INTERVIEW TRANSCRIPT

The Quest for Non-Intrusive Security

Richard Bird of Traceable on the Need to Evolve Approach to API Security

TRACEABLE

iSMG
INFORMATION SECURITY
MEDIA GROUP

RICHARD BIRD

Bird is a multi-time C-level executive in both the corporate and startup worlds. He is internationally recognized for his expert insights, work and views on cybersecurity, data privacy, digital consumer rights and identity-centric security.

Insanity in cybersecurity is trying the same failed approaches and hoping for different results. As new CSO at Traceable, Richard Bird wants to stop the insanity and bring a new, non-intrusive approach to defending the digital crown jewels – especially API.

In this video interview with Information Security Media Group, Bird discusses:

- His frustration at how security teams have responded to digital transformation;
- The expanding threats to API security;
- The value of data and context in non-intrusive security.

The Cybersecurity Echo Chamber

TOM FIELD: What is the definition of insanity as it relates to cybersecurity?

RICHARD BIRD: The old adage about insanity being doing the same thing over and over again and expecting different results applies within cybersecurity solutions as well as security practice. We think about the structure of cybersecurity frameworks today, and lots of people tout that “I’m working in a zero trust framework,” or “I’m working in a defense-in-depth framework” and then they get breached through a VPN, which basically invalidates both of those statements and suggests that they’re still working under an OSI seven-layer network model from 1983 as the structure and architecture of their cybersecurity program.

> “Within the cybersecurity solution space …, there’s this continuous repeating of whatever the new messaging is about technologies or frameworks, but about 95% of your actual compute and technology landscape is stuck in these old models.”

Within the cybersecurity solution space as well as within how cybersecurity is being executed within the corporate government agency enterprise space, there’s this continuous repeating of whatever the new messaging is about technologies or frameworks, but about 95% of the actual compute and technology landscape is stuck in these old models. And it’s not just doing the same things over and over again. There’s intellectual dishonesty today that’s saying, “Just because I say I do zero trust, I must be doing zero trust.” And in reality, we’re not doing zero-trusty kinds of things in the background. That level of cognitive dissonance between what we want to do and what’s actually being done creates an escalating curve of cyber losses and cybercrimes, exploits and breaches because we’ve gotten ourselves into an echo chamber.

Stewardship of Data

FIELD: You also have a lot of people celebrating digital transformation, which to them means they get to work anywhere they want with anything they want. Talk about your frustration with how security teams have responded to digital transformation.

BIRD: I was a program lead for a digital transformation program 24 years ago, and we keep rolling out these same labels. Digital transformation has been successfully executed across the entire commercial landscape and government landscape for years and years. There’s still paper, sure. But most of that stuff is information that’s locked up but still accessible. There’s no value to anybody in migrating that information.

When I hear “digital transformation” today, what I’m really hearing is a need, in the business world in particular, to do things faster and cheaper and create better experiences. That’s all great, but faster and cheaper is a pathway to bad security outcomes. I know people want security to be inexpensive relative to their overall spend when it comes to budget, but we’re dealing with adversaries who have no budget meetings, no forecasted spend and run rates, and no needs to manage business expectations around user experiences. The bad guys have agility and flexibility because they don’t have to think about not having friction and making things as easy as possible. Also, if it’s easy for your customer, it’s easy for the bad guys.

> “The idea of stewardship – that we have a responsibility for people’s data, privacy and security – has been lost. Instead, we barrel down a path of technology and technological improvement for the sake of technology and technological improvement.”

The idea of stewardship – that we have a responsibility for people’s data, privacy and security – has been lost. Instead, we barrel down a path of technology and technological improvement for the sake of technology and technological improvement. We want to be cooler and faster and provide more choices. We want to do more connection at the application layer so that this data can move there. And it violates the premise of stewardship that we should be held accountable for.

API Security

FIELD: What needs to be done in this new expanding world of API security – or API insecurity?

BIRD: What I find incredible as I talk to people on API security is how many folks have completely separated history data and evidence from the growth curve in API security. I’ve had senior executives tell me, “I don’t have an API security problem because I have a gateway and a WAF.” And I say, “Are you a hybrid organization? Do you have on-premises still and large business applications that you were unable to refactor to cloud in your cloud journey?”

Satya Nadella said in 2021 at Ignite that we’ve reached peak cloud aggregation. That means if you haven’t refactored that code already to cloud, you’re probably never going to do it. I say to those senior executives, “So you have a hybrid environment, so your firewall is 100% of your security.” And, of course, they give me strange looks. And I say, “Well, if you can’t say with confidence that the firewall is your security strategy for everything in your on-premises environment, you do know that WAF stands for web application firewall. It’s literally the virtualized and conceptualized equivalent of how you manage traffic, inputs and outputs, and blacklisting and whitelisting.” And they pause for a second, typically.

