PRACTITIONER BRIEF

SANS 2026 Security Awareness & Culture Report

Behavior Change Is Not the Finish Line

Workforce Security and Risk Training

SANS

What the data is telling us

If your security awareness program has moved past annual, check-the-box training and started changing behavior, that's real progress. It also means you're right where most of the industry is today. In this year's survey of more than 1,700 security awareness practitioners, 45% of programs are in Stage 3 of the SANS Security Awareness & Culture Maturity Model: Promoting Awareness and Behavior Change. That's the largest single group in the model, and it reflects a longer trend.

In 2016, only 2.2% of programs had reached the top stage of the maturity model, Optimization and Resilience, while nearly a third were Non-existent or Compliance-focused. A decade later, those numbers have essentially flipped: Just 3% are Non-existent, 19% are Compliance-focused, and 12% have reached Optimization and Resilience. The industry has slowly moved away from pure compliance toward real behavior change, and Stage 3 is where that shift is concentrated today.

The 2026 SANS Security Awareness & Culture Report draws a clear line between two things people tend to treat as a single milestone: changing behavior and building a security culture. They're connected because sustained behavior change eventually becomes culture, but they're not the same achievement. Understanding the distinction is what separates programs that continue to grow from those that plateau. The simplest way to differentiate the two stages is this: Behavior is what people do; culture is what people think and feel.

45%
of programs are in Stage 3— the largest single group in the model

3%
Non-existent in 2026, down from nearly a third a decade ago.

12%
of programs now at Optimization and Resilience stage - up from 2.2% in 2016.

> Stage 3 isn't a sign of a poorly run program. It's the longest stage in the model and the most under-resourced. The goal is to hold steady, not skip ahead.

What Stage 3 Looks Like

- Top human risks identified and prioritized
- Training delivered throughout the year, not just once
- Employees report incidents and ask security questions
- Security habits visible in everyday behaviors
- Some departments more engaged than others
- Program still dependent on key individuals
- Leadership buy-in present but not fully embedded

That's still behavior change, not culture change. The 2026 report defines security culture as your workforce's shared attitudes and beliefs about security, not just what people do when a phishing simulation lands in their inboxes. The maturity model treats behavior and culture as sequential, not separate: Sustained behavior change is what eventually becomes embedded in the culture. The shift from one to the other takes years of consistency, not a single strong quarter.

Two Ways to Tell Behavior From Culture

Lance Spitzner, SANS Technical Director, the report's co-author, puts the distinction even more concretely:

> “Behavior is teaching people what to report and how. Culture is making sure they feel safe reporting even when they know they caused the incident.
>
> Behavior programs measure how often the security team engages the workforce. Culture programs measure how often the workforce engages the security team.”

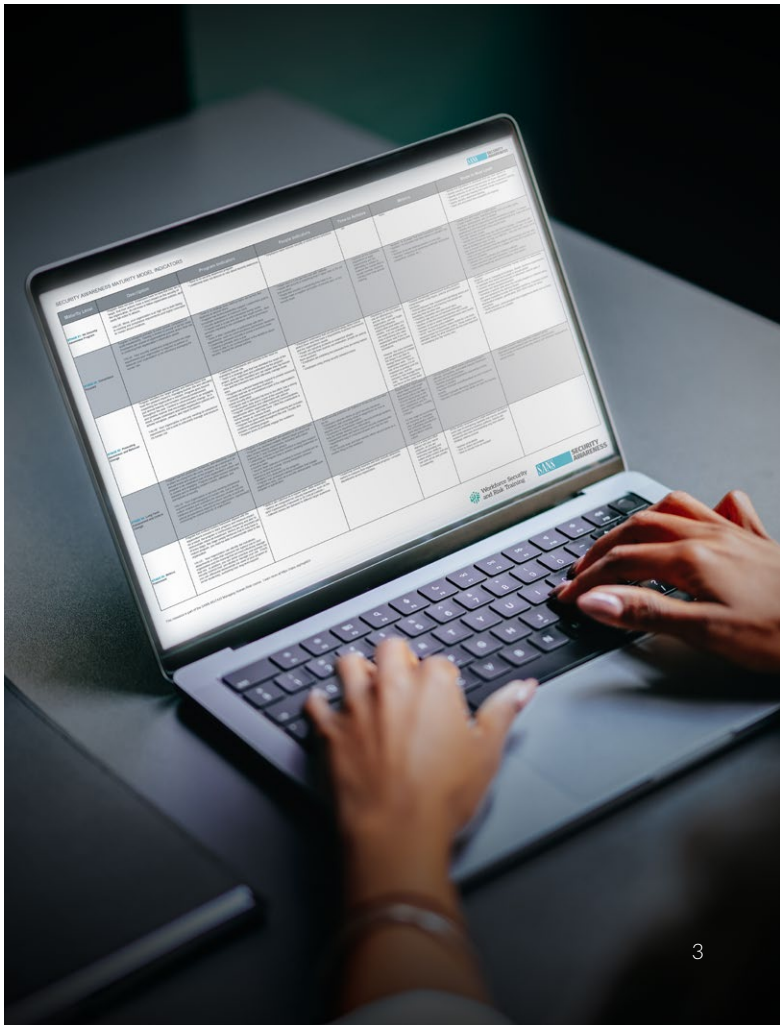
It’s a test worth applying to your own program. When someone on your team believes they may have caused an incident, do they tell you? That’s not just a measure of training effectiveness. It’s a sign of culture change.

