Leadership profile: five questions with Chris Lugo, Blue Cross Blue Shield Association CISO

Insight

November 18, 2025

Category: cybersecurity

Tags: cybersecurity, healthcare, infrastructure, leadership

When it comes to protecting sensitive health data, driving innovation, and shaping the future of digital trust, few do it with the vision and precision of Chris Lugo, Vice President and Chief Information Security Officer (CISO) at the Blue Cross Blue Shield Association (BCBSA).

Recently recognized by Crain's Chicago Business as one of its Notable Leaders in Health Care Technology, Lugo leads enterprise cybersecurity, digital innovation, technology experience, and cyber resilience across 33 Blue Cross Blue Shield Plans, safeguarding the personal information of 117 million members across the country and ensuring access to health care services.

He manages a $100 million budget and a team of 120 professionals whose mission is clear: to deliver scalable and resilient technology by ensuring member information is safe, secure, and protected.

Under Lugo's leadership, BCBSA launched a systemwide cybersecurity strategy that unified all Plans under a single "north star." This framework transformed how the organization manages risk and resilience, strengthening defenses as emerging technologies – including AI – reshapes health care services for millions of Americans.

The result: a more connected, secure, and future-ready ecosystem that makes the Blues an industry leader in digital trust.

We caught up with Chris about the evolving cybersecurity landscape, the changes in the profession, and how he recharges when he's not defending against cyber threats.

How did you get into cybersecurity and technology? Have

you always known this was your calling? Was there a moment where “you just knew?”

I didn’t always set out to be a CISO – but I’ve always been driven by curiosity. Early in my career, I was fascinated by how systems connected, getting things to talk to each other, and how one small oversight could have big consequences. My early experiences showed how interconnected our digital world had become, the imperative to embrace technology benefits, and how vital it was to protect the services that people depend on every day.

The turning point came when I realized that cybersecurity wasn’t just a technical challenge – it was personal and it was paramount to every single human. Every decision, every safeguard, ultimately protects someone’s life, livelihood, and someone’s future. This way of thinking drove my focus from “how do we defend systems?” to “how do we protect people?” That’s the mindset I carry today and that keeps me motivated to continue to advance safe technology adoption.

What do you think are the biggest challenges facing the cybersecurity industry – or technology more broadly – today?

We’re at a critical crossroads in technology; one we’ve seen before and, at the same time, one that is completely new to all of us. We’ve never been more technologically advanced, yet never more vulnerable than we are today. The speed of technology change is happening faster than ever; with benefits and challenges we won’t really fully understand for some time. AI has revolutionized innovation and brought different risks. Threat actors can automate attacks at scale, craft realistic deepfakes, and exploit human behavior faster than society can adapt. Meanwhile, the global shortage of cybersecurity professionals has created a skills gap that makes defending modern enterprises even harder.

But the biggest challenge isn’t the tech – it’s culture. Too often, cybersecurity is treated as a compliance function instead of a strategic enabler – a way to grow and to flourish. The most successful organizations are the ones that embed resilience thinking into everything they do – from product design to strategic planning with the board. At BCBS, we’ve worked hard to shift security from being a hidden secret to being visible and empowering – integrated into innovation, not in the way of it.

What does the Crain’s recognition mean to you?

It’s an incredible honor, but it’s not a solo achievement – it reflects the dedication of an entire organization and the people who work tirelessly every day in cybersecurity. At BCBS, our teams wake up with one purpose: *to protect the trust our members place in us.* That’s a responsibility we never take lightly. This recognition is really for them – for the

analysts, engineers, and leaders who make security part of the culture, not just a checklist.

On a personal level, it's gratifying to see cybersecurity leadership recognized alongside other health care innovators. Cybersecurity has traditionally operated behind the scenes – this kind of spotlight helps underscore how digital trust is foundational to public health. When people feel safe sharing their information, it enables innovation, care coordination, and better health outcomes for everyone. My hope is that recognition puts a face to the countless people who strive to make the word safer all the time in an often overlooked and not well understood field of cybersecurity.

What advice do you have for students who just graduated, or will be graduating soon, who want to make a break into cyber or tech?

Start with curiosity and humility. You don't have to know everything on day one – nobody does or ever will. What matters most is your energy, aptitude, and attitude. Cybersecurity changes daily, and the best professionals are those who are constantly asking questions and looking for new ways to do things. Challenge the status quo!

Equally important are soft skills. The ability to communicate clearly, build relationships, and empathize with others is what turns technologists into leaders. If you can explain complex risks in plain language – and build trust while doing it – you'll stand out. Cyber is no longer just about firewalls and code; it's about helping people accomplish something new, different, or difficult.

What do you do when you're not playing cyber superhero? Hobbies, passions, or interests?

Balance is critical – especially in a field that never truly sleeps. For me, that means unplugging and reconnecting with what matters most: family, travel, and time outdoors. Whether it's running, exploring new places, or experiencing the world through someone else's viewpoint, I find those moments bring clarity and creativity that you won't get from behind a screen.

I also spend a lot of time mentoring and speaking with emerging leaders. Helping others navigate their journey – especially in a field as demanding as cybersecurity – is one of the most rewarding parts of my work. At the end of the day, leadership isn't about what you accomplish alone; it's about the people you lift along the way.

Extra credit: favorite book, movie, band or song – and why?

Favorite book? *"The Art of War"* by Sun Tzu. It's timeless wisdom about preparation, awareness, and the power of understanding your adversary – lessons that translate directly into cybersecurity strategy.

Favorite movie? *"War Games."* It's a great movie that indirectly helped me start thinking about the fragility of computer systems and what that can mean to broader society. The film also influenced policy on computer security. I guess simulating the start of Word War III can have that effect on things!

Favorite band? Tool. Their music embodies innovation and patience; traits I work hard to bring into my leadership style all the time. In a field that's constantly changing, being methodical, applying different layers, and seeing things from different vantage points is a must; just like the layered composition of their music.