GUIDEBOOK

CISO Guide to Security Awareness Training

Turning Human Risk Into Human Resilience

Abnormal

Understanding Human Vulnerability in a Digital World

99%

of organizations experienced a security incident linked to preventable user actions in the past year.

Abnormal AI 2025 State of Security Awareness Training

$2.8B

in BEC-related losses annually.

FBI Internet Crime Report, 2024

60%

of data breaches in 2024 involved the human element.

Verizon 2025 Data Breach Investigations Report

Modern cyberthreats are engineered to exploit people, not just technology. Attackers know that even the most secure infrastructure can be undone by a single human action—especially when employees are stressed, distracted, or unaware. That's why phishing remains the entry point for nearly 77% of advanced email attacks. These campaigns often impersonate trusted contacts to steal credentials, initiate wire transfers, or deliver malware while bypassing traditional defenses.

The financial consequences are equally alarming. A single business email compromise (BEC) attack can cost an organization more than $137,000. On a global scale, BEC-related losses exceed $2.8 billion annually, according to the FBI's Internet Crime Complaint Center. And that's just the reported cases—the true cost is likely much higher. But beyond the financial impact, these incidents erode employee trust, damage customer relationships, and tarnish organizational reputations that may have taken years to build.

In the past year alone, 99% of organizations experienced a security incident linked to preventable user actions. From clicking on malicious links to responding to spoofed emails, human error continues to be the soft spot that threat actors exploit time and time again.

To combat this escalating threat, organizations must shift their mindset. Stopping threats requires the right technology, but it doesn't stop there. People need to be prepared, too. If something slips through, your users should be ready to recognize and report it. Teaching employees to identify and respond to social engineering tactics isn't just a compliance checkbox; it's a strategic imperative. Security awareness training (SAT) should be treated as a core pillar of any modern security program, helping organizations turn their biggest vulnerability into a frontline defense.

Threats Targeting the Human Layer

Rather than targeting technical flaws, attackers now focus on familiar communication channels, relying on phishing, impersonation, and other known tactics executed in more advanced ways. Messages are tailored with precision, stripped of obvious red flags, and often sent from legitimate, compromised accounts. They mimic the language, tone, and timing of trusted communications, making them nearly impossible to spot.

The tactics haven't changed, but their execution has. What once looked suspicious now feels normal.

Credential Phishing

Phishing has become the go-to strategy for attackers. It's quick to launch, hard to detect, and increasingly personalized. By mimicking trusted senders or familiar interfaces, phishing emails trick users into sharing login details, unlocking access to sensitive systems without raising alarms.

Business Email Compromise (BEC)

BEC attacks use carefully crafted messages to manipulate employees into taking high-impact actions, such as wiring funds or disclosing confidential information. These emails often appear to come from executives or trusted partners, and they rely on social pressure, urgency, and trust, not malicious links or attachments.

Vendor Email Compromise (VEC)

VEC is a rising threat where attackers compromise real vendor accounts and use them to launch attacks from within. These emails often appear legitimate, referencing actual invoices or ongoing projects, and can remain undetected for weeks. Because they originate from trusted sources, they exploit the strongest relationships to carry out fraud.

Payloadless Malware

Not all malware comes with an obvious attachment or link. Payloadless attacks use clean emails—no files, no URLs—to manipulate users into launching the attack themselves. A message might ask the recipient to enable a setting, change a configuration, or run a seemingly harmless command. The user becomes the delivery mechanism.

