Brought to you by:

Fable

Modern Human Risk Management

for dummies

A Wiley Brand

Understand human risk

Shape employee behavior

Measure behavior change

Fable Security Special Edition

Nicole Jiang
Dr. Sanny Liao

About Fable Security

Fable Security delivers the human risk platform that directly shapes employee behavior. Designed for simplicity and enterprise scale, our agentic platform synthesizes complex employee data, pinpoints risky behaviors, and deploys highly-relevant interventions to people automatically, in real time, right where they work. With Fable, modern enterprises tangibly reduce risk, sharpen security habits, and drive lasting organizational resilience. Check us out at fablesecurity.com and on the socials @fablesecurity.

Modern Human Risk Management

Fable Security Special Edition

by Nicole Jiang and Dr. Sanny Liao

for dummies®
A Wiley Brand

Modern Human Risk Management For Dummies®, Fable Security Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774

ISBN 978-1-394-41950-0 (pbk); ISBN 978-1-394-41951-7 (ebk);
ISBN 978-1-394-41952-4 (ebk)

Publisher's Acknowledgments

Development Editor: Lawrence Miller
Project Editor: Jen Bingham
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Molly Daugherty
Content Refinement Specialist: Bharaneedharan Murthy

Table of Contents

Introduction

Despite spending billions on cybersecurity, organizations remain more vulnerable than ever to evolving cyberthreats. Human error is the common denominator in most breaches today — whether it's misconfigured systems, mishandled data, compromised credentials, or susceptibility to social engineering.

As threat actors increasingly weaponize artificial intelligence (AI) to automate and scale attacks, legacy defense strategies are falling short. Security teams must shift from reactive controls to proactive, adaptive strategies that account for the human element and the accelerating pace of AI-driven exploitation.

About This Book

This book consists of five chapters that explore the following:

- Why human error is the main source of security breaches and how modern risk management helps (Chapter 1)
- Five key requirements for a modern human risk management solution (Chapter 2)
- How to assess your organization's human risk maturity, build a roadmap, and foster a secure culture (Chapter 3)
- How Fable can help your organization (Chapter 4)
- Ten key metrics for human risk management (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest feel free to jump ahead to that chapter. You can read this book in any order that suits you.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but this book assumes a few things nonetheless!

Mainly, it assumes that you're a security leader such as a chief information security officer (CISO); governance, risk and compliance (GRC) executive; security operations (SecOps) leader, or head of security and awareness training. As such, you're probably somewhat technical, have a strong understanding of modern security threats, and are looking for a more innovative approach to security awareness and training that actually reduces human risk.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describes you, keep reading anyway! It's a great book and after reading it, you won't be at risk of not knowing the basics (and beyond) of human risk management.

Icons Used in This Book

Throughout this book, you will find special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information that you should commit to memory — so it doesn't fall victim to Ebbinghaus' forgetting curve.

TIP

Tips are appreciated but never expected — hopefully you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice.

Beyond the Book

There's only so much that can be covered in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://fablesecurity.com`.

IN THIS CHAPTER

- Looking at the human element
- Tackling the problem with human risk management

Chapter 1
Recognizing the Problem

This chapter explores the human element in cybersecurity. From insider threats and phishing attacks to everyday missteps, human behavior remains a leading cause of costly breaches. This chapter goes over how these risks manifest, and how modern human risk management platforms are reshaping the way organizations detect, mitigate, and ultimately reduce human errors.

Why Human Error Is the Number One Source of Security Breaches

Cybercriminals follow the money — and the human layer is their most lucrative target. According to the Verizon *2025 Data Breach Investigations Report* (DBIR), human error is involved in more than 6 out of every 10 breaches and the IBM *2025 Cost of a Data Breach Report* found that insider threats, phishing, and stolen or compromised credentials are among the most frequently used and most effective employed by threat actors.

How everyday mistakes open doors to attackers

Common, routine, or otherwise dull tasks are a breeding ground for human errors — a hasty click, a recycled password, a missed software update on a personal device. Yet, most human risk management programs remain outdated and ineffective. They lean heavily on one-size-fits-all training modules and uninspired awareness campaigns that fail to resonate. The uncomfortable truth — well-known to both security teams and employees — is that despite companies spending resources on training sessions and phishing simulations, these broad-stroke efforts rarely change behavior. In fact, a recent study found that half of users exit security awareness training within the first ten seconds, and fewer than one in four users complete assigned training materials.

