

AI IN ACTION

Test your organization's readiness for deepfake attacks with tabletop and red-team exercises

BY STEVE TAYLOR, KAREN SCHULER, CFE, FIP

SHARE: SAVE:



WRITTEN BY:

[Steve Taylor](#)

[Karen Schuler, CFE, FIP](#)

DATE: JUNE 4, 2026

READ TIME: 9 MINS

Computers and Technology

Cyberfraud

Fraud Prevention and Deterrence

Services Professional Scientific or Technical

Banking and Financial Services

Artificial intelligence is changing how fraud is perpetrated and many organizations aren't prepared. In this column, the authors describe how conducting tabletop and red-team exercises can prepare employees to respond nimbly to AI-generated deepfake attacks.

During a recent media interview, a C-suite leader reflected on what his firm learned after losing millions of dollars to a deepfake fraud attack. The perpetrators staged a virtual meeting with videos of the firm's employees and an executive generated with artificial intelligence (AI). The deepfake videos were so lifelike that the only non-AI-generated employee invited to the meeting was compelled to transfer funds to the perpetrators.

The executive warned that organizations are under attack every day by social engineering schemes using AI so that people without technical skills can easily copy voices, images and videos realistic enough to [steal billions of dollars globally](#). To effectively confront deepfake fraud, he advises organizations to rehearse responses to attacks.

In our experience, [tabletop exercises](#) and red-team simulations are effective, practical activities for organizations to fortify their defenses against AI-enabled schemes. By putting teams into realistic deepfake fraud scenarios, employees get to flex their decision-making muscles, test verification processes and identify weaknesses before real attacks occur.

Real threats, simulated responses

Organizations are vulnerable to AI-generated fraud attacks as technology evolves and [becomes more difficult to detect](#). Deceptions that previously required Hollywood-level production budgets and advanced technical skills are now perpetrated with consumer-grade software and minimal training.

According to a 2025 survey by Gartner, [62%](#) of organizations have experienced a deepfake attack involving social engineering or the exploitation of automated processes. A 2026 [Anti-Fraud Technology Benchmarking Report](#) by the Association of Certified Fraud Examiners and SAS found that only 7% of survey respondents believe their organizations are prepared to fend off such attacks. Traditional fraud prevention mechanisms, including static fraud response plans, periodic awareness-training activities and traditional authentication procedures aren't sufficient on their own to address these threats. A model to identify AI-enabled threats on-the-fly, effectively manage responses under stress, and keep pace with rapidly evolving methods of attack is necessary.

Ad

ASSET FRAUD PREVENTION AND DETECTION

Virtual Seminar
June 23, 2026

CPE Credit: 8

[LEARN MORE](#)

Experiential learning approaches — particularly tabletop exercises and red-team simulations — can be powerful tools for anticipating deepfake incursions.



The imperative of experiential learning

Traditional fraud-training models were developed by observing obvious flaws in cyberfraud schemes: unfamiliar email addresses, grammatical mistakes, unusual requests or inconsistent details.

Deepfake-enabled deception, however, removes some of the most obvious red flags of fraud and exploits social interactions. AI-generated video, cloned voices, and highly contextual phishing messages reference legitimate business activity and appear to originate from trusted colleagues or senior executives. Requests may arrive through familiar communication channels and contain accurate internal details, making them appear legitimate.

Experiential learning can help employees navigate the increasing sophistication of deepfake fraud attacks. By placing teams in simulated fraud scenarios, employees practice verifying requests, coordinating with other departments and making decisions under realistic, high-pressure conditions. These exercises reinforce behaviors that help prevent fraud, such as pausing and validating instructions through secondary channels and escalating uncertainty, before a real attack occurs.

Research on [simulation-based learning](#) shows that active practice may improve both retention of information and behavioral responses. [Studies comparing experiential learning with lecture-based instruction](#) show significantly higher knowledge retention and confidence among participants who practice decision-making in simulated environments. More importantly, experiential training translates knowledge into action by building familiarity with decision processes required during real incidents.

Tabletop exercises and red-team simulations

Among experiential learning approaches, two methods are particularly effective in strengthening fraud preparedness: tabletop exercises and red-team simulations involving business and operational stakeholders.

In tabletop exercises, cross-functional teams discuss how they'd confront specific fraud attacks, including key decision-making processes, communicating the attack to the organization and any organizational barriers, such as unclear approval steps, delays in verification requests and miscommunications, that can complicate responses. Red teams, however, respond in real time to simulated attacks mimicking the pressures organizations face when experiencing a real attack. Together, these exercises and simulations build awareness, clarify roles and responses, and develop muscle memory for responding to attacks.

But the value of these exercises depends on good design and execution. Organizations must carefully consider the threats they simulate, the people involved, the decisions being tested, and processes used to verify and escalate suspicious activity.

