

Interview

Silver Bullet Speaks with John Stewart

GARY MCGRAW
Cigital

As Cisco's chief security officer (CSO), John Stewart provides direction to multiple corporate security teams throughout the company, aligning business units and IT organizations to generate leading corporate security practices, policies, and processes. He also oversees security for the e-commerce infrastructure supporting Cisco's more than US\$25 billion business.

Featured here is an excerpt adapted from the full interview between Stewart and Silver Bullet host Gary McGraw. Their conversation ranged widely, from Stewart's role as CSO to Ciscogate to raising Internet-savvy kids. You can listen to the podcast in its entirety at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet, or you can subscribe to the series on iTunes.

Gary McGraw: What exactly does a CSO do?

John Stewart: Well, some days it feels like a CSO is just a manager; the day-to-day activities can include handling employees, budgets, personnel situations, or growing a management team. At a very basic level, I think one of the roles that most CSOs play is as a builder of talent so that fundamentally, they don't have to be in the critical path. At the same time, there are unique positions de-

pending on which industry you're in. In my particular position, a second set of responsibilities includes being a straightforward and honest advocate of security and for how Cisco is doing it. I develop and describe what our overall thinking process is in the industry at the moment—how it's moving, changing, altering. That's largely unique based on each company's role in the industry, so it's partially unique to me, given Cisco's role.

On a more technological level, or as a business and technology blend, it's bringing security up as a huge cheerleader. It is certainly a topic I've been very passionate about and have enjoyed being a part of for many more years than I care to admit, and it becomes one of those things where you're just trying to make it a mainstream topic inside of the company, so you become the internal advocate for the topic.

McGraw: You started out as a technologist and quite a good one, but you've morphed over the years into a balancing act of business and technology. What kind of advice would you give to someone who wants to do that for a career?

Stewart: I think that the best experience I had—and it can be applied differently, but I'll explain what really helped me bridge it—was helping to build a company from scratch, all the way up to selling it.

McGraw: That was Digital Island?

Stewart: Exactly. That experience really filled in a lot of gaps for me when it came to the business side. It certainly taught me a lot about finance, corporate positioning, marketing, customers and how you need to constantly focus on their needs, how to talk to an executive team and board, and, as the company went public, how to talk to private or public investors, our analyst community, and the press. All those experiences helped me understand that what I largely understood security to be (which was a technology discussion in so many ways) had to change and morph to various audiences. But more important, it got me very seasoned—painfully, at times, and with a lot of bumps and bruises for me personally—from having to learn so much on the business side and what it took to make it.

McGraw: As the CSO, are you responsible for software security at Cisco?

Stewart: Yes and no. I imagine that you're particularly asking about security in our products?

McGraw: Maybe. You have tons of developers who build stuff every day and my pet bug-a-boo is trying to get all developers to have a clue about security. But in most organi-

About John Stewart



John Stewart is Cisco's chief security officer. Previously, he was the CSO responsible for operational and strategic direction for corporate and customer security at Digital Island. He also served as a research scientist responsible for investigating emerging technologies in the office of the chief technology officer at Cable & Wireless America.

Currently, Stewart sits on technical advisory boards for Grand Central Communications, Ingrian Networks, and Tripwire. He's the author of *Securing Cisco Routers: Step-by-Step* (SANS Inst., 2002), and coauthor of the W3C's Internet WWW Security FAQ (www.w3.org/Security/Faq/). Stewart has an MS in computer and information science from Syracuse University, New York.

zations, security isn't pushing the agenda on the software security front. Is it at Cisco?

Stewart: Yes, in the IT development arm—and I want to largely separate that from the engineering development arm of Cisco. When I say I'm responsible, I say it incorrectly. I am guiding them to be responsible for it themselves. For example, we're integrating quality-assurance checks and the development life cycle with the security parameters that are so necessary to keep the results relatively pristine.

McGraw: Do you think that kind of focus or attention will hop the fence over to products?

Stewart: I think it already has happened there faster than it happened in IT. I look at things both in industry as well as inside of our own company. Certainly one example is how Microsoft brought the security development life cycle in as an attempt to change the way they develop to address some of the situations that we see in our paths, respectively, in the industry.

McGraw: Yes, in fact, that's a plug for a previous Silver Bullet with Mike Howard [episode 6], who's helping to roll software security out at Microsoft.

Stewart: I couldn't be more proud

of them for taking it on because it is a monolithic task, and it's just very difficult to do. To change that culture quickly, in my mind, is pretty impressive. Here at Cisco, we are trailing them in the timeline, but we're going through the same level of awakening and then integration into development.

McGraw: Many companies are doing that right now, especially in the financial vertical.

Stewart: Right, and that's not surprising. I think every company is, again, trying to build strong defense through development—just as you've been preaching, being one of the strongest advocates for it for many years. It's only just now that the topic is finally connecting to the timeline work being interpreted.

McGraw: This would not be a responsible interview if I didn't ask you about Ciscogate and Michael Lynn at Black Hat [2005], where you guys took a lot of heat. To summarize, a Black Hat presentation regarding Cisco security vulnerabilities was pulled at the last minute from the proceedings and legal action was taken against the presenter and his company. I know that you were out of the country at the time.

Stewart: Yes. Recommendation: don't take a vacation during Black Hat!

McGraw: You did a really great job of countering the bad publicity and had some very good things to say. Did you go to Black Hat this year?

