Most insider risk isn’t malicious. It’s still a breach. Fable can help.

73%
of insider incidents are non-malicious: negligence or stolen credentials, not intent*

$19.5M
average annual cost of insider risk per organization*

80%
reduction in reported risky behaviors by Fable customers**

THE CHALLENGE

Your insider program is built for the rare case

Most insider risk programs are built to catch the malicious few: the disgruntled leaver, the recruited asset, the deliberate thief. Those cases are real. But the majority of insider incidents come from people who never meant to cause harm.

Someone forwards a sensitive file to a personal account to finish work over the weekend. Someone misconfigures a file share. Someone gets socially engineered and hands over credentials. There is no intent, and there is still a breach: still reportable, still subject to disclosure law, still a headline. Disclosure law does not grant forgiveness for good intentions.

A program that only hunts for malice misses most of its risk. A program that only runs annual awareness training changes none of the risky behavior behind it. Insider risk runs the full spectrum, from honest mistake to deliberate act, and a comprehensive program has to address all of it.

CUSTOMER QUOTE

> *“I really, truly think this is going to make a difference. If we stop one person from doing something that results in a financial loss, it was worth the investment.”*
>
> **CISO, major insurance distributor**

THE FABLE APPROACH

Coach the many. Surface the few. Cover the whole spectrum.

Coach the non-malicious majority

Most insider risk is behavior, not intent. Fable turns your data-handling and acceptable-use policies into short, role-specific briefings in Slack, Teams, or email, delivered the moment it detects the behavior drift: the risky forward, the oversharing, the unsanctioned upload. The safe path becomes the easy path, and you get the attestation trail to prove it.

Surface the malicious insider

The signals that expose a malicious insider are already in your stack: mail rules, identity events, data movement, access anomalies. Fable’s human risk engine aggregates them, scores people and cohorts, and surfaces the behavior existing controls miss, early enough to investigate through a defined, rights-respecting process.

One program, end to end

Error, negligence, manipulation, malice: one person sits at the center of every insider vector. Fable runs a continuous loop across all of it, coaching honest mistakes, hardening high-risk roles, and escalating confirmed cases into HR and Legal. One program instead of a tool per problem.

*Ponemon Institute & DTEX, 2026 Cost of Insider Risks Global Report: negligent and credential-theft incidents as a share of the total, and the $19.5M average annualized cost per organization.
**Based on Fable customer case study, available upon request.

THE SHIFT

The malicious insider is rare. The risky moment is constant.

Every forward, every upload, every external share, every login. You cannot investigate your way out of that, and you cannot train your way out of it on an annual cadence. Fable runs continuously, triggered by what employees actually do and grounded in your policies and your own telemetry, so honest mistakes get coached before they become incidents and the genuine threats stand out from the noise.

THE DISCOVERY · REAL CUSTOMER, ANONYMIZED

We surfaced a malicious insider that existing controls had missed.

At a global media company, Fable's human risk engine flagged metadata from an email auto-forward rule that had slipped past the customer's IT and email controls. That signal was enough for their security team to open an insider investigation into a real data-exfiltration event, one that would otherwise have kept running unseen.

The takeaway — the signal was already in their stack. Fable made it legible in time to act.

THE INSIDER SPECTRUM

What Fable identifies, and does, across the intent spectrum

MALICIOUS INSIDER

Deliberate theft or sabotage by a trusted insider, the case above.

Fable → Surfaced early from mail, identity, and data-movement signal, then investigated through a rights-respecting process.

NEGLIGENT INSIDER

Honest mistakes and policy drift: the risky forward, the oversharing, the unsanctioned upload.

Fable → Coached in the moment, with an attestation trail. Risky data movement drops, and no one gets blocked.

OUTSMARTED INSIDER

Compromised credentials and MFA fatigue that turn an employee into an entry point.

Fable → Targeted coaching for the cohorts under attack, plus early signal on the account takeover.

This is non-malicious insider risk, reduced by changing behavior instead of blocking it: at Pennymac, in-the-moment coaching cut sensitive-data exposure incidents by 60%, with no policy lockdowns.

CUSTOMER QUOTE

> *"We chose Fable because its personalized approach led to more effective and faster employee behavior change."*
>
> **Cyrus Tibbs** — former CISO, Pennymac

CALL TO ACTION

Ready to see Fable in action?

Request a demo to see how Fable surfaces insider risk across the full intent spectrum, and coaches the behavior behind it.

fablesecurity.com · hello@fablesecurity.com