Understanding the threat landscape

Deepfake video technology has rapidly evolved from crude digital manipulations into convincing impersonations used in recorded messages and live video calls. Publicly available footage, such as earnings calls, conference presentations, or social media videos, provide material for fraudsters to replicate facial movements and speech patterns into persuasive impersonations.

Advances in generative AI allow attackers to recreate an individual's voice with remarkable accuracy using only a few seconds of recorded speech. These synthetic voices are deployed in phone calls, voicemail messages, or voice-enabled collaboration platforms, enabling fraudsters to impersonate executives, vendors, or colleagues during urgent requests or authorization processes.

Fraudsters may use AI to create phishing and social engineering campaigns that can imitate an organization's communication style, reference real projects, and incorporate details gathered from social media, corporate announcements or public filings. Social engineering is one of the most common ways that cyber criminals manage to breach systems and attack organizations. Generative AI is accelerating the scale of attacks by creating new content instead of simply replicating it.

AI also helps fraudsters construct synthetic identities with all the requisite documentation. By combining legitimate personal data with fabricated information, these identities easily pass verification checks. Employment histories, social media profiles and other documents make identities appear credible to automated systems and human reviewers, allowing fraudsters to gain access to customer onboarding procedures, vendor management platforms or provisioning processes.



Effective exercises and simulations

A well-designed tabletop program is structured to discuss policy and test decision-making, verification processes and cross-department coordination under pressure.

Red-team simulations assess whether organizations can detect and respond to AI-enabled threats as they happen beyond discussions. These simulations may be highly controlled exercises where participants know they're being tested or simulations in which only a few employees know they're being tested. Organizations may start with controlled simulations to develop processes and build confidence before attempting a realistic scenario. Whichever form your organization selects depends on your company's culture, legal and ethical frameworks, and risk tolerance.

Successful exercises and simulations have clearly defined objectives about the scenarios to test, who participates and what questions exercise facilitators emphasize during discussions. Without these objectives, exercises risk becoming theoretical conversations rather than meaningful preparedness tools. Generic goals, such as "improving fraud awareness," won't garner results. Instead, exercises focus on specific organizational capabilities to test or strengthen.

For example, your organization may test whether employees can recognize deepfake-impersonation attempts, if verification procedures remain effective when communications appear legitimate, or whether escalation protocols function properly when conventional warning signs are absent. Exercises may also test whether employees can coordinate responses across departments during a fraud attack.

Scenario selection

Effective scenarios reflect how AI-enabled fraud occurs and engage participants while remaining focused on the specific decisions and processes being tested.

For tabletop exercises, an effective scenario could be a video call from someone posing as a technology vendor claiming that a security vulnerability requires immediate remote access to the internal system. A similar variation involves the impersonation of an executive making a financial transaction. In both scenarios, an urgent message emphasizes speed and discretion in a seemingly credible situation demanding quick verification before access can be granted.

Synthetic identity attacks are another scenario for testing. A new vendor is onboarded with documentation that passes automated verification checks, but subsequent suspicious activity raises questions about the vendor's authenticity. Participants must determine how verification procedures function during onboarding and whether monitoring systems detect fraudulent activity when a new user gains access.

These scenarios may also be used for red-team simulations. In these exercises, the "red team" generates a deepfake video message or a live call impersonating a senior executive or trusted vendor. The video message or call demands urgent action — a wire transfer, credential sharing, or an exception to security controls — and the organization tests whether employees question the request, how they attempt verification and whether established procedures withstand realistic conditions.

The red team must create convincing communications, establish credible channels of contact and anticipate how employees verify requests. They may also consider creating synthetic identities to test when verification is dependent on automated checks and when human verification can provide additional security. Simulations should be realistic enough to test defenses without creating unnecessary risk. For example, exercises involving payment requests need safeguards to prevent transfers, and planners must determine how the simulation proceeds when employees confirm the request through independent channels, such as a known phone number.

Participant selection

Exercises lose value if the appropriate people aren't involved. Fraud incidents are rarely confined to a single department. A deepfake targeting the finance department still requires verification from executive leadership, input from legal and technical support from information security teams.

Participants should involve representatives in finance, IT security, legal, compliance, operations and other relevant business units. Depending on the scenario, executives or senior decision-makers are included, particularly if exercises test escalation procedures or approval processes.

The goal is replicating a real fraud attempt. When participants from multiple departments confront the same scenario, they might realize there are different assumptions about who has the authority to approve actions and how teams are expected to communicate during an incident. These gaps frequently surface when teams test a situation together. The right participants do more than contribute expertise — they reveal whether the organization's response plans function proficiently when attacked.

Facilitation development

The effectiveness of these exercises also depends on who facilitates. A skilled facilitator guides the discussion and allows participants to explore decisions and uncertainties that emerge from the exercises. The facilitator can be an internal fraud, risk, or security professional, or an external specialist.