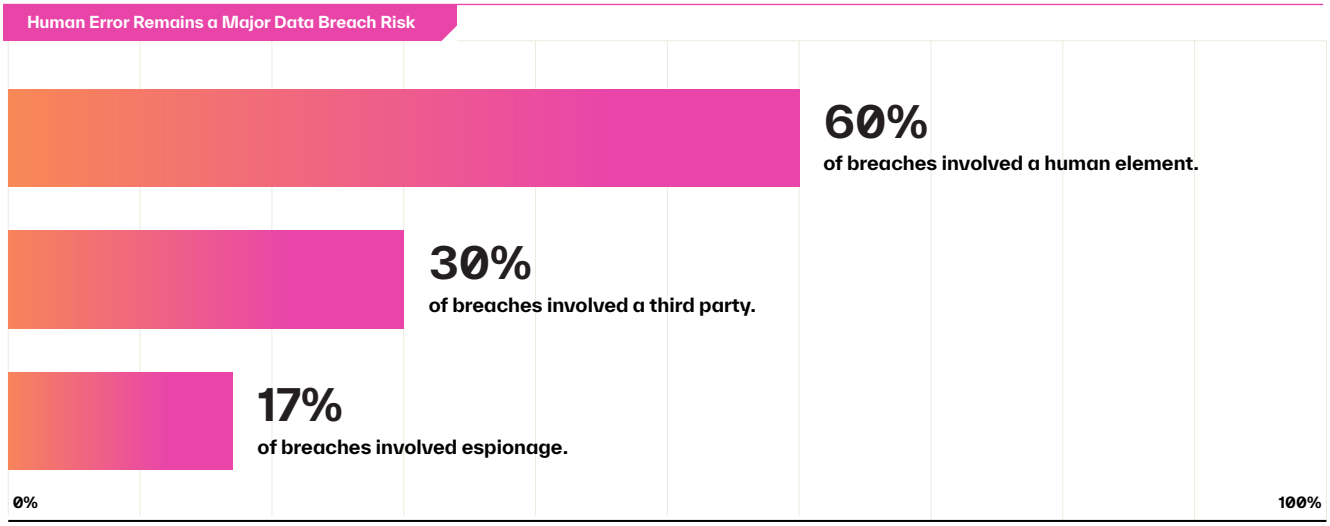
These threats aren't just technical—they're behavioral. Reducing human risk requires more than awareness. It demands training that adapts to real threats, engages users in the moment, and turns vulnerability into vigilance.

Why Traditional Training Isn't Working

Phishing, BEC, VEC, and malware aren't new attack types, but their tactics have evolved. Security awareness training has not.

Many organizations still treat security training as a one-time event—an annual exercise checked off with outdated tools that do little to change behavior. This creates a false sense of security and leaves employees vulnerable to increasingly advanced attacks. Notably, organizations relying on these less sophisticated methods report significantly higher rates of incidents linked to avoidable user actions. In the past year alone, 60% of overall data breaches involved the human element.

Human Error Remains a Major Data Breach Risk



2025 Verizon Data Breach Investigations Report (DBIR)

One-Size-Fits-All Content Fails To Engage Employees

The most common approaches to SAT—templated phishing simulations and hours-long training modules—are often generic and unengaging. This lack of personalization makes it easy for users to tune out. Employees aren't being trained to recognize threats relevant to their role, industry, or day-to-day responsibilities. And it's not just about the type of content—it's also how little employees engage with it. Many share answers, tip off coworkers when simulations have gone out, or look for shortcuts (like playing a video training in the background while doing other work) to avoid the material entirely. Our recent survey found that more than half of respondents said peer sharing undermines the value of training. When content is generic or irrelevant, employees disengage.

Current SAT Programs Require Heavy Lift and Leave Little Impact

Traditional training doesn't just fall flat with users—it also strains security teams. Half of security leaders in our survey said their biggest challenge was the time and effort needed to manage their program. Others pointed to stale content and tools that don't support meaningful improvements.

Program owners feel this pain most acutely. Seventy-five percent said they can't prove whether their training is working because they lack access to the right metrics. Without visibility into outcomes, it's nearly impossible to iterate or improve.

The problem isn't a lack of belief in training—it's the failure of traditional methods to deliver or even measure impact. Until SAT becomes easier to manage, relevant to modern threats, and measurable in its results, it will continue to fall short.

Shifting to a Security-First Culture

Reducing risk starts with creating a culture where security is second nature. Training needs to be timely, contextual, and personalized—meeting employees where they and adapting as threats evolve.

To work at scale, SAT should be continuous, not one-and-done. Automation and feedback loops can reinforce good behavior and help employees stay engaged. When done right, security awareness becomes more than just training—it becomes part of the way people work.

