WHITE PAPER

2025 State of Security Awareness Training

Evolving Training Strategies for Reducing Human Risk

Abnormal

Executive Summary

Wise investments in security awareness training (SAT) have the potential to yield enormous returns for forward-thinking security leaders. Most of today's most prevalent attacks—such as phishing, social engineering, and business email compromise (BEC)—rely on tricking *people* to succeed. After all, humans inevitably make mistakes, especially when they're tired, stressed, anxious, or simply attempting to help others. Even before the advent of modern information technology, fraudsters have long used social engineering to induce fear or a sense of urgency and press their victims to act. Bringing this criminal behavior into the digital realm doesn't change its fundamentally deceptive nature.

It does, however, mean that social engineering is operating at scale, and there are signals—sometimes subtle, sometimes obvious—when online communications conceal malicious intent. Email-borne threats are the most common way for attackers to target their victims, with phishing now serving as the starting point for nearly 77% of advanced attacks, according to our latest Email Threat Report. Their scalability, low cost, and high success rate for bypassing technical defenses make these tactics a top choice for cybercriminals.

It can be very difficult to defend against these attacks with technology alone. Of course, a robust email security solution can stop many of them, but no technology is foolproof. With each single successful BEC attack now costing its victim an average of over $137,000—and global losses to this type of cybercrime totaling more than $2.9 billion—it's imperative that organizations adopt a multi-layered approach to defending against these threats. Because a majority of attacks now incorporate human actions (like initiating a funds transfer or granting bad actors insider-level access to accounts), educating employees to recognize the signals of malicious activity can go a long way towards reducing real-world breach risks.

Security awareness training (SAT) has an important role to play in enterprise-grade cyber defense. But far too many organizations have implemented only marginally-effective SAT programs. This is training that doesn't really engage employees, that doesn't feel directly relevant, that's too infrequent to have a meaningful impact on human behavior and organizational culture, or that is in place merely to fulfill compliance requirements.

It's possible to do better—to build a security awareness training program that:

- Reduces human risk
- Supports a security-first culture
- Enables easier execution and achieves better results
- Saves administrative time and effort

This isn't yet the norm. But as threats continue to grow in volume and sophistication, it's imperative that organizations create and maintain SAT programs that live up to their full potential.

To better understand how security leaders and practitioners are thinking about this challenge, we surveyed more than 300 stakeholders in security and IT across the United States and UK. Participants held a variety of roles, with more than one third (34%) serving as CIO, CTO, CISO, or VP of IT or Security within their organization. Most (60%) were director, manager, or team lead in security or security awareness training. Their organizations ranged in size from 1,000 employees to more than 25,000 employees, and crossed a broad array of industries.

In this white paper, we explore our findings. Readers will learn how security and technology professionals are thinking about security awareness training, how they're strategizing to improve their programs, and what's needed to optimize performance and reduce human error and risk.

99% of survey participants reported that their organization had experienced a security incident attributable to an avoidable user action within the past year.

100% of security stakeholders say that improving their organization's security awareness training program is among their short-term (<12 months) objectives.

83% said their organization's current security awareness training tools require substantial effort to operate and maintain.

99% favor including AI in security awareness training solutions and workflows.

53% agreed that the effort required to run and maintain their organization's current security awareness training program isn't worth the impact it appears to be having.

98% agree that having a phishing simulation solution that delivers contextually relevant, timely lessons tailored to each employee's risk profile and past behavior would significantly improve the organization's overall security posture.

40% said a lack of effective solutions on the market is among the main reasons their organization can't build a more successful SAT program.

Table of Contents

Security Awareness Training Today: Is It Working?

Security awareness training is widely used. According to a recent Gartner Peer Insights survey, nearly 75% of organizations require their employees to complete SAT modules at least once per quarter. However, only a few have implemented continuous training programs—and many of those exist solely to meet regulatory or cyber insurance requirements.

Despite their prevalence, few SAT programs are effective in changing employee behavior. There's widespread acknowledgment that the content is boring, irrelevant, or outdated, and employees often tune it out because it's perceived as something that's compulsory, not valuable. Given how likely threat actors are to target the human element, this opens major risks for today's enterprises.