The facilitator begins a tabletop exercise by introducing the scenario. Facilitators follow with additional information — called “injects” — to complicate the situation and force participants to reassess their decisions. For example, participants may initially verify an executive request through a callback to a known phone number. The facilitator then injects a hurdle, such as a voicemail system that appears authentic but routes to a spoofed or simulated mailbox. These complications prevent participants from relying on simple solutions and encourage deeper discussion. Facilitators prompt participants to explain their reasoning, identify information they'd seek in a real situation and clarify who makes critical decisions.

A facilitator also oversees the scope, safety and execution of simulations, although the red team leads the real-time scenario. Red-team simulations require additional operational details, such as realistic scripts, technical methods and contingency plans for different participant responses.

A skilled facilitator ensures that exercises test decision-making processes rather than simply rehearsing policies. Someone other than the facilitator, however, should document the exercise. This observer documents decisions, deficiencies, differences and disagreements, unanswerable questions, and records findings and subtle observations.



Capturing observations and lessons

Running an exercise is only part of the preparation process. The most valuable insights often emerge during the analysis phase. Exercises frequently reveal vulnerabilities that are difficult to identify through policy reviews alone, including unclear decision-making authority, verification procedures that disintegrate under pressure or gaps in cross-department communications. Note-takers document how participants respond to the scenario, where confusion emerges and which questions remain unresolved.

Red-team simulations provide an additional layer of insight, allowing organizations to measure response capabilities directly. Detection rates, response times, escalation speeds and cross-functional coordination can help establish a baseline for evaluating how well fraud defenses can function. These quantitative measures are most valuable in conjunction with qualitative analyses of detection success or failure, how employees made decisions, and where procedures were unclear or difficult to execute.

Post-exercise reviews foster open discussion without fear of blame or punishment. The objective isn't to evaluate individual performance but to understand where systems and processes failed to support effective decision-making. Participants examine what worked, what proved challenging and which elements of the scenario created uncertainty.

The deficiencies revealed during these exercises don't always carry equal risks, and organizations must assess their significance and prioritize remediation based on potential impact, likelihood of exploitation and the complexity of corrective actions. Organizations then translate insights into concrete improvements. Remediation activities may include strengthening verification requirements for high-risk transactions, implementing alternative verification channels when primary contacts are unavailable, clarifying escalation procedures when conventional fraud indicators are absent, or introducing technical safeguards designed to detect AI-generated impersonation attempts.

However, weaknesses can't be addressed through training alone. Vulnerabilities often stem from process design flaws, unclear policies or insufficient technical controls that training can't solve. Effective remediation also requires policy clarification, process redesign, improved verification mechanisms and strengthened technical safeguards.

From reactive to resilient

Being prepared for an AI-enabled fraud attack requires sustained commitment and continual investment in governance and anti-fraud strategies.

Programs designate senior organizational leaders as operational owners supported by fraud prevention teams, IT and risk management to ensure that exercises receive necessary resources. By regularly conducting tabletop exercises and red-team simulations, organizations may gauge how employees respond to fraud attempts and reinforce verification procedures throughout the organization.

Equally important is adapting scenarios to address emerging threats. Monitoring threat intelligence, industry research and peer organizations' experience can align exercises with real-world risks.

Fraud preparedness exercises are part of broader security and risk management efforts; not isolated from other training programs. Insights gained from simulations may inform security awareness programs, risk assessments and improvements to internal controls. When employees successfully identify simulated fraud attempts, those successes should be highlighted to reinforce behaviors that strengthen organizational defenses.

Organizational resilience depends on recognizing fraud as it occurs and on building habits that challenge suspicious requests, verify identities and respond appropriately when the deception is real. Experiential learning is a pathway to resilience that passive learning can't build.

Karen Schuler, CFE, is the global head of Privacy, Data and AI Governance at BDO USA. Contact her at kschuler@bdo.com.

Steve Taylor is director of forensics at BDO USA. Contact him at setaylor@bdo.com.

You May Also Like



Managing insider-fraud risks in a pandemic

5 MINUTES

WRITTEN BY: [RASHA KASSEM, PH.D., CFE](#)



Fake calls from Amazon and Apple, vaccine scams, strengthening passwords

6 MINUTES

WRITTEN BY: [ROBERT E. HOLTRETER, PH.D., CFE](#)



Conduct data-driven investigations of suspicious employment claims during pandemic

7 MINUTES

WRITTEN BY: [VINCENT M. WALDEN, CFE, CPA](#)

FRAUD

MAGAZINE®

A publication of the Association of Certified Fraud Examiners



[About the ACFE](#) | [Contact Us](#) | [For Media](#) | [For Advertisers](#) | [ACFE Foundation](#)

