arrows. Everybody's pointing at everybody else expecting them to get the job done, and of course nobody's getting the job done. I'm afraid that's what's happening in a lot of SMBs, or small and medium sized businesses. Hopefully, we can begin to address that.

One of the things that I'm doing in my work, although I haven't gotten the data yet completed, is a study of smaller organizations that are just getting started with software security, to see what we can say about what people are in fact doing today.

Brian Contos: Actually, as you were describing that situation, I was starting to think to myself, the cyber czar for the U.S. government, this position that I don't think anyone's held for more than a year, and all the responsibility, but [laughs] not really the ability to execute, or the strength to execute, across the various departments.

Dr. Gary McGraw: I call it the cyber cheerleader. It's totally silly and useless political nonsense.

Brian Contos: Yeah, well, it definitely has had a revolving door.

Dr. Gary McGraw: Let me mention one thing real quick, if you don't mind. You know we have this BSIMM, which we may talk about later. But, the study I'm talking about that focuses on SMBs, your listeners can help with. It's called BSIMM Begin, and it's a web-based survey that takes about 90 minutes to complete. We're hoping to get 100 companies to complete the survey, so that we have enough data to draw some reasonable inferences about the SMB marketplace. Right now, we have 75, so if I get another 25 companies to fill out that survey, and the data turns out to be good, we should be able to say with some confidence, here's what the SMB market is doing for software security.

So, just begin with Google, and you'll find it.

Brian Contos: We'll throw a link on the podcast notes for folks.

Dr. Gary McGraw: Oh, that would be awesome.

Brian Contos: One of the things that came to mind, when you mentioned the SMBs, I was with Jeremiah Grossman, who I know you know, the CTO of WhiteHat Security. We were at Interop New York, and this was a few weeks ago. We had this co-presentation that we were doing on virtual patching, web application firewalls, and VA assessment coming together, converging if you will. One of the things that Jeremiah brought up that was really interesting, and I'd like to get your perspective, is let's say I'm a 10, 12 person organization, and I'm writing some new great application, the next Facebook, next Twitter, something like that. And my folks are really focused on creating these features, the UI, things like that.

At that level, do you think they should be considering security from a business perspective? Do you think that it's more of a push to let's get it out, and we'll fix it later? How early or how small of an organization should really start considering building security in?

Dr. Gary McGraw: [laughs] Boy, that's a good question. I really don't know the answer. I could put on my software security advocacy hat and say, "Every organization should consider building security in from the beginning."

Brian Contos: Is your Hello World secure? [laughter]

Dr. Gary McGraw: Well, you know, Hello World in J2EE is about 50 million globs, whereas in Perl it's one line. The interesting thing is, I think that it really depends on two factors. One is the agility and speed, and startup entrepreneurial aspects of the effort underway, how quickly you have to go. Because in Silicon Valley, often the answer to building software is build some crap first, get some market share, and then fix it later. That doesn't even take into account security; that just takes into account barely working. [laughs] On the other hand, if you're building something that you are in fact expecting millions of people to use, then really it behooves you to think about security.

Let me say one more thing. I think that the world has changed perspectives on security. I think that people expect software to be secure, and when it's not, they get upset about that.

Brian Contos: Yeah, I kind of see two sides of that. A perspective that I've brought up before in the past is when I was younger I had a VCR. I never did a patch update; I never did any type of configuration on it. I plugged it in, stuck tape on, and when it started eating my tapes, I threw it away and got a new one. But, now I have a PS3 as my Blu-ray player, and I have a lot of great...

Dr. Gary McGraw: [laughs] I have a Blu-ray player. I've burned the BIOS four times already.

Brian Contos: Yeah, yeah. I don't even know if my VCR had a BIOS. I doubt it.

Dr. Gary McGraw: [laughs]

Brian Contos: I know my VCR got really hot. [laughter]

Brian Contos: And I think, perhaps, this generation, or maybe this generation coming up, they're saying, "You know what, this phone's got a lot of great features. Sure, every once in awhile when I try to answer a call it reboots. Or sure, every time I want to watch a Blu-ray I have to download a new firmware for it." But, are we just getting used to it? Or maybe it's just part of life, part of technology?

Dr. Gary McGraw: I think it's part of life. It's part of this notion of what people call convergence. But, when it comes to Blu-ray, I just blame Paul Katcher.