Why AI Belongs at the Center of Modern Awareness Training

To effectively defend against these human-layer attacks, organizations need more than conventional training—they need intelligent systems that can learn and adapt to employee behaviors in real time. That's where artificial intelligence (AI) changes the game.

- AI enables a shift from static training models to behavior-informed, contextualized education. By analyzing employee roles, communication patterns, and prior interactions, AI delivers personalized training tailored to each individual—reducing noise, increasing relevance, and reinforcing secure behavior where it matters most. This transforms passive learners into active defenders.

- Beyond customization and content creation, AI automates ongoing program management, making training consistent, continuous, and scalable. By converting real threats into teachable moments—directly in the inbox—employees build lasting awareness through in-the-moment coaching. With every interaction, the system learns and improves, helping security training keep pace with evolving attacks.

- CISOs recognize the value. In a recent survey, 95% said AI is critical to freeing up time for more proactive work, and 98% agreed that personalized, timely simulations based on individual behavior would significantly strengthen their organization's security posture. AI-powered training isn't just more effective—it's the foundation for building a resilient, security-first culture.

95%

of security stakeholders agree that leveraging AI in the cybersecurity stack is critical for freeing up time.

99%

of security leaders favor leveraging AI to automatically generate training campaigns and workflows.

98%

of organizations agreed that personalized, timely simulations based on individual behavior would significantly strengthen their organization's security posture.

Abnormal AI 2025 State of Security Awareness Training

Applying AI in the Real World: From Insight to Impact

Understanding AI's role in transforming training is just the beginning. The real value comes from how it's applied in practice—closing the gap between knowing and doing. Organizations leveraging AI for security awareness are moving beyond generic, scheduled lessons. Instead, they're embedding training into everyday workflows, making it relevant, timely, and grounded in actual threat activity.

Turning Real Attacks Into Real Lessons

Rather than simply quarantining blocked phishing attempts, AI-enabled systems analyze and repurpose them into simulations that reflect real-world threats employees encounter. These simulations mirror actual tactics—tailored by department, role, and user behavior. For example, if a finance team regularly sees invoice fraud attempts, AI can generate simulations using similar language, formatting, and urgency cues to train employees on the latest attack tactics.

In-The-Moment Feedback

When a user interacts with a simulation—by clicking, replying, or reporting—AI delivers just-in-time coaching directly in the inbox. This context-aware feedback explains what made the message suspicious and reinforces what to watch for next time. By providing training insights relevant to the employee's unique role, employees are more likely to retain the information and apply it in future encounters. Secure behavior becomes a habit—not just a checkbox.

Automated, Always-On Training

AI systems also manage the operational side of training: delivering simulations, tracking participation, and adjusting future content based on employee behavior. For instance, someone who frequently engages with risky messages may receive more frequent or advanced simulations. Because the system adapts automatically, training becomes continuous rather than one-off, and it aligns with how people actually work.

Reduced Burden on Security Teams

While AI improves the employee experience, it also simplifies administration. Security teams no longer need to build training manually or guess at effectiveness, spending hours finding the most relevant templates. Instead, they can easily measure their risk reduction over time, identify high-risk users, and demonstrate compliance to stakeholders with minimal overhead.

With AI, awareness training becomes not just smarter—but also more human, more relevant, and more effective.

Conclusion

While traditional training methods may have sufficed in a less sophisticated threat environment, they no longer stack up. Human error remains one of the most exploited vulnerabilities in cybersecurity, and closing that gap requires a new approach—one that's adaptive, personalized, and built to change behavior.

Security awareness training is no longer a check-the-box exercise. It's a strategic lever for risk reduction, culture change, and long-term resilience. By embracing AI-powered solutions, security teams can deliver context-aware training at scale, turning real threats into teachable moments and employees into active participants in defense.

The future of security awareness is intelligent, automated, and deeply human. For CISOs looking to reduce human risk and build a truly security-first culture, the path forward is clear: meet users where they are, empower them with real-world insight, and let AI do the heavy lifting.

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Interested in Learning More About How Abnormal Can Enhance Your Security Awareness Efforts?

See a Demo ›

Discover Your ROI ›