Two Kinds of Stuck

Some programs don't know they've plateaued. Reporting rates are up, and the numbers look good, but although behavior has changed, the thinking behind that behavior hasn't yet become embedded in the organization. The program may appear more mature than it is.

Other programs know where they stand but are struggling to push forward. They've made the case for more headcount, executive time, and support, but they're still waiting to see whether that investment comes through.

Both are in Stage 3. Neither is a failure. What determines how long a program remains here is resourcing, and the data shows exactly how much it takes.



Why Stage 3 Takes Longer

Two variables predict program maturity better than anything else in the data: team size and program age.

Programs that successfully changed workforce behavior had at least three dedicated full-time employees, and it took three to five years for that change to become evident across the organization. Programs that progressed to culture change needed a larger team, at least 4.3 full-time equivalents (FTEs), and five to 10 years to mature. The most mature programs in the report typically had more than six dedicated FTEs and had been running for over a decade.

If your team is smaller, that points to a resourcing gap, not a performance problem. It's useful evidence for your next headcount case.

Working with Leadership

Midlevel management, senior leaders, and operations consistently rank among the top blockers. But the data complicates that story. Senior leaders rank among the top three groups for both blockers and supporters: The same group slowing progress is often championing it, too. Operations' hesitation is usually practical, not political. New tools and policies cost time, and that cost affects employees' day-to-day work.

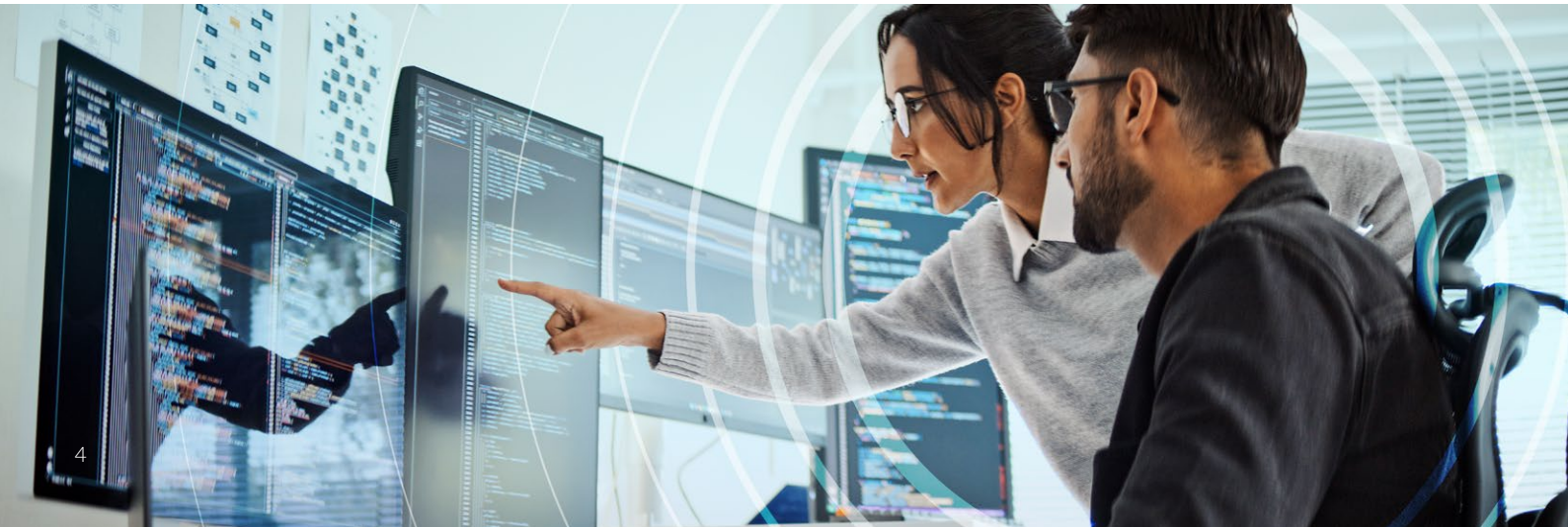
One reason many programs struggle to bring leadership fully on board isn't resistance. It's difficulty demonstrating how security culture supports the business's strategic priorities. The solution is partnership, not persuasion: Build the relationship and make the business case, rather than just asking for buy-in.