Brian Contos: [laughs]

Dr. Gary McGraw: I don't know if you want to call him, but I'll make sure Paul listens to this episode, so he gets called out. Damn it, Paul! We're tired of burning BIOS for our Blu-ray thingies!

Brian Contos: That's right; that's right. So, I don't know if you know Joe White over at SuccessFactors. He's their chief security guru in residence out there.

Dr. Gary McGraw: I don't. I'm sorry.

Brian Contos: He's an interesting guy. He came up via, definitely the security side, pen testing, etc. Then, sort of the opposite of you, started getting into the software side. So, he helps bridge that gap over there at SuccessFactors. SuccessFactors, for those who are listening that aren't aware, you're probably aware of Salesforce.com. To really dumb it down, they are an HR version for Salesforce.com, instead of a sales version. So, it's a SAS model.

But, one thing that he mentioned is, he goes, "The security folks, they don't know anything about code," just like you mentioned, and really vice versa. There are a couple folks that are somewhat aware on the software development side, but they're definitely not security folks.

He found that one of the areas that they could bridge that gap - they're a customer of ours, and they use our web application firewall - is they actually use WAF in the development phase. They use it during betas, and when they're testing. It's used primarily at that phase

for visibility into how people are actually interacting with the application. What specific URLs are being attacked, or what types of vulnerabilities are being targeted, if it's a live beta, and that type of thing?

So, all that to say this... I know your perspectives on WAF from many angles, but what's your perspective on leveraging WAF as part of the SDLC, and improving development overall.

Dr. Gary McGraw: Well, the SDLC is a long thing. You're talking about the tail end of the SDLC, because you've already got code that runs, right? Or, you're talking about some sort of a spiral model. That's fine. There are a lot of people that develop software like that. Agile methodologies tend to produce a lot of stuff that runs, and then adjust it, and change things, and re-factor over time. So, that use case that you are mentioning is possible. I have seen some evidence of use of WAFs for the very reason that you brought up, that is, standing them up in front of your thing, and finding out how it's really getting attacked, so that you can then plan to build defenses into it.

I think that's a fine use of that kind of technology. I have no problem with the notion of monitoring as an important part of computer security and network security, and think that monitoring what an application is getting on the input stream is an important thing to do.

Some of my concerns in the space are that when we limit ourselves to only web applications say, and then we further limit ourselves to only web applications that only talk over port 80, a stateless protocol, we begin to think of the problem as a little easier than it actually is.

So, if you get into testing of code, which I think is important, one of the benefits of a WAF is you could do some testing of some actual attacks, attacks that looked right, because you'd seen those in the wild, and then you could simulate them in your test environment. So, that's good. But, on the other hand, the kind of testing that you can accomplish from an outside-in perspective, by sending only network traffic to your application, will exercise usually about 10 to 20 percent of your code. The rest of your code won't even ever get run, and that's a big a problem.

So, I think that there are some fundamentals in software engineering that it really behooves everyone to pay attention to, even in the web space. And unfortunately, there's been kind of a myopic focus in what people call web application security that is drawing attention away, in my opinion, from the larger picture of software security writ large.

When I talk about software security, I'm including code written for phones, operating systems themselves, power grid code, all sorts of stuff. Not just the web facing apps. And I think that that's an important thing to understand.

I did want to mention one other thing too, when it comes to the, who does it thing. This just occurred to me. We've studied lots of companies in the BSIM Model, about 30. And if you add up the number of people that work for the software security groups that we've studied directly, it's thousands of people.

So, it's not like there are zero software security people on earth and nobody's available to do this job. It turns out that we've produced lots of people that are capable of doing that over the last 10 years. Now, do we need more? Yes, we do. But, it is possible to create these people. It's not like you can't find them anywhere.

Brian Contos: Sure. And that's actually very refreshing to hear that those numbers are larger than you might think and growing.

Dr. Gary McGraw: Well, we did a funny thing recently. The OWASP guys had a board election and I think they had 240-some people vote for the board. And I just added up the number of people in the BSIMM that were in software security groups. And I wondered what 240, what percentage that was of the total of people in software security groups. And the answer was 16 percent. So, there are a lot of people doing software security out there and we need to understand that.

