Silver Bullet Talks with Gary Warzala

Gary McGraw | Cigital

G ary Warzala, Visa’s chief information security officer, talks about the daily life of a CISO, how companies can attract and retain good security employees, and how to measure security and discuss the results with management.

What exactly does a CISO do?
More than anything, I lead and develop my organization. At the end of the day, I want to understand if we have a good handle on information risk across the enterprise and if we’re applying the appropriate resources to manage that risk. I communicate frequently with our executive team and articulate what we’re working on and why—if we need resources, I tell them why that is, in risk terms, and help set their expectation. Having credibility is extremely important—having the trust in my organization that we’re doing the right thing to enable and protect the business.

You have an MBA—did that help you with your security career?
I wanted to balance the technical side that I developed early in my career with more business skills, and the MBA was one of the best things I ever did, especially when I think about how my career advanced after I received it. The information security professional used to be viewed as someone who required an interpreter to understand what they were doing. I’m very pleased to see that it has morphed into a business-facing role in which security and risk management discussions are routinely held across the organization. Considering the state of affairs in cybersecurity, this is a timely change.

What are the underlying causes of our security woes these days, and what are you doing about them at Visa?
I believe that the root causes haven’t changed, nor has the sophistication of the exploits. Basic security fundamentals aren’t done well, which leads to exploits and incidents. I don’t think the technology has let us down as much as the people side of the equation. I strongly believe that if you start with the right people, and develop good processes along with the appropriate technology, you can build those fundamental information security controls that will secure your enterprise. So for me personally, it really starts with hiring the best security professionals.

How do you identify the good people?
Fortunately for me, it’s easy because of our brand. People looking to work for a company that has a strong security culture know what they’re getting into, and they’re going to be tested on a daily basis. I call these people our digital first responders; they’re the ones who run toward the “fire,” not away from it, the people who aren’t afraid to work in a tense situation. For those of us with this passion, it’s more than a job, it’s our mission. We certainly don’t do this for the money or the job security! For other CISOs in other markets or verticals, it might be a little bit more challenging, but those people are out there—you just have to be persistent in finding them.

Do you do anything special to retain good people?
I think it all starts with the health of the organization. Think of a revolving door—do you have more people
coming in or leaving? That will be your first sign. Retention is strong when your leaders are strong, and when your organization believes in the mission and has avenues for people to grow and advance. When you think about people in the information security field, very rarely do they leave it. How often do you hear about really strong professionals in this space moving into development or into other technology areas? They’re so passionate about security that if you can build a healthy environment that gives them progression in their career paths, they won’t go.

Do you think consumers need to know the difference between security software and software security? That’s a very subtle question that I think would be lost on most people outside the security community. Personally, I don’t think consumers know, need to know, or even care. At the end of the day, consumers are going to use a product or service of choice and expect that the trust and security is there, not how it got there.

The problem is that security is in some sense invisible, so people can make claims about security that might not be true, and it’s hard to differentiate between a strong brand with people doing the right thing, like Visa, and some fly-by-night brand with people who make false claims. Exactly. But I believe that in today’s world, you can’t fake security. It will always catch up with you. The good news is that people will always lean toward the brand that they associate with security and with trust, so you might as well make it a strategic enabler to win more market share. There is no downside.

Do you think we’ve made progress in software security? We’ve made incremental progress, but we have so much further to go, and we keep repeating the same mistakes over and over again. For example, we teach people how to develop quickly, but we don’t really teach them how to develop securely. I truly believe that every IT class taught at every level should have a security theme or thread woven through the curriculum. It has to start earlier—we can’t start the education process in the enterprise, where it’s too costly and there’s too much risk that can be introduced.

How can the education system address the problem of security engineering more effectively than it does now? I think we’re starting to gain traction; we just held the first US Cyber Challenge competition here in the Bay Area as a collaborative effort with Visa, San Jose State University, and the Bay Area Council. The president of San Jose State University, Mohammad Qayoumi, totally understands the fact that we need to expand and enhance our curriculum. Academic leaders at his level understand that we need to do more in this space, so dialogue is occurring, which is the first step in addressing the problem. When you think about the push at the national level to build a cybersecurity workforce, you can see that it’s raising awareness across the country.

Well, as long as it focuses on building security in and not reactive security, I would agree with you. Exactly, but I’m hopeful it’s moving in that direction. Leaders in the security space need to keep advancing the dialogue.

If you had to, say, build a big world view of your whole global risk management purview, would software security be one of its major continents, or is it something that you find in each region? My core software security expertise is sitting on one of the major continents, but it has tentacles that reach out to every region. An analogy about a security program being only as good as its weakest link comes to mind. I use a centralized model with very strong talent and expertise that networks out to a distributed group of security champions who support the cause and mission. This model works best for my organization.

Do they intermingle with operational risk and consumer fraud staff? Yes. We’re building the Fusion Center concept on the East Coast, where we have representatives from all facets of security, risk, and fraud working side by side. The benefits of this model, primarily in information sharing, are invaluable, and we’re looking to continue to mature in this area.

When it comes to security, how do you measure it, and which measures do you find useful when you’re talking to senior executives to garner resources? For me, it’s all about risk, so the

---

About Gary Warzala

Gary Warzala is Visa’s chief information security officer. Before coming to Visa, he was CISO at the Aon Corporation in Chicago and at GE Aviation in Cincinnati. Warzala began his career at GE, where he held senior management positions in telecommunications, architecture, application development, and information security. He has a BS from Utica College of Syracuse University and an MBA from Xavier University. Warzala lives in the Bay Area with his wife Cathi, and their two children, Kristie and Korey.
majority of the conversation centers on information risk. Can I clearly articulate those top five enterprise risks and the risk-mitigating initiatives in place for addressing them? Can I outline the inherent risk in our most critical assets and show, with confidence, the control effectiveness associated with these assets? Can I have a consistent conversation from the last time I met with the board or executive team? Sometimes it’s more art than science, but we’re making investments in our risk program to continually work on refining and improving our data and analytic approach.

One of the challenges is that if you do your job properly, nothing happens. If you frame the problem in terms of risk, it’s probably more effective. Absolutely. No organization is without informational risk. Technology and business innovation are also going to drive changes in your information risk profile, so having the risk conversation with the executive team never gets stale. There’s always a relevant conversation to have and decisions to be made regarding the amount of risk we’re willing to accept.

What are your thoughts about mobile security?
In a word, challenging. Basically, the mobile space is a huge ecosystem, made up of numerous players all with different agendas, and we can’t manage, influence, or control hardly any of it. From a security industry perspective, we’re just evolving in our capabilities. We’re playing on the edges.

And it moves incredibly fast.
It does. New application, capabilities, and products are being introduced daily. And let’s not forget about exponential increases in malware that we’re seeing target mobile applications. It’s going to be a fascinating ride as business innovation, technology, security, and our adversaries all converge into this mobile ecosystem. The “building security in” model is the only way we’re going to stay ahead in this space.

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

Gary McGraw is Cigital’s chief technology officer. He’s the author of Software Security: Building Security In (Addison-Wesley 2006) and eight 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. Contact him at gem@cigital.com.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.