PROFILES IN *Confidence*

JAVED IKBAL

CISO
BRIGHT HORIZONS

Headquarters: Newton, MA

Employees: 33,000

Annual Revenue: $2.7 Billion+

PRAGMATIC DEFENDER

Javed Ikbal isn't easily distracted by hype. As Chief Information Security Officer at Bright Horizons, he's seen enough industry fads come and go to know where real risk lives, and it's not always in the next buzzword.

"Everyone's talking about AI threats and post-quantum cryptography," he says. "But we're still losing ground to the basics. Social engineering is still one of the most dangerous threats, and too many people think giving everyone MFA is enough."

With over a decade at Bright Horizons, a global childcare and early education provider, Javed has cultivated a culture of grounded, intelligent cybersecurity, one where risk is managed not through flashy tech, but through thoughtful prioritization, storytelling, and an unshakable sense of fiduciary duty.

THE REAL THREATS ARE HUMAN

Javed places social engineering under a broader umbrella, human-centric vulnerabilities that can't be patched with software. "You can still walk into an office with a clipboard at lunch and find unlocked computers," he notes. "Remote work has actually helped reduce some of that attack surface. But in physical offices, it's still a real issue."

He sees phishing tests as another area where companies may be over-investing without evolving. "The value diminishes with each repeat test. Doing four phishing tests doesn't make you four times more secure than doing one."

What's undervalued, in his view, is application security. "If you have public-facing apps and remote access infrastructure, that's where nation-state actors are going. VPNs are often the weakest link. Once someone's in, they've bypassed your firewalls. Now it's all about lateral movement."

"IT'S MY JOB TO EXPLAIN IT"

Javed's measured approach extends to his executive relationships. "I've been very lucky," he says. "Any time I've brought something to the executive team or board, I've had their full attention and support. But it's not their job to understand this stuff upfront, it's my job to explain it clearly."

His philosophy on budget echoes this clarity. "Security doesn't get a blank check," he says. "Just like the VP of Marketing is held to their targets, I'm held to mine, mine just look different. I treat every dollar like it's coming out of my own pocket."

That mindset extends to resilience. While Bright Horizons doesn't operate critical infrastructure, it has invested heavily in continuity. "We can fully failover our services in less than 24 hours. We do it not because we have to, but to assure our clients and our board that we protect not just confidentiality, but availability."

KEEPING UP WITH THE BUSINESS

The greatest challenge, according to Javed, is scale, specifically, how to match security operations with the velocity of the business. "Companies will hire 100 engineers pushing 10,000 lines of code per day, but the application security team doesn't scale at the same rate."

He dreams of building a formula, something like a security-to-business ratio, to help organizations baseline their security investments. "If you've got millions of lines of code, how many AppSec people should you have? If you've got X number of firewalls, how many network security folks? It's all out there. We just need to model it."

The shift to DevOps and continuous deployment has transformed the game. “We used to do one big release every six months. Now it’s multiple tiny updates per day. But threat actors don’t wait until your next pen test. They’ll attack any time. And most companies are not keeping up.”

PRACTICAL AI AND REALISTIC EXPECTATIONS

Despite industry hand-wringing, Javed sees AI as a tool more than a threat, at least for now. “We use AI in our call centers for summarization and sentiment analysis. We use it in staff scheduling. We’ve blocked general-purpose tools like ChatGPT, but we’ve approved Microsoft Copilot because it has gone through privacy and security vetting.”

When asked if he’s anti-AI, he smiles. “My job would be impossible without it. I’ve been using AI in endpoint detection and response for years, it’s just called machine learning. It’s not about saying yes or no to AI, it’s about using it responsibly.”

TRAINING WITHOUT THE TRAINING

Perhaps the most innovative aspect of Javed’s approach is how he handles security awareness.

When employees report suspicious emails, they get more than an answer, they get thanks. “We tell them, ‘You did the right thing. Now please share this with your colleagues over lunch.’ That way, we avoid boring PowerPoint trainings and instead create hundreds of micro-trainings every month that are casual, conversational, and far more memorable.”

This subtle form of influence reinforces his broader belief: cybersecurity is cultural, not just technical.

THINKING THE UNTHINKABLE

Javed believes the greatest threat is what you haven’t yet imagined. “It’s the ‘unknown unknowns’ that will hurt you. That’s why we have to think about the absurd scenarios. Why wouldn’t someone steal a car if your dealership leaves the keys inside? Just because it hasn’t happened yet doesn’t mean it won’t.”

He references the concept of the “Black Swan”, unpredictable events that shatter assumptions. “We’ve seen vendors dismiss vulnerabilities as too hard to exploit. The next day someone publishes proof of concept. That’s the game we’re in.”

SECURITY THAT STAYS HUMAN

At his core, Javed’s approach is one of humility and pragmatism. He doesn’t claim to have it all figured out, but he knows what matters: explaining risk clearly, treating security like any other accountable business function, and never underestimating the power of simple human behavior.

“If we get breached,” he says, “it’s not about blaming someone. It’s about asking: did we prepare, did we warn, did we prioritize the right things?”

In an industry often dominated by noise, Javed Ikbal’s quiet clarity is a rarity—and perhaps, a blueprint.