Then I say, “We have taken APIs and moved – after a dozen years with true commercial API enablement – to the next evolutionary stage of virtualization. We started at the infrastructure and the appliance level. We’ve run through that part of the evolution. We are now at Layer 7 security. That security is needed as applications are now becoming the prime intersect for all data, all transactions and the passing of information back and forth. And yet that layer has historically had the worst track record in terms of security, which is not the fault of developers. Developers are in business to create value based upon business needs. They are the translation layer to make technology do cool things.

Our expectation that developers should provide heightened cybersecurity awareness is just kidding ourselves, because history clearly shows that human beings really stink at personal risk and security management, and developers are people. So this API security layer is laboring with a huge misperception that I don’t have a security problem – and that assumption is wrong. The traffic that looks like it’s supposed to be good can actually be malicious and not be caught by gateways and WAFs. That’s the predominant way that these breaches happen. And a lot of leaders are shocked when they realize that their statements about being OK in this space were grossly exaggerated.

"Non-intrusive security provides a way to disintermediate the potential for that moment of realization that you're threatened by negating and invalidating the threats outside of the view of a company or an individual."

Non-Intrusive Security

FIELD: How do we get to, as you call it, non-intrusive security?

BIRD: We embrace the patterns that have historically been a part of human evolution. I always use the example of the beat cop, and a lot of people say, "You use these quaint, rustic metaphors and analogies, and that's not how the digital world works." But let's not ascribe mysticism to technology. Technology is a better tractor. It is a tool that accomplishes production and delivery of value. When we take away the mysticism and look to patterns, there are tons of them that have historically been successful. For non-intrusive security, I like to use the notion of the beat cop.

The beat cop's job is to patrol the neighborhood. You don't know he's there. You have no idea what his name is. You have no need to understand the mechanics of police enforcement or law. It's being done for you. And the result is that your neighborhood, your family and your children are safer. Is it fail-safe? Obviously not. It doesn't mean that bad things can't happen. It means that there is a layer of security that is happening on your behalf that doesn't require your intervention. It doesn't require you to increase your knowledge or improve your sensitivities to all the bad things that might be out there.

The market and enterprise corporations constantly talk about making people smarter about security, but people are actually pretty smart about security. The only problem is that, although we really stink at personal risk and security management, that dynamic changes when we're threatened. Every human being on the planet becomes an expert in security and risk management when a threat manifests. Non-intrusive security provides a way to disintermediate the potential for that moment of realization that you're threatened by negating and invalidating the threats outside of the view of a company or an individual.

I believe this is how we need to start thinking as cybersecurity practitioners and solutions deliverers on how to apply and exercise security, use the patterns that we know work, and accommodate for the fact that the big difference is volume and speed – especially in the API world, which has lots of volume and speed. We need to go back to what we know is effective as opposed to continuing to rely on models that have been proven by data and results to be ineffective. The layered model of security has been proven wrong by results, but it's still the predominant mode of providing security in the marketplace.

The Importance of Context

FIELD: In the world of non-intrusive security, what's the value of data in context?

BIRD: The absence of context in the way that we manage all aspects of security has been one of the biggest blunders that we've made since the beginning of compute. The first account and password in 1961 at MIT was hacked within 11 hours by the graduate students. The context piece is now becoming a huge component of people's thinking around security. Context is the need for intelligence, information inputs and signals that give us an understanding of who, what, where, when and why.

Asking these key questions allows us to deliver not just security, but customer or user experiences. Understanding the information that answers each of those questions is what delivers a contextually aware security result, customer experience, and transaction. That's been missing because we are still in a world of patterns in history that have proven themselves not to work. Nobody is building a castle with a moat anymore. People are building air defense systems that are predictive and utilizing the context of current state warfare and engagement and all of the information that's coming in from that. And that context piece is now being aggressively pursued within the solution side by a number of organizations.

Within the API world, however, where there's so much access to so much data, we're quickly coming up to a brick wall around how to manage privacy. We may have a tremendous amount of intelligence about an individual but some of it is sensitive and could be personal, or proprietary if we're talking about relationships between partners. We have not bridged the ethical, academic and governance concerns related to this contextual side of the equation. But contextual security is not an API-specific trend. Having data-enriched information about things is where security will be heading for many years to come.

New Constructs for Security Delivery

FIELD: Richard, what attracted you to Traceable AI? And now that you're in this role, how are you helping your customers evolve their approach to cybersecurity?