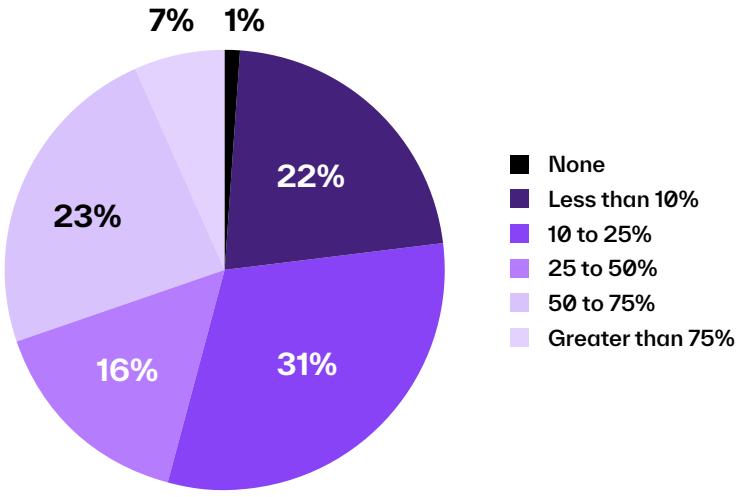
Incidents Due to Avoidable User Actions (AUA) Are Rampant

Our survey participants are experiencing significant risks that could be mitigated through the use of more effective security awareness training. Nearly all (99%) reported that their organization had experienced an avoidable security incident that was attributed to an end user action–such as clicking a malicious link in a phishing email–within the past year.

Nearly half of organizations (45%) reported that more than 25% of their security incidents could be attributed to avoidable user actions (AUA), while 33% said that more than half of their security incidents fell into this category.

Respondents in the UK were less likely to have experienced an event attributable to AUA—with only 27% indicating that more than 25% of their incidents were in this category—than respondents in the US—with 51% attributing more than 25%. We can't be certain why this is the case, but a lack of visibility into the causes of events might be responsible. Organizations in the U.K. outsource IT and cybersecurity functions at higher rates than their peers in other countries (one recent survey found that third parties are responsible for managing cybersecurity in 52% of U.K. businesses, as compared to 24% in France and 27% in Germany), leaving security stakeholders with less direct oversight of events and incidents.

What is the approximate percentage of your organization's security incidents over the past year that were caused (or significantly contributed to) by an avoidable user action?



Phishing Simulation Is a Top Training Technique

Organizations are making efforts to mitigate these risks—and the incidents they lead to—by training employees on cybersecurity best practices and using various tools to test their awareness and readiness. The most-commonly employed methods include email phishing simulations (used by 81%), topic-based training modules (used by 80%), and email-based tips or reminders (used by 71%). The least-commonly-employed methods include gamification (used by only 26%) and newsletters (33%).

Some of the most effective training strategies remain underused. Nearly 40% of organizations have not yet implemented just-in-time training, though its timeliness and relevance increase its effectiveness. An even larger group (43%) do not use video content to teach end users about cybersecurity, which misses valuable opportunities to deliver education in an engaging format.

Only a small number of participants reported that they were in security awareness training roles, but those that did were much more likely to use JIT training (67%) than other respondents. Participants who rated their organization's SAT program as "well-established" were also much more likely to have implemented JIT training (63%) than others. This suggests that organizations with more mature cybersecurity programs are dedicating resources (including the hiring of specialized employees) to adopting effective SAT techniques. Participants in specialized SAT roles were also far more likely to report using gamification (42%) than participants in other groups. And *only* those who rated their SAT program "well-established" had adopted gamification.

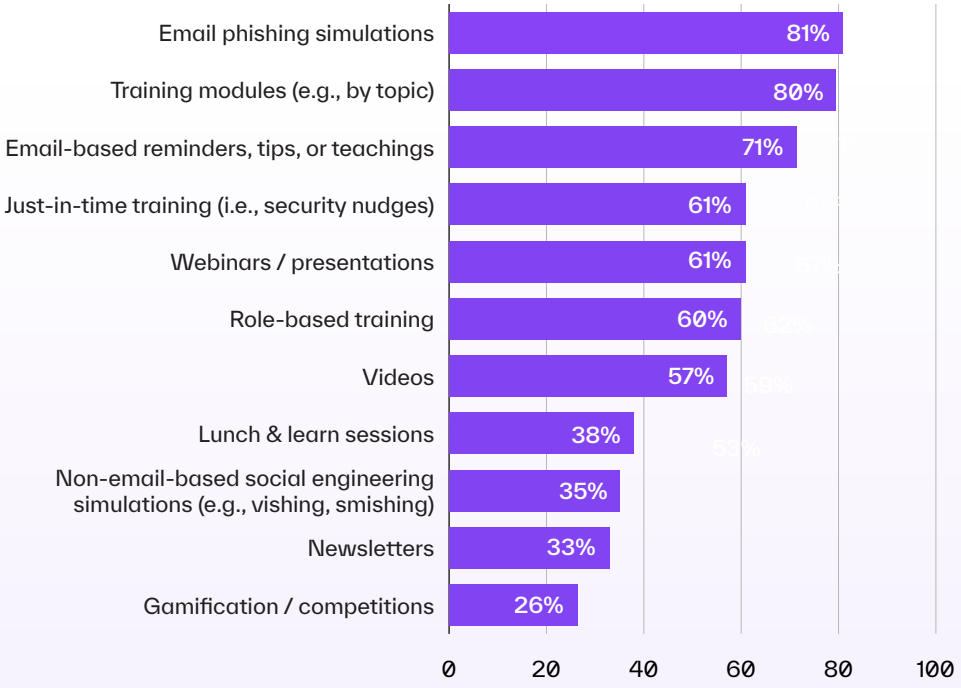
Survey participants who reported that their organization's SAT maturity was "minimal" most often used email-based reminders as a primary training technique (83%), while those who said their maturity was "basic" used training modules more often (92%).

