

Facilitating a Cybersecurity Workshop: **Overview and Learning Outcomes**



Lecture informs; facilitation makes the room do the thinking



Check-the-box stalls: 45% sit at SANS Stage 3, 19% compliance-focused



Outcomes: engagement, retention, measurable behavior change — not audit artifacts



Three formats: 90-minute session, half-day tabletop, multi-week rehearsal



Four roles: lead facilitator, co-facilitator/scribe, observer-evaluator, IT/SME support



The 2026 Threat Reality **Your Workshop Must Reflect**

REAL THREATS. REAL PEOPLE. A STRONGER TOMORROW.



- 98% of BEC is identity-driven; 79% of investigated incidents bypassed MFA—mostly AiTM, session hijacking



- 40% of Q1 2026 BEC used AI-generated content; typos and generic greetings are no longer credible cues



- Multi-channel attacks are now the norm: email, smishing, vishing, quishing, deepfake voice and video



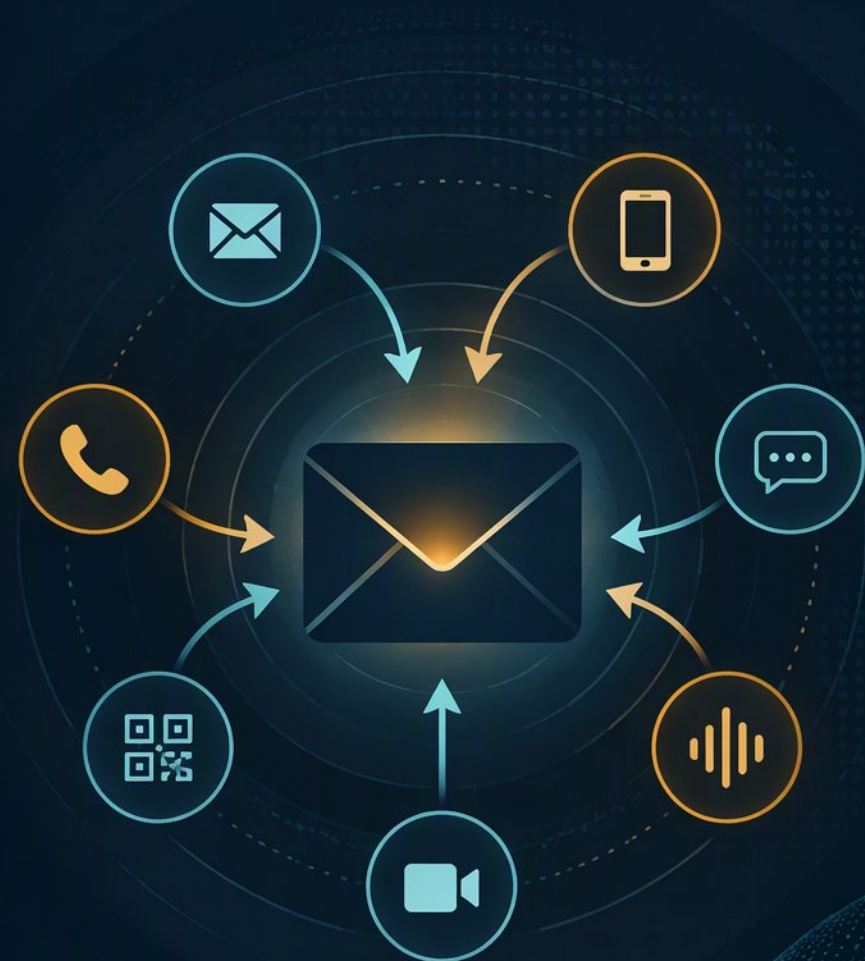
- Automation reaches 67,000 users at 42,000 organizations in under three hours



- 88% of organizations suffered trust-eroding incidents in 12 months; 60% lack confidence against deepfakes



- Teach structural and behavioral verification—callback, approval chain, out-of-band check—not typo spotting



Audience Analysis and Scoping before You Design Content

RIGHT
PEOPLE
SAFER
OUTCOMES



AUDIENCE SEGMENTS (BY RISK)

