Security Awareness Program Example: Patterns, Strengths, and Pitfalls

- Framing question: what does a real program look like day to day?
- Three lenses: recurring patterns, provable strengths, common pitfalls
- Audience contract: decision-ready takeaways for security, IT, risk, L&D, compliance, reviewers
- Roadmap: anatomy, governance, patterns, strength cases, failure modes, measurement, adaptation
- Scope boundary: awareness vs. role-based training vs. education vs. culture — conflating them weakens programs

What Counts as a Security Awareness Program

- A governed, risk-based, continuous learning capability that changes workforce behavior
- Four layers: broad awareness, role-based training, professional education, event-driven reinforcement
- NIST SP 800-50 Rev. 1 (2024): five-phase Cybersecurity and Privacy Learning Program lifecycle
- ISO 27001:2022 separates competence (7.2) from awareness (7.3, Annex A 6.3)
- NIST CSF 2.0 PR.AT-01 covers general training; PR.AT-02 covers role-specific training
- Correct up front: completion ≠ capability; 100% pass ≠ safety; phishing simulation alone ≠ a program

Anatomy of a Representative Program

GOVERNANCE CLOCK: CHARTER AUTHORITY VS. LIVING CALENDAR

- **Core components:** governance, risk assessment, content design, delivery, measurement, improvement
- **Cadence:** annual baseline, quarterly campaigns, monthly micro-learnings, just-in-time nudges
- **Named roles:** program owner, security champions, HR/L&D, GRC, executive sponsor
- **Artifacts:** charter, RACI matrix, training matrix, annual calendar, metrics dashboard
- **NIST SP 800-50 models:** centralized, centralized policy with distributed delivery, fully distributed

NIST SP 800-50 MODELS

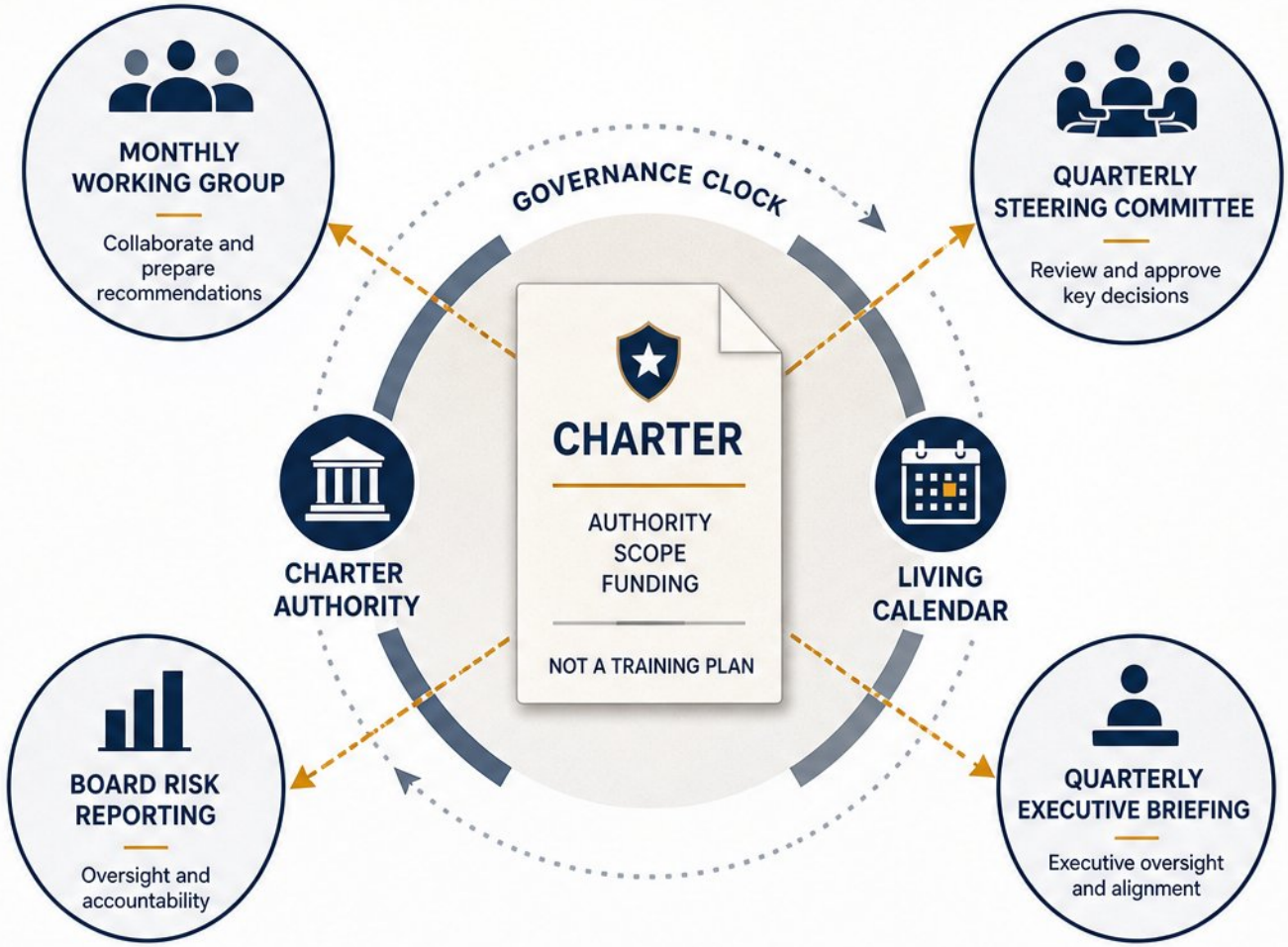
CENTRALIZED
One central entity designs, controls, and delivers the program.