What's different about today's AI-driven threats

The threat landscape has shifted into an AI-driven arms race, with adversaries using automation to accelerate, refine, and personalize their attacks. In response, defenders are deploying AI as well — but enterprise defenses still concentrate overwhelmingly on infrastructure and endpoints, leaving the human layer exposed. Attackers are capitalizing on this, and with alarming success. Studies consistently show that human behavior is the leading cause of security incidents, contributing to most breaches.

WARNING

The rise of AI-driven deception is accelerating. The Verizon 2025 DBIR confirms that human-centric threats are intensifying daily, and multiple studies show social engineering attacks have risen several thousand percent since ChatGPT was launched.

What's Needed: Modern Human Risk Management

Human risk management is a targeted discipline focused on identifying, quantifying, and mitigating cybersecurity threats driven by human behavior — from phishing susceptibility and data mishandling to the circumvention of security controls.

Modern human risk management shifts the focus from checkbox compliance to measurable behavior change. Its importance has surged as remote work, AI-enabled social engineering, and evolving regulatory requirements have transformed the human element into cybersecurity's most dynamic and vulnerable attack surface.

Modern human risk management platforms must start where the risk is greatest: social engineering and phishing. Effective human risk management doesn't just raise awareness, it also drives measurable behavior change by bridging threat detection across real-world and simulated environments. When users can recognize and report phishing attempts in both contexts, organizations gain human threat intelligence that can be integrated into the broader security stack — enabling earlier intervention and containment.

Yet the potential of human risk management extends far beyond phishing. A risk-based approach can be applied across everyday behaviors that shape an organization's security posture, including:

- Data handling and sharing
- Generative artificial intelligence (GenAI)
- Authentication and access controls
- Security updates and vulnerability patches

By synthesizing behavior signals, human risk management platforms can trigger targeted interventions to shape good security habits. Security teams can deliver dynamic briefings and nudges in response to heightened risk, reinforcing secure behavior in the moment — when it matters most.

REMEMBER

Security awareness training is designed to inform, often fulfilling a compliance checkbox by educating users about common cyberthreats. It's static, broad, and typically measured by completion rates rather than real-world impact. Human risk management, by contrast, is built to transform behavior. It focuses on quantifying and actively reducing human cyberrisk through adaptive interventions and behavioral analytics. Rather than stopping at awareness, human risk management embeds secure behavior into daily workflows, making security a lived, measurable part of organizational culture.

By adopting human risk management, security leaders can elevate their organization's resilience while translating strategic efforts into business value. Human risk management enables real-time risk reduction, empowers teams to demonstrate measurable impact, and ensures alignment with rapidly evolving compliance requirements, turning human behavior from a liability into a defensible asset.

IN THIS CHAPTER

- Quantifying and acting on human risk
- Delivering targeted, relevant interventions
- Reinforcing desired behaviors with in-the-moment training
- Beginning with the end in mind — an outcomes-based approach
- Deploying a human risk management platform at scale

Chapter 2
Defining the Five Must-Haves of Modern Human Risk Management

As organizations work to bolster their security posture, they can't afford to ignore the human layer. Mitigating human risk is no longer a nice-to-have; it's a strategic imperative that impacts the operational resilience, regulatory compliance, and bottom line of every business. This chapter outlines five essential capabilities of human risk management programs — ones that shape behavior directly and drive real outcomes.

Data-Driven Decision-Making

Many human risk management solutions fail to align with the behavioral vulnerabilities they aim to mitigate. As a result, organizations routinely miss critical opportunities — such as alerting finance teams to an emerging vishing campaign — despite having

the necessary data at their fingertips. This disconnect is particularly disturbing given the wealth of telemetry available across the enterprise: breach alerts, vulnerability disclosures, access logs, behavioral analytics, and more. With modern data lakes and visualization platforms, the technical barriers to integration and analysis have never been lower.

REMEMBER

Vishing — short for "voice phishing" — is a type of social engineering attack where cybercriminals use phone calls or voice messages to trick victims into revealing sensitive information, such as login credentials or financial details, or taking action, such as initiating a payment.

What's needed is a cohesive, data-driven framework for quantifying and acting on human risk. Such a program should ingest signals from across the digital workplace — human resources (HR) systems, identity and access management (IAM) platforms, communication tools, cloud and endpoint security solutions — and continuously refine its assessments based on both real-time inputs and feedback loops measuring intervention effectiveness. The goal isn't just data aggregation, but intelligent synthesis: building a model that can parse, weight, and correlate diverse signals into a dynamic, actionable risk score. From there, security teams should be empowered to segment risk by cohort, investigate contributing factors, and tailor mitigations with precision.