Brian Contos: Absolutely. Well, one of the interesting things you said is, software security is this very large term and people try to break off little slivers of it, web application what have you. Even our space as Imperva, of course we have web application firewalls, but we also have database firewalls, and database activity monitoring which is essentially audit. Just to get people to think of data security as, "Look, it's not just the web app. It's not just the database. It's also unstructured data." That's difficult, let alone talking about SCADA and flip phones and everything else out there. So, it's a difficult battle. It's a lot of awareness. And I deal with that quite honestly in just our space.

Dr. Gary McGraw: Absolutely, and I think the work that you're doing at Imperva is important because we're finally getting around to protecting the actual stuff we're interested in protecting: the data. It just so happens the question is, "Where do you protect the data?" Maybe at the database level, maybe at the application that is originating the data, or manipulating the data. But, it's probably not at the regular network firewall level.

Brian Contos: Yeah, that's sort of like stopping rain with a tennis racket.

Dr. Gary McGraw: That's a great analogy; I like it.

Brian Contos: Well, I tell people if you think about it this way, "Where does the data sit? Most of it is structured data that sits in the database. How do you get to it? Through a web application. So, where do you put your security controls? On a network IPS or a network firewall? Of course not. You put purpose built controls for the apps and the databases. We're, at least what I've seen in the field, 10, 12 years behind in terms of people's understanding especially at non-technical executive levels, of the data security risk. They're just not aware of it.

For years they've been making network based security investments and they get that. Bad guys over here - they don't think about insiders - good guys over here and sensitive stuff, and a network firewall here. But, I think data security is a little bit more abstract, at least the way we talk about it, or Imperva talks about it. So, yeah, it's hard to make that leap sometimes.

Dr. Gary McGraw: I think that's right. Greg Hoglund and I wrote this book called, "Exploiting Software," in 2004 for just that reason. We wanted people to understand how attacks really work in the real world. Not the hacking, exposed, pretend level attack.

Brian Contos: Sure, sure.

Dr. Gary McGraw: And I think the world's coming around to that perspective. But, you're right, we've still got our work cut out for us in getting people educated.

Brian Contos: Yeah, I actually gave some hacking examples yesterday at an online Black Hat and Dark Reading event. And one of the things I was trying to illustrate was, "You know what? In real life, a lot of these attacks, they're a lot more Columbo than they are James Bond." And people's approaches to things, a lot of times we have these uber-hacker ideas

on how things are done and a lot of it's just general flaws that are quite basic and quite old in many cases.

One of the things I wanted to ask you about was code freezes. I recently did a webcast on the whole notion of, we're coming up on the holiday season, different organizations have different code freezes for many reasons but it's easy to think of a retailer, say Wal-Mart.com. They're probably not going to shut down their applications when they find a vulnerability.

A lot of organizations say, "Well, it's commercial software, the patch doesn't exist. Or the vendor hasn't created a patch yet and we haven't tested it. It's proprietary, we've got to take developers off other tasks or we hire the person that wrote it. Sometimes it is difficult to make a business case to justify to their non-technical management why we need to make this change.

What are your views on that? It's two days before Christmas, you've got a web application that's generating a bucket load of revenue, you find some major flaws that could have devastating consequences. What do you do as an organization?

Dr. Gary McGraw: Well, the answer is, what is devastating? So, what's more devastating? A devastating consequence of the pretend security thing that could happen variety, or offline for two days, which devastates Q4, as a bottom line. And the answer is, you have to make the right business decision. And sometimes the right business decision if you're say, Amazon, is must be up. Have to be able to cope with attacks in real time including distributed denial service attacks. And so we've seen security come to that realization over the years.

My belief is that if you have code that's in a high security situation like that, that it deserves some real attention during the software development life cycle. And then if you do pay a fair amount of attention during the SDLC, that you're not going to have the horrible thing happen in the field as often as you would otherwise. And I think we've seen that over time.

And the other hand, if you are experiencing an attack in real time and you need to do something about it but you need to stay up, then it seems obvious to me that technology like an application firewall may make sense in that situation. It sort of buys you time to go back and do things right.

Now, what worries me is that people start with the notion of, "OK, let's buy some time. We'll put a web application firewall in place. And oh, look. Everything's fine. So, now we don't have a problem anymore." And they don't fix the application. That is a problem.

And I hope that the use case that we're talking about doesn't result in sweeping problems under the rug, but my knowledge of human natures says that it will. So, that's my only real major concern there.