What is Just-in-Time (JIT) Security Awareness Training?

Traditional security awareness training assumes that employees will retain the information they learned during periodic training sessions. Just-in-Time (JIT) training instead delivers education to employees at the exact moment they need it—for instance, right when they encounter a suspicious email or other potential threat. Using behavioral nudges, JIT provides instant feedback to users, explaining, for instance, why an email was flagged as malicious and how to spot similar attacks in the future. This dynamic, adaptive learning is based on current threats and individual user behavior, with bite-sized lessons that are highly relevant to real-world risks.

Organizations using training methods that we'd consider "less sophisticated" (such as phishing simulations, training modules, email reminders, webinars, and lunch-and-learn events) tended to experience a greater number of incidents attributable to avoidable user actions. In the "less sophisticated" group, 29% reported that between half and 75% of their incidents were due to AUA (versus 23% of all respondents), and 14% reported that more than 75% of their incidents were attributable to AUA (versus 7% of all respondents).

Which tactics/tools does your organization currently use to train or test employees on security policies and practices? Select all that apply.



High Effort, Low Impact

Even when SAT efforts are extensive, they don't always have the risk-reduction impact that stakeholders are seeking. Many teams find these programs difficult to manage—83% of respondents agreed that their organizations' current SAT tools require substantial effort to operate and maintain.

But all that effort often doesn't seem to be paying off. Nearly half (49%) of survey participants agree that the impact of their current security awareness training tools/programs is minimal. This skepticism is particularly widespread among respondents in specialized security awareness training roles, 62% of whom were in agreement with the above statement.

A slightly larger group (53% of participants) agree that the effort required to run and maintain their current security awareness training program outweighs its apparent impact. Respondents in SAT roles were particularly likely to agree that effort outweighs impact, with a full 69% concurring.

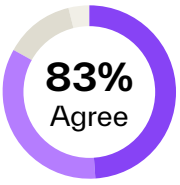
There are multiple reasons why the effort put into SAT programs doesn't always match the desired results. One key factor is that employees often try to bypass the training, which significantly reduces its effectiveness. A majority of respondents (57%) agreed that the usefulness of their organization's security awareness tools is diminished by employees' tendency to share information and answers with one another. This sentiment was even more widely held by participants in specialized SAT roles, 62% of whom agreed with it.

Another reason that stakeholders aren't convinced that their organizations' SAT programs are worth the effort is that it isn't always easy to measure the impact of those programs. A significant minority (42%) of respondents agreed that reliably measuring outcomes from SAT programs was challenging for their organization.

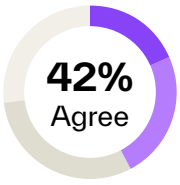
When it's difficult to gather reliable, quantitative data on the impact that an activity like security awareness training is having on an organization's risks, how can stakeholders be confident that their efforts are worthwhile? The unfortunate truth is that they can't.

Describe your agreement with each statement.

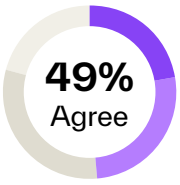
Our current security awareness training tools require **substantial** effort to operate and maintain.



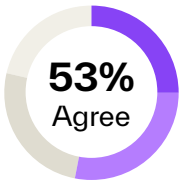
The impact of our current security awareness training program is unclear because measuring outcomes is challenging/unreliable.



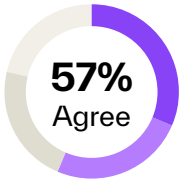
The impact of our current security awareness training tools/programs is minimal.



