Security Journey Case Study

When Everyone Became a Developer

How Procore built secure development training for the age of AI, turning a compliance requirement into enterprise-wide AI enablement.

Executive Summary

At Procore, secure code training began the way it does at many companies, as a compliance obligation. The existing program met its SOC2 compliance requirements, but Rebecca Scales, Director of Capability Development, saw an opportunity to move beyond completion toward meaningful learning and behavior change.

A learning scientist and former teacher who cheerfully calls herself a security nerd, Rebecca had already seen what hands-on secure development training could do. She secured the budget, replaced the videos with a full, hands-on OWASP Top 10 program, and built the communications runway to make it stick. Engagement followed, including the signal she trusts most: engineers reaching out, unprompted, to say they had actually learned something.

Then AI changed the definition of "developer." Engineers increasingly started using AI agents, while product managers and designers started building with AI assistants. The line between technical and non-technical blurred, and a compliance requirement written for engineers suddenly applied to people who had never seen a line of code. Working with Security Journey, Procore turned that challenge into an advantage: a role-based model that enables both technical and non-technical staff to use AI quickly, safely, and securely.

THE CUSTOMER

Procore Technologies

A leading global provider of construction management software

CUSTOMER ROLE

Rebecca Scales

Director,
Capability Development

AT A GLANCE

CHALLENGE

Before partnering with Security Journey, Procore's secure code training met its compliance requirements but offered limited hands-on learning.

Then AI turned non-technical staff into "developers" overnight, outpacing the old model.

SOLUTION

A hands-on secure development program that grew into enterprise AI enablement, reaching engineers and the non-technical staff now building with AI, co-built with Security Journey as an embedded content partner.

IMPACT

100% completion in the first cohort, engineers voluntarily reporting they learned something, positive before/after knowledge trends, and a repeatable model for enabling both technical and non-technical staff on AI.

SCALE

Grew from ~800 to ~1,500 engineers over three years, now expanding toward enterprise-wide AI enablement.

The Starting Point: Two Videos and a Checkbox

Rebecca came to Procore already knowing what strong secure development training looked like. Years earlier she had adopted the platform that became Security Journey, and she had brought it into more than one organization along the way. The pattern repeated each time: some initial hesitation about the time it asked of engineers, followed by the same positive reaction once people actually went through it.

> **"After people took it, they were like, wow, that was really good."**

So, when Procore's compliance team asked her about secure code training, she already had a benchmark in mind. What she found did not meet it. The security team had published two videos that satisfied the audit requirement but didn't foster engagement or long-term learning.

> **"There was no engagement. It was literally two videos that became the checkbox for our requirements."**

Because she had seen the alternative work firsthand, Rebecca did not need a committee or a long evaluation to know what to do. She secured the budget, made the case to leadership, and moved.

Reframing the Problem: Learning Over Training

Rebecca's core conviction is that completion is not the goal. Behavior change is.

> **"Learning is what matters."**

That reframing made the tradeoff explicit. Hands-on training is more impactful than clicking through videos, and to Rebecca, that was exactly the point.

> **"This training is going to take people longer to go through. The question is: do you care that they actually learn it? If they learn it, you will see results in your systems. You will see fewer vulnerabilities being created."**

Building the Program: Comms First, Then Hands-On

Procore rolled out the full OWASP Top 10 as hands-on exercises. It was non-negotiable, but never a surprise, because Rebecca treated communication as part of the product.

> **"We barraged people with comms before we started."**

Managers were notified weeks ahead so training could go onto sprint backlogs. Wiki pages answered "why are we doing this?" before the first module launched, and early testimonials primed the rollout.

The technical lift was light: Single Sign-On and a reporting API feeding a custom completion dashboard. The first cohort was live in under a month.

Just as important as the rollout was what happened when something needed attention. Rebecca and her team reach the Security Journey Support Team through a shared channel, and they rarely wait long.

> **"As soon as we have a problem, they're on it. We're talking a matter of minutes."**
>
> – **Rebecca Scales,** Director, Capability Development

What Changed: Engagement You Can Feel

The first round reached 100% completion across early adopters and new hires. But the metric Rebecca trusts most isn't on a dashboard.

> **"When an engineer takes a moment to step away and write a Slack message to me or someone on my team about this training, that means it was impactful."**

Engineers who had never engaged with security training were telling her, unprompted, that they had learned something. That almost never happens with videos or SCORM modules. Recognition even came from leadership: a VP who recognized the same hands-on program from a previous company told her that adopting it was fantastic.

> **"People remember this training. It matters because their hands are on it."**

Before-and-after knowledge checks trended positive across cohorts. There was participation and genuine learning.

The AI Inflection: When Everyone Became a Developer

Then the ground shifted. AI began to collapse the very distinction the program had been built around. Engineers moved from writing code by hand to directing agents, and non-technical employees started building and shipping software with AI assistants. Product managers and designers who had never opened a repository were suddenly doing the work of developers. The scale of the shift was hard to overstate.