CENTRALIZED POLICY WITH DISTRIBUTED DELIVERY
Central authority sets policy and standards; distributed teams deliver locally.

FULLY DISTRIBUTED
Multiple entities collaborate to design, manage, and deliver the program.

Governance, Charter, and Decision Rights

- Charter governs authority, scope, funding — not a training plan
- Name decision rights: scenario approval, data use, budget, exceptions, termination
- Monthly working group; quarterly steering committee; quarterly executive briefing
- Stable charter, living calendar: absorb incident-driven changes without renegotiating scope
- Write down amendment authority — or scope creep erodes the program



STABLE CHARTER
Defines enduring authority, scope, and funding.

LIVING CALENDAR
Adapts to incidents and emerging needs without renegotiating scope.

Patterns That Recur Across Effective Programs

- Risk-based targeting by exposure and leverage, not org chart
- Role-relevant rehearsal: finance on BEC, developers on secrets
- Positive reinforcement over shame; reporting kept to one click
- Just-in-time prompts at the moment of risk
- Transparent, trended metrics segmented by department
- Continuous iteration; retire content that stops engaging

Patterns by Maturity Stage

1 Non-Existent	2 Compliance Focused	3 Promoting Awareness and Behavior Change	4 Long Term Culture Change	5 Optimization and Resilience
No formal program or structure in place.	Policies and training in place to meet requirements.	People apply knowledge; behavior change becomes measurable.	Security is integrated into culture across the organization.	Continuous improvement drives resilience and adaptability.

- SANS five stages: Non-Existent, Compliance Focused, Behavior Change, Culture Change, Optimization
- Stage 2 compliance programs assemble in about one month
- Stage 3 sees measurable behavior change within 6–12 months
- Stage 4 organization-wide culture change commonly takes 3–10 years
- Metrics evolve from completion rates to detection and recovery times
- Scale requires dedicated staff, program age, and cross-department partnerships

Strengths: What the Example Program Does Well

- Visible executive sponsorship: leaders train, receive briefings, and report human-risk trends
- Measurable risk reduction: phishing susceptibility, credential submission, report volume, time to report
- Blended delivery: mandatory baseline, role-based modules, simulations, just-in-time learning
- Inclusive design for global, multilingual, hybrid, and shift-based workforces; localization and accessibility are requirements
- Feedback loop: simulation results, employee reports, and real incidents drive documented content changes
- Audit-ready by design: versioned curriculum mapped to controls, per-employee records, review minutes

Case Evidence: What Measurable Strength Looks Like

Vendée Habitat
(~300 staff)

- Vendée Habitat (~300 staff): vulnerability 20%→2% in three years; 200+ reports/month; CEO fraud stopped

lastminute.com
(1,700 staff)

- lastminute.com (1,700 staff): vulnerability index halved in 12 months via Slack coaching, 24 micro-sessions/year

CoreDux
(~300 users)

- CoreDux (~300 users): phish-prone ~12%→5% average (low 2%); ~900 reports in six months

YAMAM Group
(~80 staff)

- YAMAM Group (~80 staff): click-through 24.64%→1.41% — 94% cut in eight months

- **Credible claims share: honest baseline, steady difficulty, rising reports alongside falling clicks**

Pitfalls: Where Awareness Programs Commonly Fail

REPORT–TO–CLICK RATIO

AWARENESS THAT INFORMS ACTION— NOT JUST CLICKS.