TIP

A dynamic risk score is essential in modern human risk management because it enables organizations to respond to threats with precision, agility, and context. Here's why it matters:

- **Real-time visibility into human risk.** Static assessments quickly become outdated. A dynamic score continuously ingests signals — like access anomalies, behavioral shifts, or policy violations — giving security teams a live view of who poses elevated risk and why.
- **Contextual decision-making.** Not all risky behaviors are equal. A dynamic model can weigh factors like role sensitivity, access privileges, and historical behavior to differentiate between a misstep by a junior analyst and a pattern of negligence by a privileged user.
- **Targeted interventions.** With granular, up-to-date scores, organizations can tailor responses — such as just-in-time training, access restrictions, or direct outreach — based

on the severity and nature of the risk, rather than blanket policies.

- **Feedback-driven improvement.** Dynamic scoring allows for feedback loops. If an intervention reduces risky behavior, the score adjusts — helping refine what works and where to focus next.
- **Strategic resource allocation.** Security teams can prioritize high-risk cohorts or individuals, optimizing limited resources and avoiding alert fatigue. This supports proactive risk reduction rather than reactive damage control.

Highly Targeted Approach

Most human risk management solutions remain blunt instruments, relying on generic training and infrequent, one-size-fits-all simulations. Although these may check compliance boxes, they rarely move the needle on actual risk reduction. Consider a finance team member whose device lacks a critical security patch: broad phishing awareness or hygiene training does little to address that specific exposure.

Even platforms boasting extensive module libraries often suffer from poor discoverability, stale or irrelevant content, and sluggish update cycles, rendering them ineffective against emerging threats or policy changes.

WARNING

Beyond being scattershot, most traditional solutions fail to stick. They're rarely personalized, seldom risk-specific, and almost never tied to observable behaviors. As a result, they're easy to ignore and difficult to apply when it matters most.

What's needed is a highly targeted approach to human risk mitigation. Programs must deliver timely, relevant interventions — tailored in both format and substance to the risk at hand. AI enables this shift by detecting behavioral signals, selecting the appropriate response, and scaling it through intelligent customization. For example, the finance employee with the missing patch should receive an immediate, automated prompt to remediate — no waiting, no guesswork.

Just-in-Time Interventions

Traditional human risk management programs rely on generic, scheduled training — typically annual sessions supplemented by occasional reminders or phishing simulations. Although these may satisfy compliance mandates, they rarely address the specific risks individuals face in their roles, and they almost never intervene when it counts: in the moment. Consider a developer who inadvertently logs personally identifiable information (PII) to an observability tool or an employee who uploads confidential financial data to a generative artificial intelligence (GenAI) chatbot. Without guardrails to show them what went wrong in the moment, the behavior will continue — and eventually may lead to real exposure.

REMEMBER

The timing gap matters. Ebbinghaus's forgetting curve (first described in 1885) and decades of cognitive research since show that retention falls steeply in the hours and days after learning (see Figure 2-1). Training that isn't reinforced in the moment rarely changes behavior. For security, that means brief, just-in-time reinforcement — not postponed slide decks — is essential to lock in safe practices; without it, even well-intentioned employees may lapse, leaving systems and data exposed.

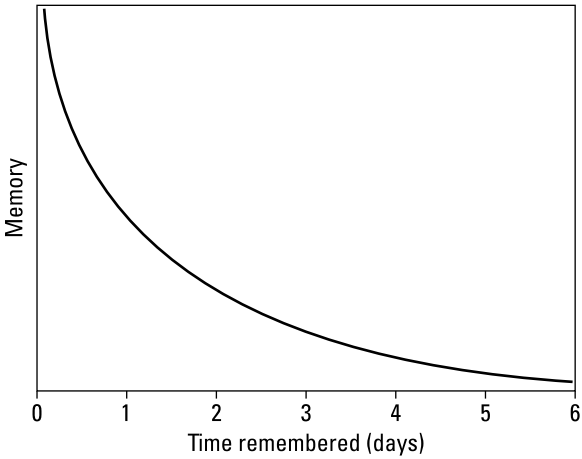


FIGURE 2-1: A representation of Ebbinghaus' forgetting curve.

What's needed is a responsive, risk-aware program that delivers targeted interventions in real time. These nudges should be triggered by actual behaviors, tailored with business context and policy, and delivered directly within the tools and workflows people use. This shift — from static education to dynamic, in-the-flow correction — is essential for reducing human risk at scale.

