Cybersecurity

WELLS FARGO

The Blind Spot: Why Attackers Study People Better Than We Defend Them

Sarah Gosler, Managing Director - Head of Cyber Resiliency and Human Defense

August 2026

Overview

In 2023, a sophisticated intrusion at a casino began not with malware, but with a phone call. An attacker reportedly contacted the IT help desk, impersonated an employee, passed basic verification checks, and convinced support staff to reset credentials. The breach that followed disrupted casinos and hotels across the country.

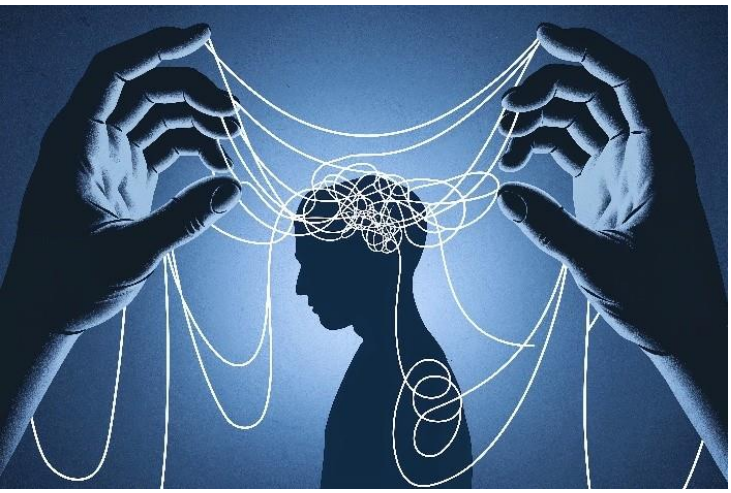
No zero-day exploit. No novel malware strain. Just persuasion.

We continue to describe incidents like this as “social engineering,” as though they are peripheral to cybersecurity. They are not peripheral. They are central. And they reveal a structural blind spot in how we think about human-centric defense. Attackers are not primarily exploiting lack of awareness. They are exploiting psychology.

We Are Measuring the Wrong Thing

Human-centric cyber programs often focus on awareness, training completion, and phishing click rates. These are important hygiene metrics. But they measure whether employees recognize a suspicious email — not whether our systems withstand deliberate psychological manipulation.

Consider what the adversary actually studies: authority bias, urgency and time pressure, reciprocity, shame and secrecy, status and reward. These are not technical vulnerabilities. They are predictable human tendencies, remarkably consistent across industries, cultures, and roles.



The attackers understand this. Many organizations do not.

In a breach involving a cryptocurrency exchange, the initial compromise reportedly involved social engineering contractors to gain access. In other high-profile incidents, from an energy company to numerous ransomware intrusions, the path in was not brute-force cryptography. It was human trust.

We keep treating these as awareness failures. However, they are design failures.

Human Behavior Is the Attack Surface

For years, cybersecurity was framed as a technical arms race: patch faster, monitor better, segment networks, deploy EDR. That remains essential. But the modern threat landscape, accelerated by AI-generated content and scalable impersonation, has shifted the terrain. The attack surface is not just code. It is cognition. Adversaries conduct reconnaissance on social media platforms. They study organizational charts. They identify new hires, high performers, contractors, executives traveling abroad. They craft pretexts tailored to individual roles and psychological profiles. This is human reverse engineering.

They do not blast generic phishing emails and hope for luck, that happened in the 1990s. Today, they iterate. They test language, refine tone, mimic internal workflows, and map escalation paths. In short, they study people better than most organizations defend them.

That is the blind spot.

Why Awareness Alone Fails

Most human-centric programs are designed around the individual employee — did you click, did you report, did you complete the training? When something goes wrong, the reflex is to retrain.

But if a help desk process allows a single persuasive phone call to bypass identity verification, that is not primarily an awareness problem. It is a systems problem. If executives are consistently targeted with business email compromise because of public travel patterns and predictable delegation behaviors, that is not a vigilance failure. It is a structural exposure. Blaming individuals is easy. Redesigning systems is harder.

True human-centric defense does not ask, “Why did they fall for it?” It asks, “Why did our system make it possible?”

AI Will Widen the Gap

Artificial intelligence will not eliminate social engineering. It will industrialize it. Language models can generate perfectly tailored messages at scale. Voice cloning can replicate tone and cadence. Deepfake video can produce credible executive impersonations. The cost of psychological precision is collapsing.

But AI also offers defenders a mirror. It can surface behavioral anomalies, model escalation patterns, simulate adversary tactics in wargames and pre-mortems, and help organizations see how their own workflows create opportunity for manipulation. The question is not whether AI replaces human defenders. The question is whether organizations are willing to confront their blind spot before attackers exploit it more efficiently.

Human-centric cyber defense must evolve from awareness programs to adversary-informed design — testing help desk protocols against realistic pretexting simulations, running executive wargames that stress authority and urgency bias, modeling insider threat not just as malice but as pressure and coercion, and measuring systemic resilience rather than individual compliance. The shift is from “train the workforce harder” to “design the organization smarter.”

Cybersecurity became human the moment attackers realized that trust scales faster than malware. The organizations that will outperform in the next decade are not the ones with the most training modules. They are the ones that understand the human mind is part of the infrastructure, and defend it accordingly.

Until then, the blind spot remains. And adversaries will continue to study it more carefully than we do.