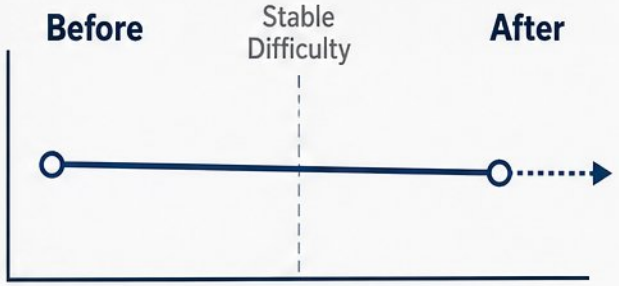
- Compliance theater: 100% completion, high click rate — proof of nothing
- Annual-only training; knowledge decays and most of the year is uncovered
- Blame-oriented simulations: leaderboards and discipline kill reporting
- Generic modules for developers, finance, and frontline staff satisfy nobody
- Weak measurement, easy templates; 90%+ pass rates signal inflated results
- Under-resourcing, ignored local culture, and distress-based lures erode trust

The Evidence on Training Effectiveness

UC San Diego Health Study

≈19,500 employees

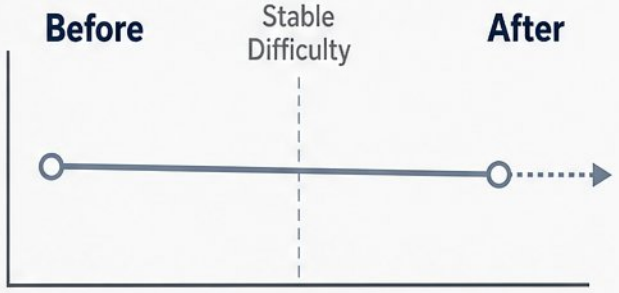
- UCSD Health (≈19,500 employees): annual training showed no significant phishing-failure link



Fintech Reproduction

(N=12,511)

- Embedded training cut click likelihood by only ~2 points; 75% engaged under a minute
- Fintech reproduction (N=12,511): neither lecture nor interactive training improved clicks or reporting