HIGHER
RISK



LOWER
RISK



staff



managers



IT



executives



finance/AP

SCOPING CHECKLIST



Segment by risk, not org chart:

staff, managers, IT, executives, finance/AP



Pull baseline data:

simulation results, incident trends, help-desk themes, audit findings



Define success before content:

report rate, time-to-report, repeat-click reduction



Settle constraints early:

time, room/lab, hybrid, language, accessibility, approvals



Align HR, legal, privacy, sponsors before

layoff, benefits, or payment lures

Designing the Learning Journey and Content Architecture



Start with “why this matters to my job”—relevance before content



Progress from awareness to comprehension to judgment under pressure to team decision



Games and hands-on practice beat lecture-only formats for behavior change



Open with a disorienting dilemma, then group reflection—not red-flag checklists



Reusable library: scenario modules, injects, question banks, assessments, microlearning



Map each module to ISO 27001 7.3/ A 6.3 and NIST CSF 2.0 PR.AT-01/-02



Building Realistic Scenarios and Defensive Drills



PEOPLE
PRACTICE
PREPARE
STAY AHEAD



Start from your truth: sector, geography, money-losing workflows, observed attack patterns



AI-era scenarios: CEO invoice fraud with forwarded thread, payroll redirection, deepfake callbacks, QR phishing, MFA fatigue



Run every tabletop the same way: objectives, ground rules, injects, timebox, hot-wash, AAR with owners and dates



Match format to question: tabletop for judgment, functional drill for procedures, red-team only with written authorization



Rules of engagement in writing: no live attacks, whitelisted domains, no real credentials or production data



Facilitation Techniques:

Engagement and Psychological Safety



Contract the room first: purpose, agenda, no-fault framing, confidentiality



No-fault rule: scenarios test plans and systems, never individual people



Ask open questions with generous wait time; redirect the loudest voice



No spectators: every participant—including remote—has a role and must speak



Real-incident disclosure: pause, route out-of-band to security, reassure—don't interrogate



Structured prompts plus small breakouts increase airtime and reduce dominance



Running the Drill:

Pre-Brief, Injects, Timekeeping, and Hot-Wash



- Pre-brief: objectives, roles, rules, ops-safe handling, no-fault framing



- Inject one update at a time; ask a question that forces a decision and named owner



- Scribe captures who decided what, why, and how—notes feed the AAR



- Hot-wash immediately: objectives met, strengths, gaps, next steps



Timebox 30 minutes; structured beats an open-ended debrief

Handling Difficult Moments: Conflict, Blame, and Real Incidents



Spot the blame spiral early: IT versus business, "we told you not to click"



De-escalate: slow down, reframe to the system, separate observation from person



Real-incident disclosure: triage out-of-band, protect the reporter, promise nothing you can't keep



Sensitive lures (layoffs, payment fraud) need HR consent and care



Co-facilitator signals and pause points let you step out briefly



Document system gaps, not employee identities—this is not an audit



From Hot-Wash to After-Action Report and Improvement Plan



The AAR is the product, not the appendix: summary, analysis, findings, plan



Write findings as observation, analysis, recommendation—never personality judgment



Every corrective action: finding reference, action, named owner, due date, verification



Keep it short: ten pages read beat forty filed; break large work into milestones



Re-test the weakest capability with a new scenario, then compare ratings



Set TLP classification and distribution up front; sponsor signs off owners and dates

Inject / Scenario

Executive Summary

Findings

Observation

Analysis

Recommendation

Improvement Plan

Finding Reference	Action	Named Owner	Due Date	Verification

Measuring Learning and Behavior Change **That Sponsors Believe**

- Kirkpatrick spine: reaction, learning, behavior, results—state which level each metric proves
- Reporting rises with training: 21% of simulations reported vs. 5% for untrained users (Verizon DBIR)
- Normalize clicks by difficulty tier (NIST Phish Scale) and program maturity before comparing
- Go beyond click rate: report rate, median/90th-percentile time to report, real-threat reporting quality
- Aggregate and anonymize—no league tables, no punishment tied to simulation results