As part of Procore's SOC 2 compliance program, developers complete secure code training, making the implications of this shift immediate. The definition of a developer had quietly expanded to include people who had never written a line of code, and the technical framing that worked for engineers did not fit them.

> **“The top 10 vulnerabilities are technical. How do I explain SQL injection to someone who has never seen SQL?”**

Rebecca had already read where this was heading.

> **“Agentic coding is very 2025. Agentic SDLC is today.”**

Her mandate for the year came as a single directive from Procore’s president: be at advanced stages of AI usage by mid-2026. It is a sharp version of a problem Security Journey now hears from organizations everywhere. Companies have handed people powerful AI tools but not the skills to use them well and securely, and access has raced ahead of capability. That gap, between adopting AI and actual capability, is where wasted spend, uneven adoption, and new risk collect.

Closing that gap was exactly what Rebecca had been building toward. In 2025 alone, her team ran AI enablement that drew roughly 6,700 session attendances across the company. The answer was not more OWASP. It was a role-based model that meets engineers, product managers, and designers where they are, so the whole organization can move quickly and safely without the business slowing down.

Governance for a New Kind of Developer

As AI assistants put more people close to real code, Procore saw early what many organizations are only starting to confront: the long-held assumption that only engineers touch production no longer holds. When product managers and designers can prototype directly against engineering repositories, access has to be rethought on purpose.

As AI assistants put more people closer to real code, Procore recognized that access, governance, and training had to evolve together. The company responded by deliberately matching access and preparation: employees with higher levels of repository access complete technical secure development training, while non-technical employees receive training designed for the ways they interact with AI-assisted development. As access expanded, leadership backed accelerating the rollout so enablement could keep pace.

An AI Enablement Partner, Not Just a Platform

A lean enablement team had to help an entire workforce, engineers and non-engineers alike, use AI quickly, safely, and well, and keep pace as the tools changed week to week. That is an AI enablement problem, and it is not one a catalog solves on its own. What Rebecca wanted was a partner who could help her read a landscape moving faster than any single team could track.

> **“We look to you all as a partner to help us understand that landscape.”**

As Procore prepared to roll AI tools out to thousands of employees, Michael Burch, Security Journey's VP of AI Enablement and Transformation, took Rebecca's feedback and worked with the Security Journey content team to produce video walkthroughs and hands-on lessons for non-developers. They teach people to build a real application with an AI assistant and share it on GitHub, with security woven into the practical moments: why a repository should default to private, how to use tokens safely, and how version control lets you roll back when an agent does something you did not intend. New lessons shipped in days rather than months. This was enablement content Rebecca's small team would otherwise have had to build from scratch and maintain.

That value does not depend on which AI platform Procore ultimately standardizes on. Even while the company weighed competing enterprise AI assistants against each other, Rebecca saw the training as the constant beneath the tooling decision, the thing that stays relevant no matter which vendor wins.

> **"I think your content is going to be incredibly relevant to a lot of people… this content is going to be really critical with any kind of rollout of any larger enterprise agentic tooling."**

The relationship settled into a genuine working partnership: a shared channel, feedback that shaped the product roadmap, and a two-week rhythm of review and iteration. What that adds up to for a lean enablement team is the thing an enablement leader needs most.

> **"This is really proving to be much more of a partnership than I thought it was going to be… that means I don't have to create the content."**

For an enablement leader moving at the speed of AI, that is the difference between a platform you operationalize alone and a partner helping you get an entire workforce productive and safe.

> **"I see you as a very strategic partner in all of this, no matter what our initiatives are."**

Looking Ahead

Procore's roadmap now runs straight into the agentic SDLC, and Security Journey is building toward it, including early work on governance for AI-assisted and "vibe" coding, where security scanning and guardrail rules can travel with the developer even outside a traditional repository. The underlying philosophy hasn't changed: enablement means meeting people where they are, across the full spectrum of skill levels, and making security a practical instinct rather than a checkbox.

Advice to Other Organizations

Rebecca's guidance is direct and grounded in having done this more than once.

> **"Get that leadership buy-in at the very beginning… and have a comms plan for how you're getting it out."**

Put the training on people's backlogs so it is planned, not sprung on them. And hold the line on the time-versus-learning tradeoff, because a program that takes longer but changes behavior beats a faster one that changes nothing.

Key Takeaways

- Compliance is the floor, not the goal. Behavior change is what actually protects the codebase.
- AI has erased the line between technical and non-technical staff; secure development training has to cover both.
- Hands-on beats video-and-quiz. People remember training their hands are on.
- A communications runway is as important as the content itself.
- The strongest early signal is not a report. It is learners telling you, unprompted, that they learned something.

> **"If you care about behavior changing, that's where you need Security Journey. No other product we've seen makes that outcome the central focus."**