DIALING UP the FUTURE

AT&T was around for the horse and buggy; now it's a "power user" of AI, according to Chief Information Security Officer **RICH BAICH.** He talks about building—and defending—the invisible infrastructure so integral to the tech's future.

It's 2:34 AM and a chief information security officer gets a call saying their company's network has been hacked—so opens Rich Baich's 2005 book, *Winning as a CISO*.

In the 20 years since Baich wrote his book, cybersecurity risks have surged—think remote workforces, countless connected devices, AI-fueled hackers—and made the opening scene of Baich's book read more like a prediction than a simulation.

The first question Brunswick Partner Ash Spiegelberg put to Baich: "Do CISOs ever sleep through the night anymore?"

"The older CISOs do," Baich said, laughing. "They recognize there's a lot you can do—get the right people, the right strategies and tools and information—and they don't lose sleep over what you can't."

In addition to writing the book on being a CISO, Baich has served in that role for Wells Fargo, AIG, the Central Intelligence Agency—and now, AT&T.

For most people, leaving the CIA would mean stepping away from national defense. For Baich, it was a kind of continuation. "I took this role at AT&T because of the criticality for our customers and for the country," he said. "Finance, healthcare, education, our military—without telecommunications, they're all at risk."

A 140-year-old telecom giant might not be the first name you think of when it comes to AI, but AT&T's network is critical to the technology's future in America. Every ChatGPT query on a smartphone, every autonomous vehicle navigating traffic and every other AI-powered device that uses real-time data depends upon fast, reliable cellular networks and internet connections.

Baich recently sat down with Spiegelberg, who co-leads Brunswick's technology, media and telecoms practice. The pair talked about how the company is already using AI to defend that network, while also enlisting the technology to help with everything from blocking robocalls to mapping technicians' routes.

AI may be the future, but their conversation frequently returned to the past—it was, in fact, where their conversation started.

When people think of AI, they probably don't think of telecoms companies. Can you give a sense of how you and your teams use AI?

There are two things to say about that. First, AI isn't new to AT&T. Some of the first examples of machine learning took place in AT&T Bell Labs in the 1950s, when a mechanical mouse learned to navigate a maze from experience. In 1956, our researchers helped organize the conference where the term artificial intelligence was born. AT&T was one of the first companies to create a firewall. We've always been innovative in this particular space.

And second, we're power users of AI. We use AI to dispatch and schedule our technicians more effectively. In 2023 we launched "Ask AT&T," an internal GenAI tool that can summarize calls and documents, answer questions, things like that. More than 100,000 employees use it, and it's generating over a billion tokens a day—essentially a billion words.

As for our cyber operations, we're using algorithms to detect and respond to threats. They help us prevent and detect fraud, identify anomalies and deviations from the norm, and shorten the time frame between identifying a threat and being able to act on it.

We also use it in robocalls. So AT&T ActiveArmor, for instance, we use machine learning and the power of the network to help detect and frustrate illegal robocalls in real time—every month, roughly 1.5 billion robocalls are blocked or labeled as spam.

What role do you see AI playing in the future of cybersecurity?

What you're seeing today with AI, you see with any emerging technology. When the internet was built, the director of the CIA said we built something we've yet to know how to protect. We learned to build firewalls, antivirus and so on. Then you move to the world of cloud. The industry didn't build security into the cloud. So we all started asking: Do we know where our cloud is? Do we have a configuration? Do we have access management? Are we protecting the vulnerabilities?

It's the same with AI. We're asking: Where is AI in our environment? How are we making sure that it is secure? Are we scanning for access controls? How do we know that AI from a third party is secure?

There's a long history of having to protect emerging technologies or platforms; AI isn't much different than any other new, important infrastructure you have to protect.

How the bad guys use AI—deepfakes, spreading misinformation—attracts more attention than how people are using it to stop them. Is that imbalance a fair reflection of the landscape?

I'm going to go back to history again, because whenever you look at IT advancements, the same issue always comes into play. It's not the actual technology that creates the risk, it's the application. Bad actors figure out how to use the technology to circumvent existing safeguards and controls. They're at an advantage, because they're purely focused on finding one way around a control that's in place.

Back in the '90s, when firewalls were initially released, all the ports were wide open. They quickly realized that meant the human had to know what to close; it was like Swiss cheese. So about 18 months into the cycle, they switched it—all the ports were closed, and you had to go in there to open one. Fast forward to the cloud and you saw something similar with S3 buckets, which were left open by default until someone manually closed them. Now they ship them closed and allow you to open them.

It's not the exact same thing with AI. But adversaries are using AI, and it helps them move with speed—speed to weaponize, speed to deliver. But AI allows us to move with much greater speed as well.

The area you work in requires such deep technical knowledge. How do you help leaders grasp the risks and investments needed to manage it?

So first off, it's being part of the whole AI team. We work very closely with our Chief Data office, which creates a lot of our AI engines and really drives our AI vision. We're part of our data and AI governance review board. We're talking about these issues and incorporating the controls well in advance of launching any large language models, AI-powered agents, things like that.

That's primarily how we try to do this: get ahead of it in the design cycle, understand and point out the risks, and put the controls in place.

As you look ahead, what most excites you about AI? What most concerns you?

I'm excited about AI helping us do things like data analytics and anomaly detection with much greater speed and granularity. The unique insights that come from those—that's really exciting.

My concern: As quantum computing emerges and the power associated with that, combined with AI practices—those could allow bad actors to perform and deliver executable risks at a whole new speed and volume in power. And attackers always tend to be at an advantage in some respects, because as a defender, you almost have to reengineer their techniques to then be able to guard against it.

I think most people assume cybersecurity is largely a question of technology, yet you often talk about the importance of culture.

I've had 15 people that have worked for me now that have gone out to be CISOs, and whenever they call me, I focus on the culture.

Because the type of leader you are needs to be matched with the cultural appetite of the organization. If your vision, your goals and the discipline that you want to bring to the organization align, then the entire workforce gets behind it.

We talk about tone at the top, but ultimately, to be successful, every person in the organization has to be part of the cybersecurity team, the risk team, whatever you want to call it.

That's such an important piece when you think about AI. We provide guiding principles around AI—and I think every organization should have them so their workforce has something to lean on when they're thinking about using it. We believe AI should be by people, for people; it should be responsible; and it should be secure and ethical.

We've published those guiding principles; we stand behind them. We know no organization is going to do it perfectly, but we're committed to doing it right. ◆

"WE USE MACHINE LEARNING AND THE POWER OF THE NETWORK TO HELP DETECT AND FRUSTRATE ILLEGAL ROBO-CALLS IN REAL TIME—EVERY MONTH, ROUGHLY 1.5 BILLION ROBO CALLS ARE BLOCKED OR LABELED AS SPAM."

RICH BAICH,
Chief Information Security Officer, AT&T

ASH SPIEGELBERG, a Partner, is co-head of Brunswick's tech, media and telecoms group. He is based in Dallas.

ILLUSTRATION: LINCOLN AGNEW; PHOTOGRAPHS IN ILLUSTRATION: COURTESY OF AT&T ARCHIVES AND HISTORY CENTER