BIRD: My reputation in the last several years has been heavily oriented toward the identity domain within security. But worry motivated me to step into the domain of API security and application security. I worry that the identity solution space is so constrained by the models of the past. For example, passwordless arose and everyone talked about it as the next best thing since sliced bread and a toaster. But passwordless is just iterative. It's the next iteration of strong authentication. It's still dependent upon all of the necessary good behaviors and best practice execution in order for it to be able to work right.

Andre Durand, the founder and CEO at Ping Identity, said it best: "Passwordless is great, but if you authenticate the wrong person, you still have a bad day." When we look at the constructs constraining the identity solutions space, we're still talking about directories. We're still not using security language when it comes to the human attack surface or the threat vectors of identity or identity intelligence. The identity space is not giving room for innovation. API security is nascent. We're playing catch-up. Historically, application developers and engineers are three to eight years ahead of security in every single technological innovation, which means that we are years behind in securitizing APIs and providing capabilities for visibility and guardrails.

That's exciting. It allows you the opportunity to not just innovate but to really drive toward a possible new construct for how we deliver security – whether it's non-intrusive or done in a way that everybody in the future has their own API that provides permission for you to use my data, not use my data, delete my data or transfer my data. Maybe that's the world that we potentially have coming, but the identity solution space does not have the mechanics available to be able to execute on that. When I moved to API security, everyone thought I had abandoned identity. But if you look at the OWASP top 10 relative to security threats for APIs, 30% of them are about identity. Security is still rooted in the basis of identity, whether it's the hard security trades or threat intelligence.

Flexible Deployment Models

FIELD: Given how organizations are shifting to distributed microservices architectures, what are your thoughts on flexible deployment models?

BIRD: Flexible deployment models are an absolute necessity. Bad actors aren't beating us with technology; they are beating us with a substantial amount of flexibility and agility that has been atrophied within the corporate and government sectors. We love to say that we're flexible and agile, but it's not really true. We love to say that moving to Agile and Scrum and getting away from Waterfall SDLCs has improved our flexibility and agility. But the evidence clearly shows the bad guys are 10, 20, 30 times more flexible and agile.

Flexible deployment capabilities and strategies are fundamental to changing that. The challenge, which we all recognize, is: Operations are still operations, and operations risk is still operations risk. We can't ever put ourselves in a situation where we're executing deployments that increase our risk. Doing a deployment where we accidentally leave an endpoint API input publicly exposed has happened in the last couple of weeks.

We have to take the flexible deployment models and capabilities and build in the layer of non-intrusive security where APIs are being monitored and understood, and not just guessing that the behavior patterns of those APIs are anomalous. We're putting a tremendous amount of rich data into analytic tools that show us how an API is changing over time to be used for bad things. We need those capabilities because, without them, we create models that allow us to be flexible and agile but then exponentially increase the risk of self-harm because of irresponsible use of those capabilities.

The Value of Diverse Deployments

FIELD: Why should companies consider vendors who can deploy into multiple environments?

BIRD: Because nothing in technology ever dies. There are a few technical reasons, but a lot of important business reasons, whether it's distribution of risk or management of compliance regulations. You may want to use a particular cloud solutions provider, but you've got data control and restrictions because it's in a particular nation or region. The diversity available from infrastructure capabilities and application deployment capabilities is incredible. It's probably the key benefit to cloud and hybrid strategies, because now we don't have to navigate, with a tremendous amount of trickery, our global expansions, how we operate in this region versus that region or how we respond to catastrophic world events.

As we've seen the need to extract assets, value and data out of areas of the world that have chosen to do things that cause us to no longer do business with them, this cloud capability makes us able to extract ourselves from those events and situations. But when we think about the strategies that are associated with this, we run into the same problem we talked about with flexible deployment patterns, which is what Jeff Goldblum said in "Jurassic Park": "You thought just because you could do a thing, you should do a thing."

The rush to have a multi-cloud strategy or move into a particular region frequently comes without understanding what's needed and without the ability to underpin the security. More importantly, there is not a lot of good thinking about what the unintended consequences of those choices might be. Making a huge decision on changing your overall platforming strategy just to gain incremental value or revenue opportunity should be part of the equation, and many times I don't feel that it is.

Watch the full interview at https://www.bankinfosecurity.com/quest-for-non-intrusive-security-a-20323

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 34 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.

(800) 944-0401 • sales@ismg.io

BANKINFO SECURITY® CUINFO SECURITY® Just for Credit Unions GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

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

iSMG
INFORMATION SECURITY
MEDIA GROUP

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