Brian Contos: Yeah, I tell people it's not. It's like if you're walking through the woods and you cut your leg open on a rock, you're going to wrap it up with a t-shirt or something. But, a t-shirt wrapped around your leg probably as a final solution, isn't the best way to handle things. On the WAF side, what's funny is that... So, I see people using VA and integrated with WAF and using a virtual patching, that's definitely a common use case. It's really common, actually, in power and energy. I know you're familiar with critical infrastructure. And a lot of these folks are running NT4.0 systems, un-patched, no anti-virus, no local firewalls.

And they're not doing it because they're dumb. They're doing it because they can't touch these boxes; they're ruggedized solutions. If they change them it breaks the warranty. They won't get support from their vendors.

And some of these systems are built in a vacuum with totally different TCP/IP stacks so if you ping them, they don't understand what the ICMP echo request three is. They actually fall over and die. Forget a buffer overflow; ping. Right? So, what do you do, right?

So, a lot of these guys say, "Well, let's do this." But, they don't actually use it for blocking. What they do is they have the virtual patches installed on the WAF and then they alert so at least they know something's going on. And then they can use human analysis. You make a good determination, like you said. What's the real life risk at that particular point?

Dr. Gary McGraw: Well, my view is that watching is a good idea. And being alert when it comes to computer security and doing monitoring is an essential part of any security situation. Thinking that you built something perfectly and that you can thereby just close your eyes and pretend you're never going to have a problem is just plain old dumb.

Brian Contos: Yeah, prevention simply doesn't scale. I tell people, if prevention was the end-all, be-all, banks would just have a big safe. No need for video cameras, security guards, a red button that calls the SWAT team, auditors, just a big safe, right?

Dr. Gary McGraw: The problem is you would always be closed and you could never put more stuff in there.

Brian Contos: That's right, that's right. Withdrawal, what are you talking about? We just take deposits. [laughter]

Dr. Gary McGraw: Man, it sounds like a good idea. Let's open a bank like that.

Brian Contos: That's a good business model. So, looking into your crystal ball a little bit, when we talk about this big thing of SDLC and we talk about VA and abuse case testing and WAF and database security, whatever, there's tons of stuff out there, white-box and black-box testing, et cetera. Where is it all headed? It seems to me that we're all sort of addressing the problems in our own way and getting there in our own direction, at our own speed, but is this going to converge? What are we going to see down the pipe? What does the future hold for us?

Dr. Gary McGraw: That's a good question. I think that the discipline of software security and the notion of putting best practices into the SDLC is, in fact, moving from good philosophy into good practice, and it has been doing so, since around 2006. So I've been involved, personally, in seven or eight large-scale software security initiatives at organizations that have tens of thousands of developers. I've helped these huge organizations. That's what we do at Cigital, we help these guys figure out how to do software security, when they have 30 thousand guys that are their developers, whether they're a major bank or they're an ISP or something like that.

The good news is that there are some things that everybody does now. So, it's not like everyone's doing their own thing. I think that the notion that you can willy nilly do whatever in software security, and well that's better than nothing, is thinking that reflects 2005 or so. Sure there are lots of people who are still approaching it that way, but I think that the people that are leading the software security field are, by and large, doing things in a similar fashion.

And those things have common tools and common activities. If you looked at the way those software security initiatives evolved from say, didn't exist, to 14 years later, in the case of say, Swift in Europe. They started from nothing but it's been 14 years, and so now they've got a lot of stuff that they've accomplished.

But, their own story, the way they did it, is not something that's going to work, necessarily, for any other corporate culture. So the real tricky factor here is kind of a factor that - the reason that McKenzie exists as a consulting firm - is that different corporate cultures have different ways of accomplishing the same idea or the same set of activities.

So, as a result of that, when we came to try to describe what's going on in the software security with BSIM Model. We went out and gathered data and we just built a model based on the data, instead of saying, "Gosh, you should do it this way. Now let's go out and justify our position on why you should do it this way."

And I think that's a sea change in software security. It's putting the horse before the cart, instead of putting the cart before the horse, like we've been doing for the last decade. That's a good and important change.

It turns out that even though the stories of evolution, of software security in these organizations, are all diverse and they are all specific to particular cultures of organizations. If you stand back and squint and look at these organizations all together, they have lots of activities in common. They have lots of tool sets in common, including WAF and database security and code review tools and penetration testing services and training their guys.

That's what we describe in the BSIMM. I think that what you're seeing is a discipline that's growing up from "shooting from the hip" and just getting anything done, to something where we literally have thousands of people working in concert, in large organizations, to solve a very difficult problem.