Stewart: I did. In fact, I actually ensured that we were a platinum sponsor of the conference, and then I was there for three days. We joke about it, saying we bought a beer for everybody on us, and we threw a bit of a bash over at the Red Room [inside Caesar's Palace]. It was kind of ironic: Caesar's was celebrating an anniversary, so you had the very traditional, and somewhat stereotypical, security people all dressed in black and a toga party going on at exactly the same time.

McGraw: Did you see any talks or participate in any conversations that were noteworthy while you were at Black Hat?

Stewart: Yes, in fact, with Dave Mortman's help and Nico Sell's and a couple of others, we actually brought 10 people onto a panel discussion about the previous summer's topic, which was responsible disclosure. Steve Lipner from Microsoft and I were two members, then there were customers and independent researchers like David Litchfield, and Raven Alder for the network security part of the world. Then we had an audience of heavy interaction, and questions and answers moderated by David.

McGraw: That sounds fun.

Stewart: It was. I think we made some mistakes in handling things in 2005 that we've learned from—which was, it just came across wrong. And it's not the spirit of the company that was seen in the actions that resulted and were interpreted. So I wanted to get out there—and we were somewhat faceless in 2005 behind PR spokespeople, who sometimes weren't even named, and that's just by prac-

tice how we handle those—but I wanted to get out there and go, “Bring it on. If we screwed up, and you want to yell at somebody at Cisco because you’re frustrated, I’m here. And I’ll take the beating I need to because I don’t want the spirit of Cisco to be interpreted that way because it’s not who we are.”

McGraw: I think it worked. You did a very good job with that.

Stewart: I fully and genuinely enjoyed listening to people explain to me what they saw and then ask questions. I bought Michael Lynn and FX, another person who has done a lot of research on Cisco kit, a beer. In fact, I think there’s a photograph of all of us hugging. But it really was a good time. It was trying to put to rest, or at least heal, some of the wounds that were created, and I think we owned our own piece of that.

McGraw: There’s been another time when you were sort of on the other side of the mirror, so to speak. You were the victim of identity theft while buying your wife a motorcycle.

Stewart: Actually, trying to buy it after I’d been a victim of identity theft. The California state DMV lost my renewal driver license when they sent it to me. And all of a sudden—

McGraw: Somebody else had it.

Stewart: Yes. I had [apparently] repaired a car in San Leandro, California. I was six foot five, weighed about 210, and was black. I had very short hair and, in some respects, the guy possibly looked better on his license photo than I did, but we won’t get into that. It started a chain of events that took the better part of about 18 months for me to unglue.

McGraw: It’s interesting to be on the other side of that, to find out what it’s really like.

Stewart: It was not fun. Now, I’m the largest advocate for simple things like pulling your credit report twice a year. It’s a derivative thing that ensures that anything weird will trigger an alert. And I also did something very dumb: I saw in my mailbox something from the company that did the car repairs, and guessing it was a credit card solicitation—

McGraw: You just threw it out.

Stewart: I shredded it and didn’t even look at it. It was a bill. I just didn’t put it together.

McGraw: That would have tipped you off, right there.

Stewart: It would have tipped me off faster. It’s that classic example of deleting spam that was really an electronic note to you that you needed to read. I did it in a physical way.

McGraw: If you delete that email and it’s important, they’ll just send you another copy.

Stewart: That’s true. Well, now I’ve learned they’ll send new bills, too.

McGraw: You have two kids who are old enough to be on the Net now. What are you teaching them? Are you trying to instill in them some kind of security clue?

Stewart: Neither one of them have email. They have the ability to get on the Net, but you’ll just love this: it’s through a proxy server, meaning where they go is controlled by me.

McGraw: As it should be. Dad watches all. That’s the way it is in my house, too.

Stewart: That’s my attitude. I said, “I won’t look and watch unless I feel worried.” They are not going to get ubiquitous access. My son is now 13, and he’s getting to the age

where he’s beginning to realize that not everybody’s nice, that not everyone is out there to do the right thing. So his responsibility level is higher, and I can start releasing some of the restrictions I put on him so he can mature into using it with an educated sense.

McGraw: Well, I’m going to keep a close eye on what you do, because my guy’s 11, and he’s on the Net now, too, but he’s pretty restricted as well.

Stewart: I think it’s the responsibility of the parents, and my son would be the first to tell you that the reason he doesn’t have ubiquitous access is because his dad’s a security guy.

McGraw: He probably says that with much derision in his voice.

Stewart: Oh, he does—having overheard it at least once.

McGraw: You try not to laugh.

Stewart: Exactly. But as much as I want to be his friend, I’m his dad first.

You can find additional podcasts, such as a podcast featuring the Fortify Software Technical Advisory Board discussing the importance of security principles and vulnerability pimps, at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/. □

Gary McGraw is chief technology officer of Cigital. His real-world experience is grounded in years of consulting with major corporations and software producers. McGraw is the author of *Software Security: Building Security In* (Addison-Wesley 2006), *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), *Java Security* (John Wiley & Sons, 1996), and four other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. He is a member of the IEEE Computer Society Board of Governors. Contact him at gem@cigital.com.



\$29

New Lower Subscription Price!

IEEE
SECURITY & PRIVACY

Subscribe to our
magazine today
for only \$29—
our lowest price ever!

You'll receive 6 issues of today's
leading-edge, peer-reviewed
software development information.

Ask us how
you can get this great deal on
IEEE Security & Privacy magazine!

S&P is the premier magazine
for security professionals.
Every issue is packed with
tutorials, best practices, and
expert commentary on:

- attack trends
- cybercrime
- security policies
- mobile and wireless issues
- digital rights management
- and much more.

Subscribe at www.computer.org/services/nonmem/spbnr