The effort required to run and maintain our current security awareness training tools/program outweighs the impact they appear to be having.



The usefulness of our security awareness training tools are diminished by employees sharing information and answers with one another.



Strongly agree | Somewhat agree | Somewhat disagree | Strongly disagree

Uncovering the True Impact of Security Awareness Training Programs

With ongoing uncertainty around whether security awareness training meaningfully reduces cyber risk, measuring its effectiveness has become a top priority. Yet for cybersecurity and risk leaders, it remains a persistent challenge.

Traditional measures, such as how many employees fall for phishing simulations or how often they complete training modules, offer only a weak proxy for organizations' susceptibility to real-world attacks. And it isn't easy to find—or implement—better ways of measuring SAT effectiveness.

Metrics for SAT Effectiveness

Participants in our survey are experiencing these challenges firsthand. When asked which metrics they use to measure the effectiveness of their security awareness training efforts, survey respondents reported that they turned to phishing simulation metrics most often (71% use this method), and employee feedback almost as often (69%).

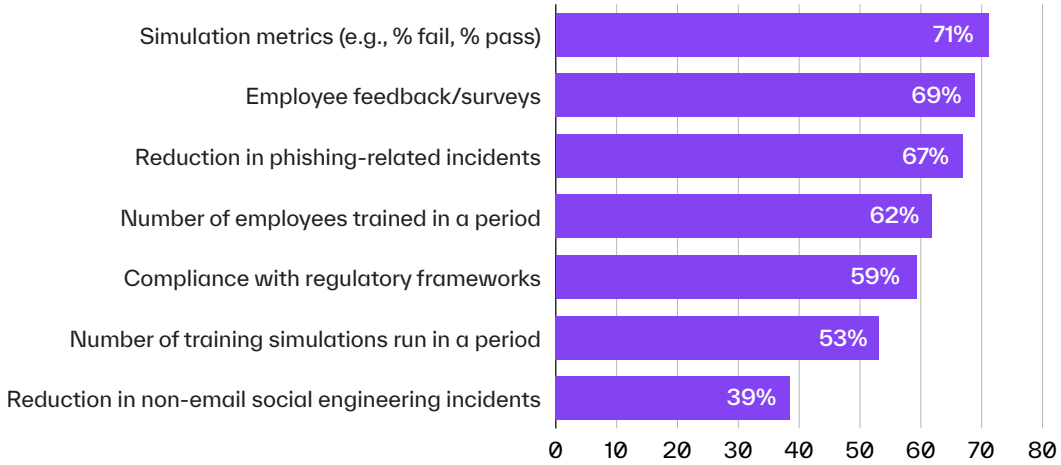
While phishing simulations do provide a snapshot view of short-term program outcomes, their results are a poor measure of long-term behavior change or real-world risk. And because employees don't know what they don't know, surveys and other forms of feedback don't accurately reflect the results of SAT efforts.

Ranked third by participants in our survey was reduction in phishing-related incidents before and after security awareness education is conducted. While this is a somewhat better measure of real-world risk, it is far from perfect. After all, phishing rates vary over time and with shifts in the cyber threat landscape. They also reflect other defensive measures the organization is putting in place, like email security solutions, so that phishing email click rates cannot be considered in a vacuum.

It's worth noting that nearly all of the metrics we asked about—aside from those related to non-email social engineering incidents—are used by more than half of the participants' organizations. In other words, most organizations are trying to measure a wide range of factors, which, like SAT itself, requires significant effort.

What's less clear is whether all this measurement is delivering meaningful results.

Which metrics does your organization use to measure the effectiveness of its security awareness training efforts and investments? Select all that apply.



SAT Performance Blind Spots

With no accurate means of assessing the effectiveness of their SAT programs, organizations are left to fall back on guesswork.

Often, also, they're left without the means to imagine anything better. Even though incidents caused by avoidable end-user actions are rampant (recall that 99% of respondents reported that their organization had experienced at least one such incident within the past year [see p. 6]), most survey participants are broadly satisfied with the capabilities of their current SAT tools and program.

Approximately 60% of respondents report that their current solutions' setup and deployment capabilities are strong (despite the fact that running phishing simulation campaigns is often labor-intensive) and a similar number say that automated reporting and compliance tracking capabilities are strong.