Tooling, Hybrid Logistics, and Accessibility



Test platform against access needs:

WCAG 2.2 AA, screen readers, keyboard-only, phone dial-in



Hybrid rooms fail predictably:

one speaker, one mic, one chat-watcher



Accessible material:

captions, editable formats, alt text, 4.5:1 contrast, 200% resize



Contingency kit:

printed materials, offline injects, fallback dial-in, platform-death plan



Protect the exercise:

whitelisted domains, no real credentials, no production data



Sustainment: Embedding the Workshop in a Program, Not a Calendar



One workshop fades fast—plan microlearning, refreshers, and repeat simulation from day one



Reminders and interactive examples extend retention months beyond initial training



Locate your SANS maturity stage; move one high-impact behavior, not six



Realistic resourcing: 3+ dedicated FTEs and 3–5 years for measurable behavior change



Scale through HR, Communications, Operations, and internal audit partnerships



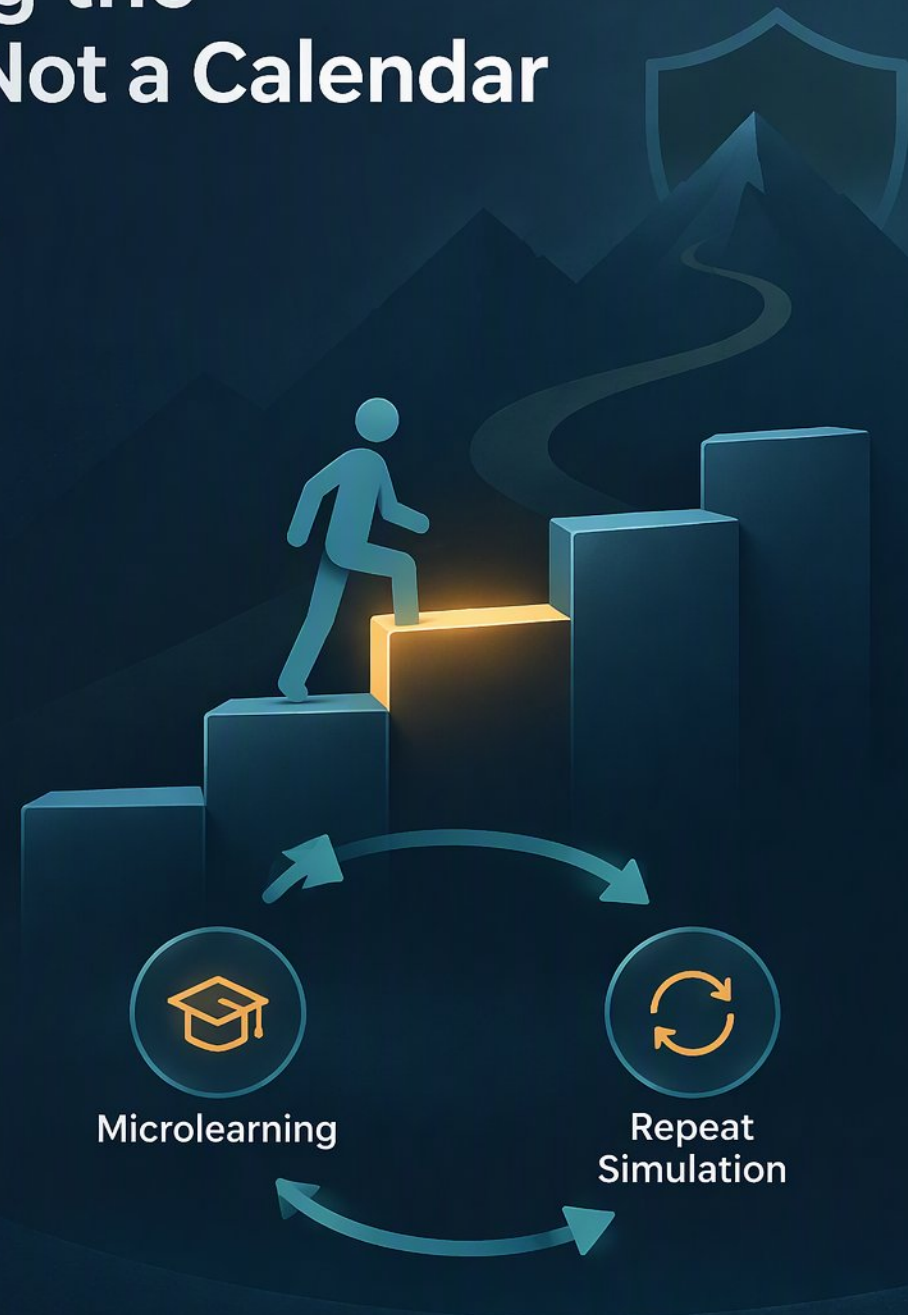
Grow a facilitator community with shared scenarios, peer observation, coaching loops