Outcomes-Focused

Human risk management has long struggled to demonstrate measurable security outcomes or a clear return on investment (ROI). These programs are traditionally measured by their completion rates and phishing clicks rather than true behavior change. For many security teams, compliance remains the primary justification for investing in awareness campaigns and phishing simulations. Rarely are these efforts backed by security ROI — and in some cases, research suggests they may inadvertently increase risk by fostering complacency or fatigue.

What's needed is a behavior-centric model that drives real change. Effective programs must deliver targeted interventions — timely, contextual, and aligned to the behaviors that contribute to risk. Just as important, they must quantify impact: tracking reductions in social engineering susceptibility, data exposure, patch latency, and misuse of GenAI applications. A robust feedback loop should continuously refine the approach, ensuring interventions remain relevant, adaptive, and demonstrably effective.

Enterprise-Grade

Many human risk management tools remain isolated point solutions — fragmented modules buried in learning management systems, disconnected from the broader enterprise ecosystem. They falter under the operational complexity of large organizations: diverse user roles, layered regulatory requirements, global footprints, and the need for centralized oversight. Picture a multinational enterprise attempting to launch a security awareness campaign, only to discover the platform lacks localization, role-based access, or scalable administration. Those who've managed legacy systems know the pain — manual setup, brittle workflows,

and outdated content that lags evolving threats simply because the team couldn't keep pace.

In environments where simplicity, scale, and security are non-negotiable, these limitations aren't just inconvenient — they're operational blockers. They stall adoption, dilute impact, and leave organizations exposed.

What's needed is an enterprise-grade solution built for integration, automation, and global execution. That means seamless interoperability with existing systems via robust APIs. It means intuitive administration backed by granular controls — role-based permissions, audit trails, and centralized configuration. And it means operational readiness: localization for distributed teams, brand alignment for internal engagement, and the kind of reporting, compliance posture, and support experience security leaders expect from any core platform.

IN THIS CHAPTER

- Assessing your organization's human risk maturity level
- Getting started
- Achieving tangible benefits
- Building a secure culture

Chapter 3
Putting It All Together

This chapter introduces a human risk maturity model to help you assess your organization's current level of risk, provide best practice tips for creating your human risk management adoption roadmap, explore the business benefits of human risk management, and explain how you can build an employee-friendly culture of security and awareness.

Adopting a Human Risk Maturity Model

How do you know where to begin with the five must-haves of modern human risk management (discussed in Chapter 2)? Use the maturity framework in Table 3-1 to quickly assess where your organization stands today and to chart your path forward.

TABLE 3-1 The Fable Human Risk Maturity Model

	Low	Medium	High
Data-driven	Not data-driven	Some data used to target interventions	Signals from across your tech stack used to target interventions
Highly targeted	Generic training and one-size-fits-all phishing simulations	Role-based interventions	Targeted interventions based on risk
Just-in-time	Periodic delivery	Delivery in response to role	Delivery based on risky behavior
Outcomes-focused	Compliance checkboxes	Some risk reduction	Behavior change
Enterprise-grade	Standalone training modules	Enterprise integration, ease of admin, and basic reporting	Robust enterprise integration, security built-in, automated campaign creation and deployment, and audit-ready reporting

Building Your Roadmap

Once you have assessed the human risk maturity level for your organization, you have a starting point.

Begin where the stakes are highest: social engineering and phishing. These human-driven risks are among the most costly and pervasive causes of data breaches — encompassing everything from spear phishing, business email compromise (BEC), and ransomware to credential harvesting, adversary-in-the-middle (AitM) attacks, smishing, vishing, and more.

Make employees aware of how their behavior can make them a target or put their company at risk. This includes helping them recognize how everyday actions, such as oversharing online, using weak passwords, or ignoring security updates can create openings for attackers. Training should highlight real-world examples of how small mistakes can lead to significant breaches, reinforcing the importance of vigilance.