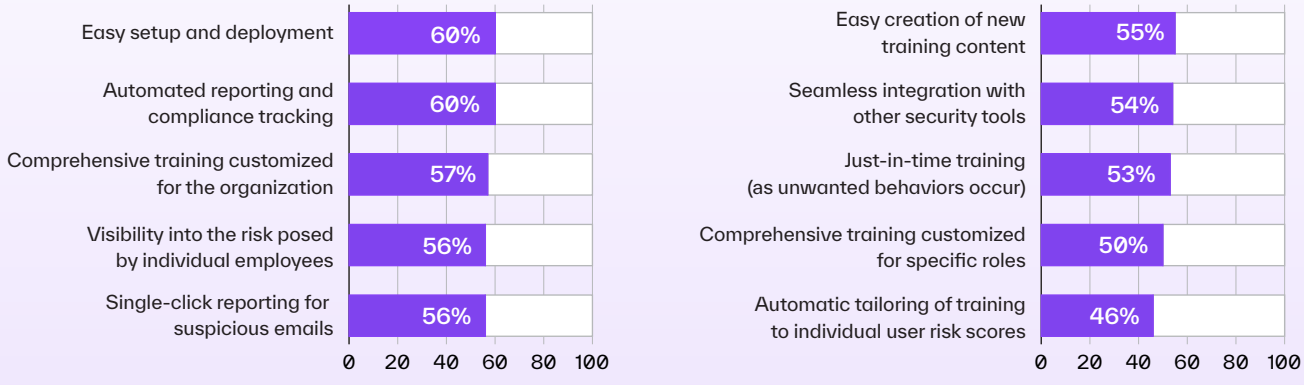
In several areas, though, respondents in SAT roles are less sanguine about their organizations' capabilities than the average survey participant. For instance, 58% of survey participants in SAT roles stated that their current visibility into the risks posed by individual employees was less than strong, as compared to 44% of survey participants overall. In addition, 58% of survey participants in SAT roles said that their current ability to create new content for use in training was less than strong, as compared to 45% of survey participants overall.

These discrepancies suggest that respondents with more hands-on experience working with SAT solutions may be more aware of their limitations than the average respondent.

Still, most participants' (relatively high) level of satisfaction with their current SAT tools and program isn't aligned with the large number of preventable incidents their organizations are experiencing.

99% **of survey participants reported that their organization had experienced a security incident attributable to an avoidable user action in the past year.**

The chart below shows the percentage of respondents who said their SAT tools and capabilities were strong in each of the following areas.



Why SAT Programs Fall Short

The amount of time and effort required to run an effective security awareness training program is the biggest blocker preventing organizations from achieving success.

A full 50% of respondents ranked the effort- and labor-intensiveness of SAT programs as a top factor inhibiting their success. A significant number (40%) of survey participants also mentioned a lack of effective solutions available on the market. Nearly as many (39%) indicated that an inability to keep training fresh (and incorporate the most relevant current threats) keeps their SAT program stagnant and ineffective.

Survey participants in SAT-specific roles were much more likely than the average participant (75% vs. 38%) to report that an inability to demonstrate their program's impact and value was inhibiting its success. Stakeholders with this kind of hands-on experience are much more aware that it's difficult to find and gather the metrics that matter to support a SAT program.

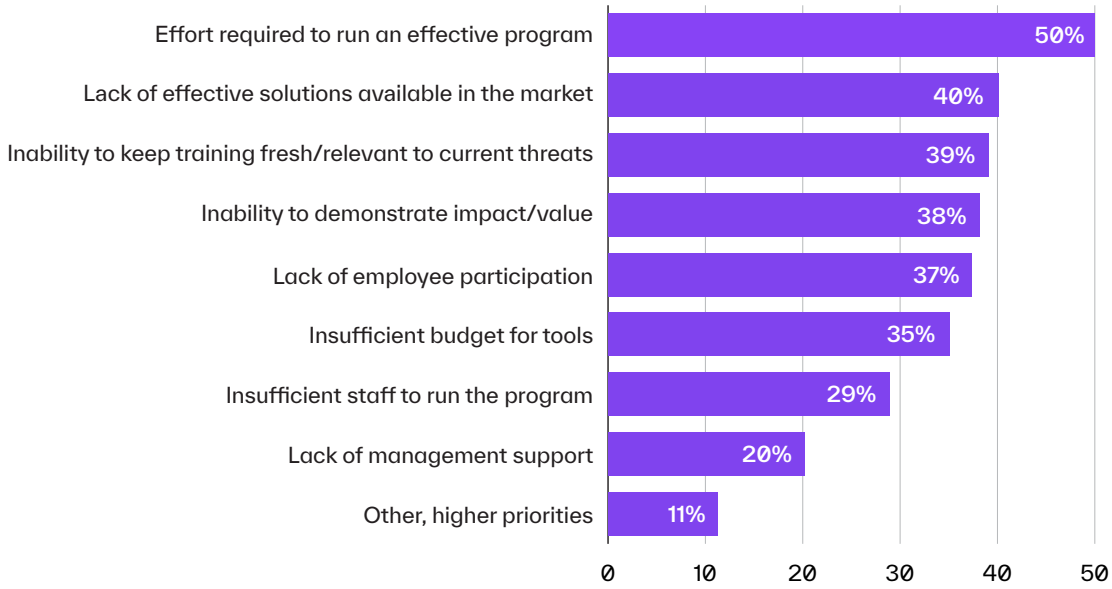
Our survey suggests that organizational leaders do believe that security awareness training is important.