Click



Report



Putting It Together: Take-Home Checklists and Next Steps



PEOPLE
PREPARE
PRACTICE
STAY READY



Pre-workshop

- ☐ scope
- ☐ objectives
- ☐ audience segments
- ☐ baselines
- ☐ approvals
- ☐ accessibility



Design

- ☐ current-threat scenario
- ☐ difficulty tier
- ☐ injects
- ☐ key questions
- ☐ assigned roles



Delivery

- ☐ contract
- ☐ no-fault framing
- ☐ timeboxes
- ☐ disclosure protocol
- ☐ hot-wash agenda



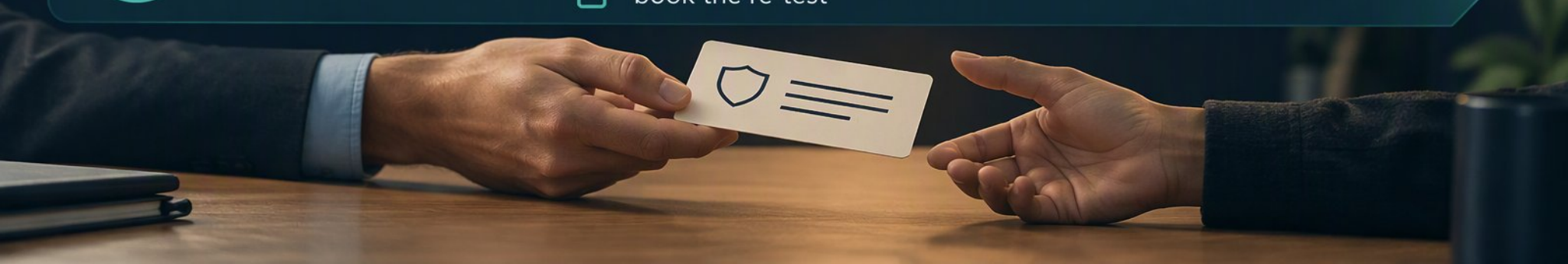
Post-workshop

- ☐ AAR within 14 days
- ☐ owned and dated actions
- ☐ re-test booked
- ☐ Metrics: report rate, time to report, click rate by tier, real-threat reporting—as trends



First 30 days

- ☐ one 90-minute session plus a small tabletop
- ☐ baseline
- ☐ book the re-test



Practice Clinic: Rehearse the Room Before You Run It

PRACTICE
BUILDS
READINESS

SAME SKILLS
SAFER ROOMS
STRONGER OUTCOMES



Micro-rehearsal 1:

open in five minutes—
purpose, ground rules,
no-fault, first question



Micro-rehearsal 2:

deliver an AI-era inject;
land a decision with
a named owner



Micro-rehearsal 3:

de-escalate a blame
outburst and a real-incident
disclosure



Micro-rehearsal 4:

10-minute hot-wash
yielding three corrective-
action candidates



Peer rubric:

objective clarity, airtime balance,
time discipline, safety, notes quality



Commitment:

name one workshop next quarter
and the metric you will report

Plan
Rehearse
Facilitate
Improve

PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/094aa933/public