By understanding the tactics that adversaries use to exploit human behavior, employees become more capable of identifying suspicious activity. Ultimately, empowering staff with this awareness strengthens the organization's overall security posture. Your human risk program should be grounded in behavioral science, cybersecurity best practices, and simply meeting people where they are. It should include the following:

- **Adaptive learning:** Dynamically adjust content and difficulty to match user role and context
- **Behavioral focus:** Prioritize behaviors that matter, with an eye toward building good security habits
- **Customization:** Tailor interventions to individual roles, risk profiles, and learning styles
- **Gamification:** Use behavioral design to drive engagement and retention
- **Metrics:** Track the behaviors that actually reduce risk
- **Motivation:** Empower users to protect themselves and their teams

Realizing the Payoff

Human risk management reframes the human element from being a vulnerability into being a defense layer. By systematically identifying, measuring, and mitigating risky behaviors, human risk management delivers tangible benefits across operational, financial, and strategic dimensions:

- **Resilience at scale**
  - *Behavioral hardening across the workforce:* Human risk management equips every employee — not just technical staff — with the skills to recognize and respond to threats like social engineering and data mishandling.
  - *Adaptive interventions:* Platforms use behavioral signals to deliver personalized briefings, nudges, or automated mitigations, ensuring that risk reduction scales with organizational growth.

- *Threat intelligence amplification:* Incorporating threat telemetry into human-risk briefings arms employees with timely intelligence about relevant scams, cybercrime activity, and emerging attack patterns.

» Incident reduction

- *Targeted risk mitigation:* Human risk management focuses on high-impact behaviors — for example, threat reporting, secure data handling, and multifactor authentication (MFA) adoption — that directly correlate with breach prevention.
- *Faster detection and containment:* By integrating human threat intelligence into security operations center (SOC) workflows, security teams can identify and neutralize threats earlier — often before they escalate.
- *Reduced exposure windows:* Timely alerts and automated responses shrink the time between risky behavior and remediation.

» Cost efficiency

- *Lower breach-related costs:* By preventing incidents tied to human error — a leading cause of costly data breaches — human risk management helps avoid legal, reputational, and operational consequences.
- *Optimized training spend:* Unlike traditional awareness programs, human risk management focuses on measurable outcomes, ensuring that investments yield real behavioral change.
- *Compliance without waste:* Human risk management aligns with evolving regulatory requirements by demonstrating proactive, data-driven human risk reduction — minimizing fines and audit friction.

REMEMBER

In short, human risk management transforms cybersecurity from reactive education to proactive defense — enabling organizations to build resilience, reduce incidents, and contain costs through smarter, behavior-driven security.

Fostering an Employee-Friendly Security Culture (Yes, It's Possible!)

In today's threat landscape, building a resilient cybersecurity posture requires more than technical controls — it demands a culture where employees feel empowered, not policed. Human risk management offers a transformative approach by aligning security with human behavior, fostering a workplace culture that is both employee-friendly and secure.

Traditional security awareness programs often rely on rigid training modules and punitive simulations that alienate employees. Modern human risk management flips this model by focusing on behavioral insights, adaptive learning, and positive reinforcement. Instead of treating users as liabilities, it positions them as active participants in the organization's defense strategy.

Modern human risk management platforms use personalization and mass-customization to engage users meaningfully and give them precisely what they need to know — in the shortest amount of time. Training is tailored to individual roles, system access, risk profiles, and other business context, making it relevant and as nonintrusive as possible. It should be enriched with policy and process so the user knows precisely what action to take, and it should reward them for taking the correct actions, such as with gamification badges or other recognition.

REMEMBER

Modern human risk management supports psychological safety. Employees are more likely to report mistakes or suspicious behavior when they know they won't be penalized. And when they do make a mistake, such as failing a phishing simulation, training should take a nonjudgmental, collaborative approach to providing the employee with information and best practices — without punishing them. This transparency accelerates incident response and builds trust between security teams and the broader workforce.

By integrating human risk management into daily operations, organizations move beyond compliance to cultivate a proactive, security-aware culture — one where employees are equipped, engaged, and accountable. The result is reduced incidents, lower breach-related costs, and a workforce that sees cybersecurity not as a burden, but as a shared mission.

IN THIS CHAPTER

- Exploring the Fable human risk management platform
- Tackling the must-have requirements of modern human risk management

Chapter 4
Discovering How Fable Can Help

This chapter introduces you to the Fable human risk management platform and explains how Fable meets the five key requirements of a modern human risk management platform (discussed in Chapter 2).

Exploring the Fable Platform

Fable shapes employee behavior in three simple steps:

- **Pinpoint risk**
  - Understand employee risk
  - Prioritize by severity and impact
  - See recommended interventions
- **Deploy highly targeted interventions**
  - Take advantage of over 50 agentic workflows
  - Autogenerate targeted interventions using artificial intelligence (AI)
  - Deploy briefings, nudges, chats, and workflows

- **Measure change**
  - Track behavioral shifts over time
  - Quantify the organization's risk reduction
  - Validate intervention effectiveness with clear metrics

TIP

Book a demo at `fablesecurity.com/book-demo` to learn more about the Fable human risk management platform.