Significant majorities of respondents reported that insufficient staffing was *not* among the top inhibitors issue (mentioned by fewer than one-third [29%]), nor was lack of management support (mentioned only by 20%), or a failure to prioritize SAT programs (mentioned by just 11%).

Taken together, these responses suggest that organizations have a strong need for solutions that will greatly reduce the amount of effort required to run effective SAT programs. Our findings also indicate that solutions that can deliver robust, quantitative evidence of the impact of SAT programs can make a paradigm shift possible, enabling stakeholders to escape an impasse that's all too common today, in which they don't know what they don't know, and can't tell what's not working.

40% **of survey participants reported that their organization had experienced a security incident attributable to an avoidable user action within the past year.**

Which are the top factors keeping your organization from having a more successful security awareness training program? Select three.



Strategies for Improvement

Respondents recognize that security awareness training programs can deliver enormous value, but in most organizations, that value remains unrealized.

Across cybersecurity, AI is already enhancing operations, amplifying human expertise, and enabling teams to do more with less. When applied to SAT, AI can bring the same benefits—improving both the efficiency and effectiveness of training programs.

Priorities for Improving SAT

We asked survey participants about their near-term priorities for improving their security awareness training programs. All participants stated that achieving such improvements is among their organization's objectives for the next year.

Even though more than two-thirds of respondents (71%) did not rank "insufficient staffing" among the top inhibitors to their SAT program's effectiveness (see p. 13), the top response, mentioned by nearly two in three (65%) respondents, was increasing SAT program staffing.

The second-most-common response was developing more relevant training (mentioned by 49%).

Nearly as many survey participants (48%) are planning to implement AI-powered solutions to supplement their current SAT tools. If done correctly, this could also help them accomplish the previously-mentioned goal of developing more relevant training.

A sizable majority (78%) are looking to purchase a new AI-powered solution within the next year, either to supplement their current tools or to replace what they already have.

Taken together, these findings indicate that many organizations are prepared to invest in people and technology to improve their security awareness training capabilities. With the right solution—one that realizes the same benefits that AI is already delivering in other aspects of cyber defense—it may be possible to improve program performance and results without hiring.

Because a significant cybersecurity skills shortage remains the reality (and even fewer professionals are available who are specifically specialized in SAT), this AI-driven approach stands to realize significant value for those who adopt it.

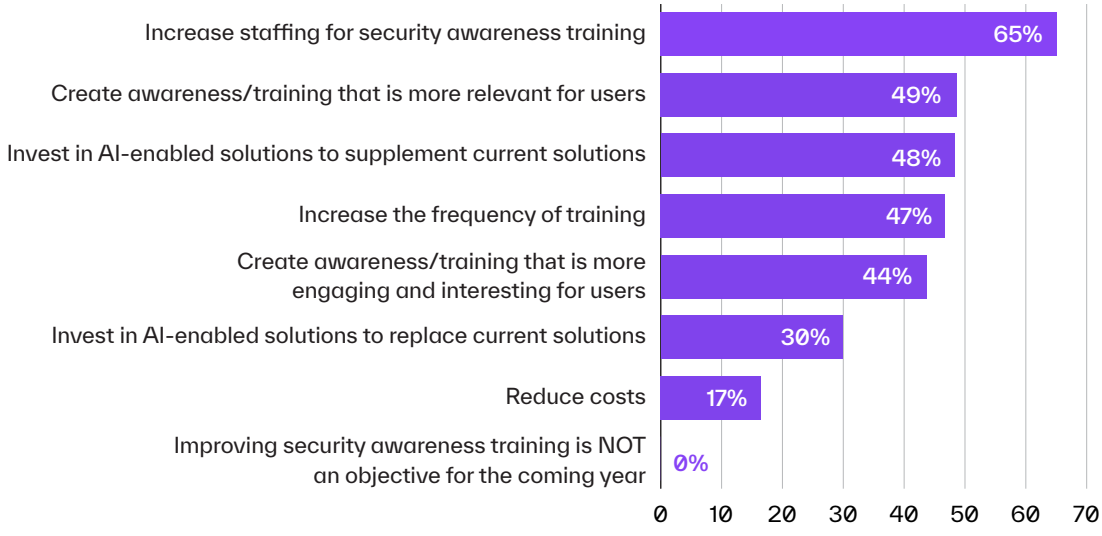
78%

of organizations are planning to adopt AI-powered solutions within the next year to improve their SAT capabilities.

