

Why India needs more women at the table when designing digital security



As India faces a surge in AI-driven cyber threats, experts say the country's digital defenses must become more human-aware and inclusive. Increasing women's participation in cybersecurity leadership is no longer just about representation, but a strategic necessity in designing products that better understand user behavior, trust, and emerging "cognitive attacks"

"Who was in the room when this product was designed?"

The question sounds simple. But in cybersecurity, it is one of the most consequential questions you can ask. Because the gap between a product that protects people and one that merely processes threats often lives not in the algorithm, but in the assumptions baked into how the solution was conceived, communicated, and built.

India's threat landscape in 2026 demands that we take that question seriously. In 2025, India witnessed 265.52 million malware detections across over 8 million endpoints, averaging 505 detections every minute. These are not isolated incidents. They are AI-assisted phishing campaigns that read context and respond like a human would. They are fake government app clones - like the NextGen mParivahan malware - that steal UPI credentials from people who did everything right except trust the wrong interface. They are digital honey traps built on AI-generated personas. The sophistication of the attack has far outpaced the simplicity of the defense. That gap is a universal problem, and such problems are solved by diverse teams.

This is where the gender conversation belongs - not as a footnote, but as a strategic imperative.

Women and men bring distinct yet complementary strengths to decision-making in cybersecurity product strategy. Women often infuse proceedings with a high Emotional Quotient (EQ) and

empathy, enabling deeper connections with end users whose trust and behaviors are central to countering cognitive attacks. This user-centric approach ensures solutions resonate on a human level, fostering intuitive designs that bridge technical protections with everyday usability. In contrast, men tend to excel in practical, logic-driven decision-making, delivering efficient, scalable implementations. Both of these approaches are required to power robust defenses like behavior-based NGAV and anti-ransomware layers and much more.

Women leaders consistently bring this lens, not out of obligation, but from lived experience. Navigating systems as underrepresented participants often builds a sharper awareness of blind spots. And in today's world of "cognitive attacks," where threats exploit human trust and behavior, that awareness becomes a critical advantage. This synergy extends to the boardroom, where women's relational skills harmonize end-user insights with stakeholder alignment, while men's pragmatism drives execution.

However, the conversation cannot stop at representation alone. Today, access to opportunities is improving. More and more women are joining the technology and security ecosystems. But reaching leadership and owning that space still comes with invisible barriers: perceptions, constant evaluation, and self-doubt. What often holds women back is not capability, but hesitation. The tendency to overthink, to question readiness, to consider how decisions may be perceived, while others move forward without that pause.

This must change

Women in cybersecurity and in technology need to be more forthcoming, more competitive, and more fearless in putting themselves forward. The industry is evolving rapidly, especially with AI reshaping the landscape. Opportunities are no longer simply given; they are created and claimed. This is not the time to wait. It is time to step up, build capabilities, and take ownership of leadership roles.

Women remain underrepresented across cybersecurity leadership in product, strategy, governance, and policy. This is not just a pipeline issue; it's about sponsorship, visibility, and mindset. While organizations must continue building equitable systems, women also need to step forward with confidence and conviction.

As India builds its digital security architecture in real time, the defense must be dynamic, human-aware, and inclusive. And that begins with who is in the room - right from the inception of a product till the time it's safeguarding the end user. Women must not wait to be invited; they must claim their space, bring their voice, and lead from the front. Because the future of cybersecurity will not just be defined by technology, but by the people who design it. And it's time more women are not just present in that room but leading it. India news analysis.

(The writer is a Head of Product Strategy, Quick Heal Technologies Ltd)