Editor: Gary McGraw, gem@synopsys.com

Silver Bullet Talks with Bruce Potter

Gary McGraw | Synopsys

Hear the full podcast and find show links, notes, and an online discussion at www.synopsys.com/silverbullet.

Bruce Potter is chief information security officer (CISO) at Expel where he's responsible for cyber risk and securing the operation of Expel's services. Previously, Potter cofounded Ponte Technologies, which was sold to KeyW Corporation. He served as chief technology officer at KeyW for two years. Well before that, Potter was a security consultant at Cigital at least twice. In another life, he founded the Shmoo Group and to this day helps run the yearly hacker conference ShmooCon. He regularly speaks at DEF CON, Black Hat, and O'Reilly Security.

I'm interested in what Expel actually does and why you guys decided to found security startup now.

Expel is a very interesting place to be right now. Rewind to 2016: I was the senior tech advisor for the presidential commission on cybersecurity. I spent a year running around the country, working with the commissioners, helping them understand what was going on in the industry, interviewing public and private sector people, and talking about what's working and not working with respect to cyber risk management and IoT and controls systems. And what struck me about what I was hearing during the interviews and commission meetings is there was a very bright edge between companies that understood risk management and had cyber risk management as part of what they did. It doesn't mean they were doing it well, but they were mature enough that they could think about risk in large brush strokes, think about cyber risk, talk about the controls they're trying to place. A lot of it was still stumbling around in the dark, but for the most part, they were somewhat sophisticated about it.

And then very quickly you got to companies that were basically like "hey, can you give me a purchase order that just says quantity one, item security, cost $20,000, and I'll sign it?" They went out and bought the antivirus, they bought firewalls, and they just didn't know what to do next. They were really struggling on what to with all the security technology they had. And I realized at the time small and mid-sized businesses really need help, maybe law enforcement backstop, better technology, better operations. And I couldn't really wrap my head around what that looked like. So at the time, I was at KeyW and I was actually going take a break. It was earlier last year in February I resigned and I was going to take some time to spend with the family.

I actually got a call from Yanek [Korff] and he said, "Hey, we started this company. We're looking for a CISO, part time through the summer and maybe even the fall. But it's really hard as a startup to find somebody who knows what they're doing and is willing to take a risk with a startup and be part time. Do you know anyone?" And Expel told me what they were doing and I was like oh, this is the thing that I think can make a huge difference for organizations that are looking for the next thing they need to do to walk down this path. And I'm like "hey, I'm interested." That was the job interview, and we went from there.

What we're doing is really transparent security operations, so the idea is that you take your existing security technology, the firewalls you already have, antivirus, endpoint, whatever you have, you send us the alerts, and then our people dig through the alerts, try to identify bad things happening, and then work with you to remediate it. But the kicker is, unlike an MSSP [managed security services provider] where they kind of hand over a bunch of data out of a black box and say "here's some stuff you should

Copublished by the IEEE Computer and Reliability Societies
1540-7993/18/$33.00 © 2018 IEEE

look at," we hand you actual ongoing incidents to say "this is the thing you need to worry about. It's not something you *might* have to worry about; this is actually a thing."

But secondarily, the interface we use, the portal, all of our tech is totally open to our customers, so our customers can work right alongside us. They can work with our analysts, dig through the same data, task their own infrastructure to go prosecute systems to get process lists and files and all that—the same way that all our analysts work. So it's very open and transparent as opposed to black box-y, which this part of the industry has been plagued with over the years.

What's the most important recent development in network security? I know you have deep network chops, and I'm interested in what's going on in that world.

The push toward a cloud-first organization is changing a lot of what we've conventionally thought about network security. But there was this idea of deperimeterization, and everything would just be connected and every endpoint would be on its own thing. But what's striking to me is we haven't realized that goal, and I don't think we're going to. People still have a warm fuzzy about having a perimeter. Even if it's squishier and got some parts that stick out further than they would like, they still are wrapping their arms around it. But we still have all these somewhat-legacy network security controls in place, and we're getting more value out of them. If you look at Palo Alto's offering and what they can do at the network level with URL filtering and all the firewall stuff they can do, it's actually comprehensive, and I get a warm fuzzy from having that in front of a network. It's the same thing when people talk about not needing NAT in IPv6 because there's a billion addresses. I like NAT. I like the fact that it hides things; it's okay to hide stuff. I feel people expected a lot of change in this space and it hasn't materialized because common sense won the day. People still want to know "this is my enterprise and this thing over here is not my enterprise." They want to be able to label that, and so I think network security has not evolved nearly as much as we thought it was going to.

About Bruce Potter

Bruce Potter is chief information security officer at Expel where he's responsible for cyber risk and securing the operation of Expel's services. Previously, Potter cofounded Ponte Technologies, which was sold to KeyW Corporation. He served as chief technology officer at KeyW for two years. Well before that, Potter was a security consultant at Cigital at least twice. In another life, he founded the Shmoo Group and to this day helps run the yearly hacker conference ShmooCon. He has coauthored several books including *802.11 Security*, *Aggressive Network Self-Defense*, and *Host Integrity Monitoring*. He regularly speaks at DEF CON, Black Hat, and O'Reilly Security. Potter lives in Maryland with his wife Heidi and their three boys.