48%

are planning to implement AI-powered solutions to supplement their current SAT tools.

What are your organization's top priorities over the next 12 months for improving its security awareness training program? Select three.



The Case for Engaging, Personalized Training

Survey participants are very conscious of the need to better engage employees in SAT programs. We asked them which capabilities were most important for improving security awareness training solutions.

The top responses were:

- Content that is engaging (mentioned by 59%)
- Content that is personalized (that is, relevant to each individual employee) (mentioned by 51%)
- Content that is customized to the organization (mentioned by 44%)

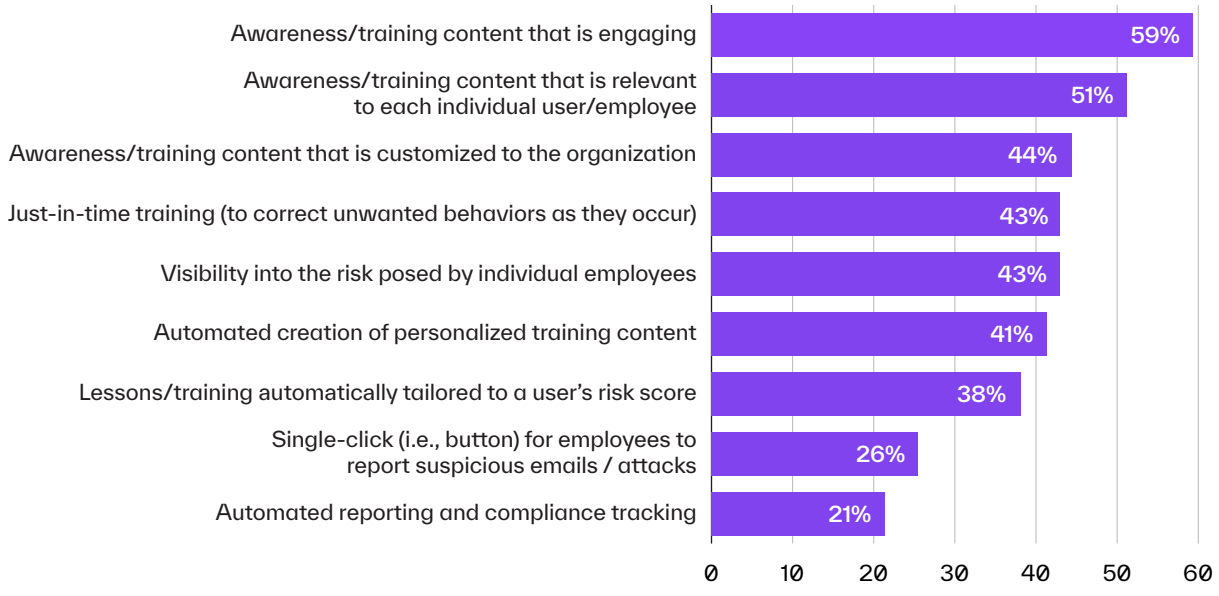
There was less interest in implementing a one-click system for users to report suspicious emails (mentioned by only 26%) and in automated reporting and compliance tracking (21%).

Among professionals in SAT roles, there was significant interest in content customized to the organization, just-in-time training to correct risky behaviors as they occur, automated creation of personalized training content, and tailoring training to individual users' risk scores. Each of these was mentioned by 58% of SAT professionals.

For stakeholders overall, compliance appears to be less of an issue than culture change and real-world risk reduction.

Truly engaging employees, after all, is the best way to help them learn and retain the lessons over time. Personalizing and customizing training content ensures that it addresses the most relevant risks, while just-in-time training makes it possible to teach employees what they most need to learn, exactly when they need to learn it.

Which are the most important capabilities/characteristics of an ideal solution for security awareness training? Select up to four.



AI Is the Missing Link

Given their goals, it's no surprise that survey participants overwhelmingly support the use of AI in SAT solutions.