Addressing the Five Must-Haves of Modern Human Risk Management

Modern human risk management requires more than check-the-box training and simulations. To keep up with increasingly sophisticated, AI-driven threats and drive real change across their employee bases, organizations need solutions that are data-driven, highly targeted, just-in-time, outcomes-focused, and enterprise-grade. By embracing these five must-haves (discussed in Chapter 2), security teams can move beyond compliance toward actual risk reduction — addressing the right behaviors at the right moments with the right interventions to change behavior and drive security resilience across the organization.

REMEMBER

Fable helps customers address the five must-haves of modern human risk management in the following ways:

- **Data-driven:** Modern security demands real-time visibility into human behavior. A data-driven platform should use security signals from your technology stack to drive decision-making and target behaviors. Look for platforms that create a centralized behavior data lake, model employee risk dynamically, and enable both deep analysis and plain-language queries. Data is the fuel that powers everything else.

  With its human behavior index, Fable synthesizes employee behavior signals from systems across the enterprise — identity and access, human resource, workspace, and security systems — identifying where gaps in human behavior introduce risk into the business.

  From there, the Fable Risk Engine layers in business and employee context to generate a comprehensive risk score, and breaks it down among factors that comprise that score.

Security professionals can drill in to understand risk at the individual, cohort, business unit, or organization level, as well as deploy AI interventions — such as personalized video briefings — in a data-driven way.

- **Highly targeted:** One-size-fits-all training and phishing simulations don't move the needle on behavior. Today's solutions must deliver personalized, one-to-one interventions that are directly tied to an individual's risk profile — based on their role, access, behaviors, and threat level. From AI-generated video briefings to nudges to modern "ishing" simulations, interventions should be tailored, relevant, and precise. Targeted means fewer alerts, greater engagement, and higher efficacy.

  Fable features highly targeted agentic interventions that address specific risks. Security professionals can automatically deploy AI-generated video briefings, small nudges, or two-way chats, delivered one-to-one to employees. Each intervention is personalized with names, details about the employee's role, system access, and behavior, as well as customized with organizational nuances and concrete calls to action. Most importantly, Fable makes it simple to do this in just a few clicks through a clear, streamlined user interface.

- **Just-in-time:** The best time to intervene is the moment of risk. Just-in-time capabilities allow security teams to respond immediately — when someone reuses a password, downloads sensitive data, or falls for a suspicious message. These are teachable moments, and the platform should meet people where they are — figuratively and literally in the channels where they work. This is how security becomes embedded in culture — not just compliance.

  Fable delivers targeted interventions to people based on their risky behavior, right to their email or chat app like Slack, Microsoft Teams, or Google Chat. By targeting specific risks in the moment, Fable gets people's attention and prompts meaningful behavior change when it matters most — and delivers a sticky message that lasts. Beyond delivering interventions in real time, Fable makes it easy for administrators to automate follow-up timing, frequency, and channel.

- **Outcomes-focused:** Security teams are under pressure to show results, not just activity. That's why your platform should measure and improve performance continuously — tracking reduction in risky behaviors, campaign effectiveness, and employee feedback. A modern solution doesn't

just check boxes; it delivers meaningful, measurable behavior change.

With a laser focus on shaping behavior directly, Fable embodies outcomes-focused human risk management. Fable customers describe measurable improvements in security behavior, from decreasing phishing clicks by 86 percent to reducing personally identifiable information (PII) exposure by 60 percent, to shrinking time-to-behavior change from weeks to hours.

- **Enterprise-grade:** Human risk management solutions must be built for scale, security, and ease of administration. Enterprise-grade means easy integrations with your tech stack, robust automation, flexible content customization, multilingual support, role-based access, and strong data protection. It should be simple for security teams to administer, and invisible to employees — except when it matters most.

  Fable was built for the enterprise from day one. The platform is simple to administer, globally scalable, and secure by design. Security teams can configure global settings, assign permissions with fine-grained, role-based access, and maintain audit readiness with robust logging and reporting. Perhaps most important, Fable supports automated campaign creation starting with a library of templates for minute-long briefings, crisp written nudges, compliance training modules, and phishing simulations. You can mass-personalize campaigns to include employees' name, role, access, and behavior, as well as customize them with your company's branding, policies, processes, and business context. You can even localize them for your employees around the globe. Fable seamlessly integrates with your existing stack — and the team offers white-glove implementation and world-class support to ensure your team's success.