This same patience runs throughout the report, not as passive waiting, but as time spent deliberately, building champions and supporters across the business, not just within security. One respondent described what that looks like in practice:

> "Leadership support is a critical piece. Speaking in the language of the business *(for us, it's all about risk, potential reputational damage, and the cost in person-hours for incident triage)* will help gain support for the program."
>
> *- 2026 SANS Security Awareness & Culture Report survey respondent*

Another respondent put the broader mindset simply:

> "Be patient. It's a marathon, not a sprint. Stay educated yourself, lead by example, learn something new every week or month, and be excited to pass that knowledge on."
>
> *- 2026 SANS Security Awareness & Culture Report survey respondent*



How Programs Move Past This Stage

The path varies by team size, industry, and leadership access. But a few practices consistently separate the programs that break through:

- They provide leadership updates on a fixed schedule, not just when something breaks or once a year during budget season.
- They partner with audit, compliance, and governance, risk, and compliance (GRC) teams to explain why a policy exists, not just to deliver the training that explains it. Simpler policies get followed. Complicated ones don't.
- They support all security related communications, including tool rollouts, policy changes, and incident response, instead of focusing only on training-related communications. The workforce hears one consistent message, not five competing ones.
- They make the case for additional staff using industry data, not internal anecdotes.

For global teams, there's an added challenge: Scaling a security awareness program across regions, languages, and local risk cultures takes work. That's a large part of why team growth doesn't scale in a straight line with employee count. A 5,000-person person company operating in a single region and a 5,000-person company spread across four regions do not have the same resourcing needs, even though their headcounts are identical.

AI Is Adding to the Load

AI is now the second-highest human risk concerning security awareness professionals, and it gives Stage 3 programs has another risk to address, often without additional headcount. One respondent described what that risk looks like in practice:

Security awareness teams are also turning to AI themselves: Over 70% have already adopted it, most often for content creation. That's why this year's report devotes an entire section to AI, covering both the risks programs must address on and how small teams can use AI to extend their own capacity when headcount and budgets won't stretch any further.

> "Employees started pasting sensitive material into public AI tools without thinking twice. Customer details, internal documents, draft contracts, sometimes whole chunks of code. Not out of bad intent, just because the tools made their work faster."

- 2026 SANS Security Awareness & Culture Report survey respondent

BEHAVIOR CHANGE IS NOT THE FINISH LINE

It's a Bigger Job Than Training

There's no single right term for this work. Some organizations call it security behavior and culture. Others call it human risk management or simply security awareness. Whatever the label, the job itself is fundamentally evolving. It now involves moving beyond delivering training to managing the specific behaviors that drive human risk and building the relationships needed across the organization to change them.

We are no longer in the training business. We are in the behavior change business. That's a bigger job than most programs are staffed to handle, which is exactly why so many stall here.

> Behavior change was never the finish line. It's a sign that you're on the path to embedding a strong security culture because behavior is what people do, while culture is how people think.

Your Next Step

Knowing where your program sits on the Maturity Model is the best place to start. Even better is having a report that shows you how to grow and mature your program.

The SANS Security Awareness & Culture Maturity Model Assessment is designed to do that. It's free, and it maps your program against this year's data to show you where you stand and what to change next.

TAKE THE FREE ASSESSMENT

Built on eleven years of practitioner data.

This Practitioner Brief draws on the findings from the SANS 2026 Security Awareness & Culture Report, based on responses from over 1,700 security awareness professionals across the globe. The SANS Security Awareness & Culture Maturity Model has been the field's most trusted benchmarking framework since 2011.

LEVERAGE SANS MATURITY MODEL INDICATORS MATRIX

DOWNLOAD THE FULL REPORT

SANS Workforce Security and Risk Training