Reputational Risk and Third-Party Validation

CA Veracode's Ryan Davis on the Value of Security Ratings

BITSIGHT

ISMG
INFORMATION SECURITY
MEDIA GROUP

BITSIGHT

Davis is an Information Security Manager at CA Veracode.

Security ratings are increasingly popular as a means of selecting and monitoring vendors. But Ryan Davis at CA Veracode also uses BitSight's ratings as a means of benchmarking his own organization for internal and external uses.

"Taking somebody's word for it isn't enough these days," says Davis, an Information Security Manager at CA Veracode. "You can't just say 'Oh, yeah, well that person said they're secure."

For CA Veracode, security ratings provided by BitSight offer validation to prospective customers. "We want [customers] to be able to have that comfort that somebody else is also asserting that we're secure," Davis says.

In an interview with Tom Field, Senior Vice President of Editorial at Information Security Media Group, Davis discusses:

- How he employs BitSight ratings;
- The business value – internally and externally;
- How these ratings can be a competitive differentiator.

TOM FIELD: Tell me a little bit about your role at CA Veracode.

RYAN DAVIS: I manage the information security team. What this means is I'm managing everything from risk that presents itself on desktop endpoints through our network infrastructure to our server environment, all the way up through all of the instances we have out in AWS. My team is also responsible for risk and compliance, so not only do we get to make sure that we're doing the right thing from a security controls perspective, but we also are the ones who go and work with our customers to do the validation on that.

Third-Party Validation

FIELD: So, Ryan, about validation: In today's threat environment, why do you find that third-party validation of a company's reputation is really so critical?

DAVIS: We've seen throughout the information security community, and you don't even have to stop there, you can just say any industry … taking somebody's word for it isn't enough these days. You can't just say, "Oh, yeah, well, that person said they're secure." In many cases, when that has been the assertion, we come to find out that there's some residual or remedial risk there that gets exploited, and that's presenting the opportunity for bad guys to be able to get in.

The way we think about it is, we want you to be able to have that comfort that somebody else is also asserting that we're secure. And that's probably the biggest trend right now: You can't just take the company's word for it. You really want to have that independent attestation from somebody that's unbiased, not being paid to say, "Oh, yeah, that company does, in fact, know what they're doing from a security perspective."

Multiple Methods

FIELD: Well, that’s a great point. How do you currently get that attestation?

DAVIS: Well, for us, we do it a couple different ways. We, of course, have our own controls in everything that we attest to, and we allow our customers to come in and audit us and ask us questions about those policies and procedures.

In addition to that, we go through a SOC audit, – a SSA16 SOC 2 audit – and we go through and present all of our controls and all of the evidence to an independent third party, and then they weigh in on their assessment of whether we are, in fact, doing those things or not.

And we employ third parties to come and pen test us. Whatever results that they find, we try to respond to those. So there’s no single tool that we’re relying on; we’re really relying on a couple of different mechanisms to assert not only are we saying these things, but we’re actually doing them and here’s the evidence of that.

Role of BitSight

FIELD: Ryan, I want to ask you about a specific vendor, BitSight. Where does BitSight add value to you, both externally and internally?

DAVIS: From where I sit, I’m looking at all these different dashboards to say, “How are we doing from a security perspective?” We have tons of different metrics, and it’s really tough sometimes to say, “Well, does that actually mean we’re more secure?” So where BitSight comes in is they’re providing that independent attestation. They’re giving that third-party voice to say, “Hey, you know what? Veracode does know what they’re doing and here’s the evidence.”

The way we use BitSight here internally is to be able to tell that story not only to our peers in the security industry, but also to executive management and say, “Hey, listen. Here are a number of different dimensions for which you can go and look at a security posture for an organization.” And they give you this lens to be able to look at that and give you a score. It’s very much like a credit score. They’re giving you a rating, if you will, about what the security posture looks like.

We use that as a mirror for ourselves to say, “Here’s what we believe we’re doing and how we feel we’re doing. But from the outside perspective, how does it look like we’re doing?” So we use that as a self-assessment tool to not only be able to look at ourselves, but also share that with folks like executive management or customers.

A Competitive Edge

FIELD: Ryan, as you know, these ratings have become increasingly popular. How can they be used as even a competitive differentiator?

DAVIS: There’s an inherent cost to security. You can’t just go and “do security.” There’s an investment of time, money, resources to have a security program. If you’re trying to assert that, “Hey, we do security,” you have to have something to be able to measure it.

So, when you have an independent attestation, especially with a rating system like BitSight, it gives you the ability to

> "Taking somebody's word for it isn't enough these days."

compare one against the other. And if you say, "Our BitSight rating is 800," and somebody else who is a competitor of ours has a 700 rating, the story kind of writes itself. Of course, there's much more detail there, and when we get in to the minutiae, there are reasons that one rating might be different than another. You're not always comparing apples to apples, but the reality is you can very quickly be able to say, "Oh, well, at first glance one is clearly more focused on their security posture."

It comes up in conversations, especially as part of a sales cycle with our customers – and that's another big aspect to my job. Not only do I have to make sure all of that stuff is secure, but I also have to be able to evangelize it back to our customers. And it's a heck of a lot easier when it's not just me saying, "Oh, yeah, we do those things" but when I can also say: "Go look at this independent third party. They run this rating system. There are thousands of companies which they've rated. Go and take a look at what our rating is out there. Don't take my word for it." It gives you that independent voice.

Why It Matters

FIELD: In this growing and competitive marketplace, why does this one particular differentiator matter?

DAVIS: The reason it matters is because as time goes on, we're getting more and more investment throughout the industry into security. You really have to be able to justify those dollars and say here's why we need that. And when you tie the sales aspect to this, being able to say, especially as a security company, "We're secure and we know what we're doing" makes it an easier story to tell. And hopefully, the customer or prospect in this case has already heard of your reputation, because maybe they went out and did the research beforehand, especially with how much information is available on the internet. A lot of customers are making a decision about which tool is their preference before they even get to you.

So you need to have that reputation of doing security and doing security well, because if you don't, then that's the reputation that's going to precede you. I don't have to look any further than the Target breach. Everybody was very up in arms and hesitant to shop at Target right after because they didn't know what the reputational security posture was, other than the fact that they knew they got breached. So having a tool to be able to represent the reputation of the company that's independent is invaluable. ■

Listen to the full interview at:
https://www.bankinfosecurity.com/interviews/reputational-risk-third-party-validation-i-4126

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io