HOW PENNYMAC SUPERCHARGES HUMAN RISK REDUCTION AND INCREASES SECURITY TEAM EFFICIENCY

As one of the top lenders in the country today, Pennymac has helped nearly five million lifetime homeowners achieve and sustain their aspirations of home.

Pennymac's Human Risk Challenge

As a leading mortgage lender that handles sensitive financial data, Pennymac has a major task in managing its employee risk. Traditional security awareness products offer one-size-fits-all solutions that fail to engage their employees. Pennymac found that generic content broadcasted to the entire company didn't lead to swift employee security behavior changes.

Instead, they recognize that personalization and timeliness are key to changing employee behavior. "Our employees are at heightened levels of risk due to their roles, data access, and behaviors. We tailor our security program to address these varying levels of risk more effectively, providing higher protection where it's needed most," said Cyrus Tibbs, Pennymac CISO. "Our security awareness program needs to engage employees when the behavior occurs, not months later as part of an annual training program."

To achieve this vision, Pennymac proactively correlated data from different products to assess employee risk for targeted training. However, this was a manual process that took away from other security priorities.

Pennymac knew there was a better way to automate human risk assessment and awareness interventions that actually improved employee behavior. "The faster we can identify risky behavior and train on it, the faster we can shore up our human firewall."

Fable's Human Risk Solution

Pennymac decided to evaluate Fable against its existing manual awareness approach with an official A/B experiment, measuring the impact on employee behavior change.

The Fable proof of value was quick from setup to results within two weeks. Through application programming interface (API) integrations with Pennymac's technology stack, Fable developed an understanding of employee risk and formulated employee cohorts to target personalized security briefings in their email or chat environment.

Pennymac then built its first campaign targeting a subset of employees who needed to take a high-priority, mandatory security action. The

(continued)

(continued)

Fable platform generated a personalized training video outlining the security action which Pennymac was able to quickly customize to their policies.

Then, Pennymac deployed the campaign to relevant employees with the click of a button, easily scheduling reminders to employees who didn't complete the security action within the required time.

Why Pennymac Chose Fable

"We ultimately chose Fable Security because its personalized approach to security awareness led to more effective and faster employee behavior change." In the A/B experiment, Pennymac employees changed their behavior at a 38 percent higher rate than the generic alternative, but the real difference was that they completed the security action 13 times faster than normal, allowing Pennymac to shore up human risk faster than ever before.

Additionally, Fable improved the Pennymac security team's efficiency. It took Pennymac just minutes to deliver this campaign in Fable, compared to the over two weeks it would have taken to create, send, and track the campaign manually.

Fable's employee risk engine, which takes in signals from multiple products to identify employees at risk, automated Pennymac's previous manual processes. Its AI-powered content generation engine allowed Pennymac to rapidly generate training videos tailored to their needs in just minutes, which was previously impossible to achieve. And its automated campaign scheduling and drip reminders meant no manual overhead for the Pennymac security team.

Pennymac was able to deliver personalized training and follow-ups at scale. Going forward, Pennymac can increase awareness coverage for any attack topic without burdening its security team.

Finally, employees enjoyed the Fable personalized experience. Employees shared that the training was relevant and to-the-point. With relevant, personalized, and timely training from Fable, the Pennymac security team turned its employees into security champions.

Chapter 5
Ten Metrics That Matter

Here are ten important metrics to help you measure and report on the effectiveness of your organization's human risk management program.

Human Risk Score

An explainable numeric score that expresses the human risk of an individual, department, or organization. The score is based on available data about employees' roles, access, behaviors, threat targeting, and attack impact.

Top Human Risk Factors

The top factors comprising risk, including categories such as authentication hygiene, device security, data handling, phishing resilience, and more.

Toxic Combinations

The increase in risk brought on by two or more co-occurring behaviors and/or attributes, for example, access to sensitive data *and* weak multifactor authentication (MFA).

Targeting Lift

The percentage difference in behavior change of a targeted versus a generic campaign.

Time-to-Threat Response

The time it takes for a security team to warn targeted people about an emerging threat, such as a new social engineering scam.

Behavior Change

The percentage change in employee behavior from a human risk campaign, for example, adoption of a password manager.

Time-to-Behavior-Change

The amount of time it takes to change employees' behavior in a human risk campaign.