- 99% favor leveraging AI to automatically generate training campaigns and workflows.
- 95% favor leveraging AI to automate the creation of training videos (so that there's no longer a need to do so manually).
- 95% favor taking advantage of AI to automatically create individualized attack simulations based on individual user profiles (instead of having only general simulations available for use with all users).
- 95% favor leveraging large language models to conduct conversational coaching as part of SAT.
- 96% favor using AI to create dynamic risk scores based on past user behavior and the types of attacks targeting certain types of users.

What's more, 100% of stakeholders in organizations with mature SAT programs favor using AI in these programs.

A large majority (95%) agree that using AI in the security stack is critical for freeing up time, so that the security team can shift from a reactive to a proactive approach. And nearly all respondents (98%) agree that having a phishing simulation solution that delivers contextually relevant, timely lessons tailored to each employee's risk profile and past behavior would significantly improve the organization's overall security posture. In fact, 74% *strongly* agree with the above statement.

95% **of security stakeholders agree that leveraging AI in the cybersecurity stack is critical for freeing up time, empowering the team to shift from a reactive to a proactive approach to defense.**

The Abnormal AI Phishing Coach

Abnormal has developed a new AI-powered approach to security awareness training, one built to empower employees to identify *today's* threats and designed to take full advantage of generative AI:

Delivers Hyper-Personalized Phishing Simulations

The AI Phishing Coach uses real (but defanged) threats intercepted by Abnormal's email security solution as content. This makes it possible to deliver realistic, personalized phishing simulations—tailored to individual roles and the current attack landscape—to every employee.

Enables Effortless Creation of Training Videos

With no need for scripts or production teams, the AI Phishing Coach builds custom training videos from scratch, videos that will match your brand's identity and remain compliant with Center for Internet Security (CIS) and National Institute for Standards and Technologies (NIST) guidelines.

Provides Contextual, Just-in-Time Coaching

Whenever an employee interacts with a phishing simulation, the AI Phishing Coach immediately responds—using generative AI—with a personalized coaching email, reinforcing learning at the exact moment it's needed.

Improves Information Retention with Dynamic, Real-Time Learning

By continuously adapting the training to current threats and real-world user behavior, the AI Phishing Coach helps employees change how they react to threats, sharpening their phishing detection skills.

Replaces Generic Training with Targeted, Role-Specific Content

The AI Phishing Coach automatically generates training that reflects each employee's responsibilities, industry, and unique threat exposure.

Bridges the Gap Between Compliance and Engagement

Security awareness training is no longer just a checkbox activity. The AI Phishing Coach transforms it into an ongoing interactive experience, with lessons that actually stick and content that employees will remember and apply.

Conclusion

Despite the ongoing investments organizations make in improving their technical capabilities, the number of successful email attacks continues to rise. To reduce risks, supplementing technical defenses with a robust cybersecurity awareness training program is a must-do, but few of today's programs are as effective as they could (or should) be. With endless emails in their inboxes and back-to-back meetings on their calendars, employees rarely feel they have the time and mental bandwidth to give SAT programs the attention they deserve. The faster the pace of business, the more unrealistic it may be to expect people to retain the lessons they learn from training modules for an extended period of time.

A lack of effort or investment isn't the issue. What's most problematic is a failure of imagination—stakeholders can't yet envision the disruptive change that's needed for this technology to live up to its full promise. Because few people have experienced the kind of timely, relevant, and deeply personalized training that can truly engage employees, they don't know what they are missing.

An entirely new approach to SAT is needed, one that puts less responsibility on end users for remembering what they've been taught and carving out time to complete additional modules. Instead, the solution should engage employees in real-time dialogue whenever they report a suspicious email, giving them feedback on whether the message was truly malicious and offering security best practices for the specific threat in question. The solution should also provide hyper-personalized training for individual end users, ensuring relevance while reinforcing good habits and educating employees about the latest threats.

For years, this kind of security awareness training—dynamic, responsive, and highly personalized—was something that security leaders might have wished for, but implementing it in the real world would have been far too labor-intensive. Today, generative AI is putting such next-generation security education within reach for organizations of all sizes, regardless of the size of their security team or the state of their infrastructure.

A truly effective SAT solution can mitigate risks that cannot otherwise be addressed (that is, the risk of human error) in a way that's both cost-effective and culturally transformative. Abnormal created the AI Phishing Coach to make the dream of highly effective SAT a reality.

About Abnormal AI

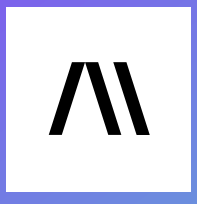
Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and 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 Your ROI ›

Request a Demo ›



ABNORMAL.AI