Slightly related, what are your thoughts about hacking back? I know you like being very active in monitoring, but what about hacking back—good or bad?

I think it's a terrifying idea. Just on the face of the economics and motivation of the thing. If I'm a car company and I build cars, I have to pay people to keep my network secure, and it's all in support of building cars. If I'm running a criminal enterprise that's breaking into companies to steal stuff, that's my primary mission. And so when a car company, as an example, gets attacked at sites and they want to hack back, they're directly hacking back against the main mission and purpose of this criminal organization. The criminal organization has nothing better to do than be like "you wanna take a street fight? Let's have a street fight."

It's kind of like using a BB gun to shoot at a tank.

Yeah. It's a terrible idea. And what gets me about it is it's a very visceral response to how helpless companies feel right now where they don't know what to do. They don't have a law enforcement backstop of any material amount unless it's a huge breach. If it's a huge breach, then the FBI and everybody will get involved. But if it's small-time everyday background noise ticky-tacky stuff you're battling, there's nothing law enforcement can do, so companies are left standing there on their own being like "I don't know what to do; I guess we'll go after the bad guys ourselves." And it's a losing proposition in my mind.

What is the relationship between preventive security engineering, including software security, which you know I totally dig, and operational security?

The relationship in this day and age is getting closer and closer, with more and more organizations trending toward something that smells like DevOps. I think you're seeing the operational security components being integrated more and more into the developmental and software engineering components, and that's a good thing, because true DevOps environments are

highly instrumented. They're learning from them all the time. They're able to rapidly deploy right on top of themselves over and over, which from an operational perspective is great. Box has been owned, okay, press the big red button, new box is there, box is not owned anymore, and it's patched. That's your recovery process; it's fantastic.

I will say that the one thing I've seen is that there's potential benefit from doing it that way, but the reality of how organizations implement it is often very different because they don't have the security expertise and the development processes. That's where you need to have it in order to have the operational gains. What ends up happening is the developers take over the infrastructure in those kind of environments, and you lose the system administrators. You lose the network security engineers, so you lose all the gates that were associated with it.

You also, by the way, lose architecture. So I'm with you; DevOps can be really good, but it has some gigantic pits on both sides you need to be super careful about.

And for every one organization that's doing this well right now, there are 99 that are doing it terrifyingly badly. And that's what I struggle with, because there's so much potential there. And I've had this argument with people, "there's a lot of potential but if you're not heads-up about it you're going to cause problems." Think about back in the day, when we did waterfall and slower kind of development, if the engineers had something terrible and they threw it over the wall to QA, QA would say "no" and throw it back over the wall. There were all these natural gates because a person would look at it and say "well this is dumb" and throw it back over. But now that infrastructure is code, those gates have disappeared.

Let's talk about CISOs. In your view, what do you think a CISO should do?

In my mind, it's all about managing cyber risk. It comes down to cyber risk management and being able to bring it to an acceptable level for the organization to continue to run its business. So it's a fairly broad brush with which to paint, and it covers a lot of ground, but I found it to be a very useful backstop. I think the role is evolving over time and it's been interesting to see when I was a consultant on the other side where organizations try to home their CISO. It would be homed under the CIO, which in my mind is a conflict of interest. It would be homed under general council, be homed under the CFO, be homed directly under the CEO, and all of those options are better than CIO. And now we're starting to see companies flip it to say hey, the CIO is actually subordinate to the CISO.

And there's a new role too, chief risk officer, which has popped up recently—let's put all the tech stuff under risk.

It makes a lot of sense because it helps the decision-making process. It's not a visceral or a tech thing anymore. It's about supporting the business, and that's the most important thing. I've certainly worked in organizations where the security function was very much, maybe not an island to itself but they felt super self-important.

I think that evolution is going to continue for a while, but we saw the same thing with CIOs. As the CIO concept came into being and then evolved, it went from being kind of a tech thing to driving cost out of the business to enabling the business to whatever. So I think it's an ever-evolving thing. The one true thing is it seems to be the scapegoat when things go sideways.

Last question: You've been tying fishing ties for some time now, especially last March, which is fun to watch on Twitter. You've also been collecting Christmas hats for a longer time. Are there any plans to merge those two things?

So I tied a Santa fly the other day; it was a red fly with some camel hair tufts on the end, which I thought was somewhat symbolic of the Christmas season. When I go on vacation, I'm actually hoping to tie an elf one, which will be a take on an Adams that has little wings, but it'll have little elf ears instead and a green body. So I'm trying to bring them together, and maybe if I'm lucky I can find a Santa fishing hat, but that seems to be going too far.

The Silver Bullet Podcast with Gary McGraw is cosponsored by Synopsys and this magazine and is syndicated by SearchSecurity. ■

Gary McGraw is vice president of security technology at Synopsys. He's the author of *Software Security: Building Security In* (Addison-Wesley 2006) and eight other books. McGraw received a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him via garymcgraw.com.

myCS
Read your subscriptions through the myCS publications portal at
http://mycs.computer.org