Security Incidents Avoided

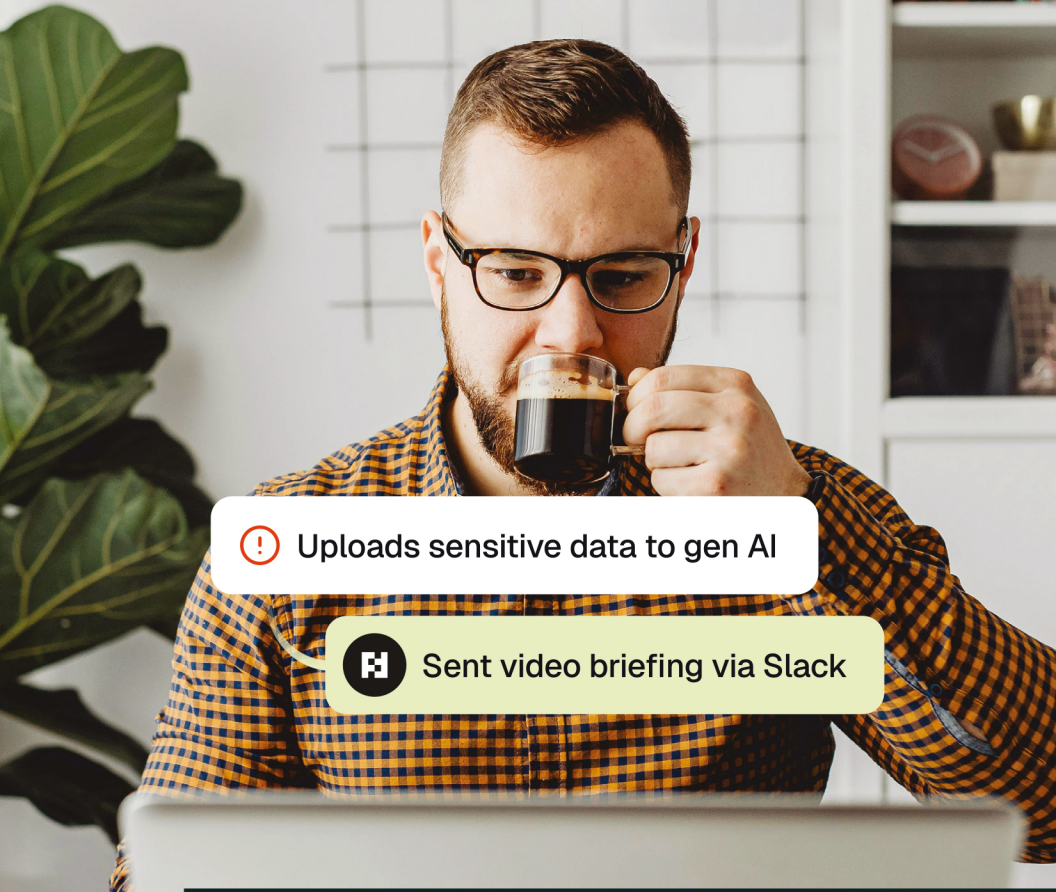
The estimated reduction in incidents avoided by prompting behavior change and reducing the exposure window of fast-moving threats.

Security Team Hours Saved

The estimated amount of security team hours saved not responding to incidents.

Cost-per-Security Incident Avoided

The estimated cost savings of incident avoidance, including both hard dollars of fines, penalties, legal fees, and lost revenue and soft dollars of redirected person-hours saved not responding to incidents.



Make *people* your first line of defense

Get modern human risk management from Fable.

FABLESECURITY.COM

Fable

Reimagine human risk

Despite spending billions on cybersecurity, organizations remain more vulnerable than ever to evolving cyberthreats. Human error is the common denominator in most breaches today — whether it's misconfigured systems, mishandled data, compromised credentials, or susceptibility to social engineering. This book shows how security teams can shift from reactive controls to proactive, adaptive strategies that account for the human element and the accelerating pace of AI-driven exploitation.

Inside...

- Taking a modern approach to human risk management
- Shaping behavior with targeted interventions
- Building a secure, resilient culture
- Assessing your organization's human risk maturity

Nicole Jiang is the chief executive officer of Fable, product leadership at Abnormal AI, Mixpanel, Microsoft, and Palantir Technologies.

Dr. Sanny Liao is the chief product officer of Fable, data science leadership at Abnormal AI, IFTTT, Ride.com, TellApart (Twitter), and M-Factor (IBM).

ISBN: 978-1-394-41950-0
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.