So, what are they all going to look like in the future, if I got out my crystal ball? I can't tell you. But, what I can tell you is what they all look like now. There's plenty of room for people to get up to that speed. So, we have a lot of work to do. We're not done with our work in software security, but we no longer need to say, "Gosh, we're not sure what to do." When I wrote "Building Secure Software" in 2001 [laughs], it was philosophy.

Brian Contos: Sure.

Dr. Gary McGraw: And if you compare that to "Software Security" from 2006, or "The BSIM Model" from 2009, 2010, you see that we've moved from philosophy to what you should do to what is being done. That's a really important distinction.

Brian Contos: Yeah, that's interesting that you mention that for that book. A lot of our customers that we work with, and talk to, they essentially say, "Yeah, we feel like we're 10, 12 years behind, when it comes to data security."

Dr. Gary McGraw: Yeah.

Brian Contos: I've actually looked it up. 1997 is about that time-frame. The "Titanic" was the #1 movie and Helen Hunt won an award for the TV show "Mad About You." If you kind of put yourself in that place, you're like, "Wow, we're really that far behind." [laughs]

Dr. Gary McGraw: You know, I was working on a book called "Securing Java." [laughter]

Dr. Gary McGraw: That was a long, long time ago. But even in the last decade, if you just started, I think 10 years ago was more like 2000, 2001, than 1997. There was a huge difference in those three years, because that was the advent of the web.

Brian Contos: Sure.

Dr. Gary McGraw: When I got out of Computer Science School with a PhD, in 1995, that was when Netscape was founded, they did their IPO. At that time, we were all using the Mosaic browser from NCSA and things just, the world has changed, just a tad since then [laughs].

Brian Contos: That's right, that's right. So, Gary, last thing, where can people learn more about BSIMM and where can they go to check out that survey?

Dr. Gary McGraw: So, the BSIM Model is all published for free, under a Creative Commons license, so it's an open-source model, so to speak. You can get the BSIMM document at the website BSI-MM.com. If you're interested in helping us with the survey of SMB, Small and Medium-sized Businesses, or people just getting started with software security, there's a tab on that website called "begin." You just click on BSI-MM.com/begin and that will aim you right to the survey. We would hugely appreciate help. Anybody who helps us with these studies gets a lot of data back, as thanks. Because we'll build a model and then we'll show everybody where they stand according to the model. That's been an incredible power behind the BSIMM.

One of the things that I think was an unanticipated side effect of the work, in the big BSIM Model, is that the people that have been doing software security in these large organizations, they knew that there were other people doing this, but they didn't know the other people. So, for example, Steve Lintner had never met Brad Arkin. And Steve runs software security for Microsoft and Brad runs software security for Adobe.

And now, because of the BSIMM, they know each other and Brad can call up Steve and say, "Hey, Steve, dude, I'm in the hot seat [laughs]. I seem to recall that you were in the hot seat before. What do you do? What's the best way to focus on the real stuff and avoid the media hoopla and get some hard work done." And Steve has a lot of good answers about that.

So, I think that the BSIMM has resulted in a community of like-minded practitioners, who are grownups, who are working on this problem, and spending millions of dollars on getting this problem solved for their corporations. And that's great, because I think it's helping to move the field in the right direction.

Brian Contos: Yeah, that's good stuff. And I can just tell you from experience, there's nothing more powerful to an organization than comparison to other peers. Are we better?

Dr. Gary McGraw: Yeah.

Brian Contos: Are we the same? Are we worse? Especially, especially, in the finance world Those guys won't make a step unless they think they validated that piece. It's a really interesting group think.

Dr. Gary McGraw: We started the BSIMM with a study of nine companies that included Microsoft and Google and EMC and Wells Fargo and DTCC and Qualcomm, I don't know who I'm forgetting, and a few other companies. But, by now, we have tripled the size of the study and in January, we will have 30 companies, 31 in fact, that are participating in

Software Security with Dr. Gary McGraw

BSIMM. That's a superb, very quick, acceleration. The model is becoming the de facto standard for measuring a software security initiative.

Brian Contos: Thanks so much for joining us in today's podcast.

Dr. Gary McGraw: I'm super pleased to chat with you. Thanks for your time and attention.

Brian Contos: If you would like to learn more about this subject and Imperva, please visit <http://www.imperva.com> or send us an e-mail at blog@imperva.com.



Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004