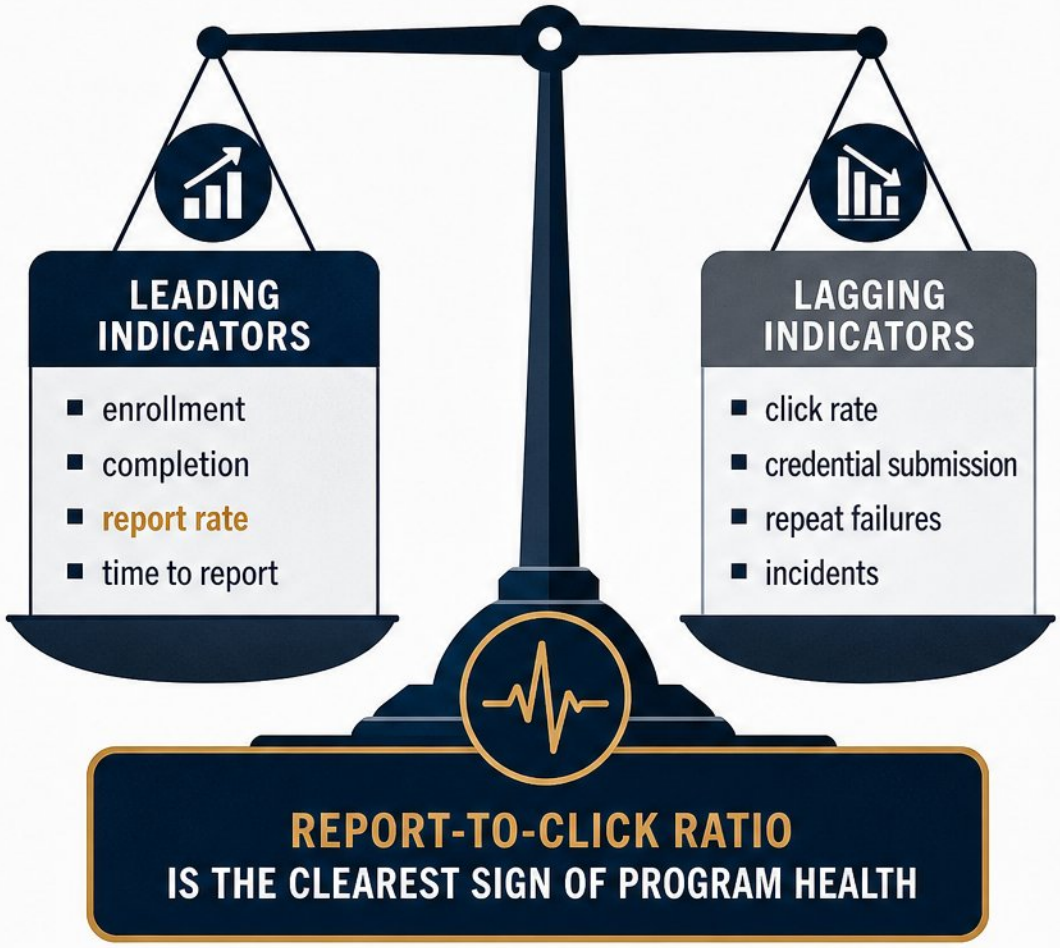


NIST Phish Scale

- NIST Phish Scale: click rates doubled, ~7% easy to ~15% hard lures

- **So training is a weak control — pair it with reporting channels, JIT coaching, technical controls**

Measuring Strength Without Gaming Metrics



- Leading indicators: enrollment, completion, report rate, time to report

- Lagging indicators: click rate, credential submission, repeat failures, incidents

- Report-to-click ratio is the clearest sign of program health

- Trend click, leak, and report together—falling clicks only count if difficulty holds

- Avoid vanity metrics and traps that reward hiding incidents or easy lures

BALANCE QUANTITATIVE SIGNALS WITH QUALITATIVE CONTEXT. | BENCHMARK DISCIPLINE. | FOCUS ON BEHAVIOR CHANGE.

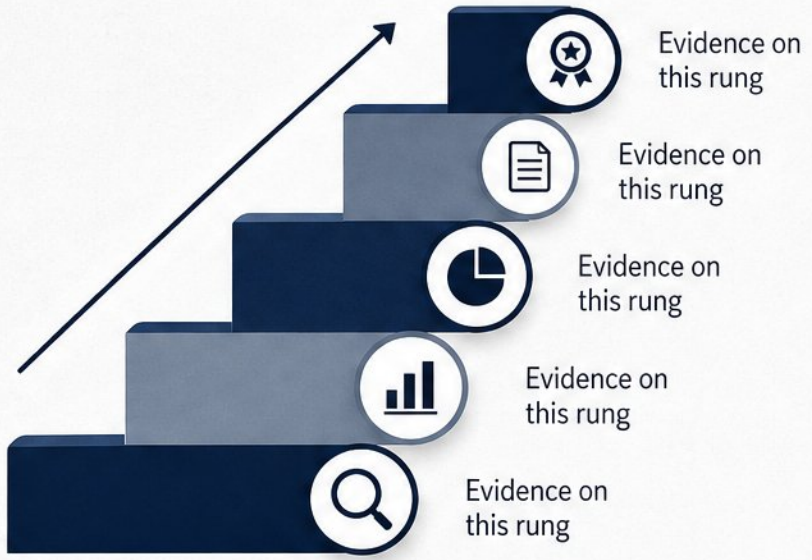
Adapting the Example to Your Own Context

- **Step 1:**
  Baseline simulation and content audit; map to a maturity model
- **Step 2:**
  Map stakeholders; secure executive sponsorship early
- **Step 3:**
  Select delivery mix by workforce, budget, and regulation
- **Step 4:**
  Define a few outcome metrics and baseline before intervening
- **Step 5:**
  Pilot one audience, learn, then scale; document decisions

CHECKLIST

- **Checklist:**
  copy governance, reporting culture, measurement discipline

MATURITY LADDER



Reviewer's Playbook: Evidence, Questions, and Red Flags

Evidence to Request

- Request the charter, risk assessment, versioned content, and per-person records

Questions for Program Owners

- Ask owners: how is content refreshed, how is success defined, what triggers remediation

Red Flags vs. Green Flags

- Red flags: perfect completion, no sponsor, punitive simulations, stale templates
- Green flags: risk-based targeting, calibrated difficulty, trended metrics, triaged reports

- Separate design gaps from evidence gaps; name the owner and date

90-Day Action Plan and Key Takeaways

DAYS 1–30

- Days 1–30: working reporting channel, blind baseline simulation, named owners across security, HR, IT, GRC

DAYS 31–60

- Days 31–60: publish behavior baseline, segment by exposure and leverage, start monthly micro-learning

DAYS 61–90

- Days 61–90: just-in-time coaching post-click, click/leak/report dashboard, first management review

PROGRAM VITAL SIGN

REPORT-TO-CLICK RATIO

- Patterns beat one-off tactics; behavior change against stable difficulty proves strength

- Commit: instrument one high-impact behavior and change something visible in 90 days

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/3d04a984/public