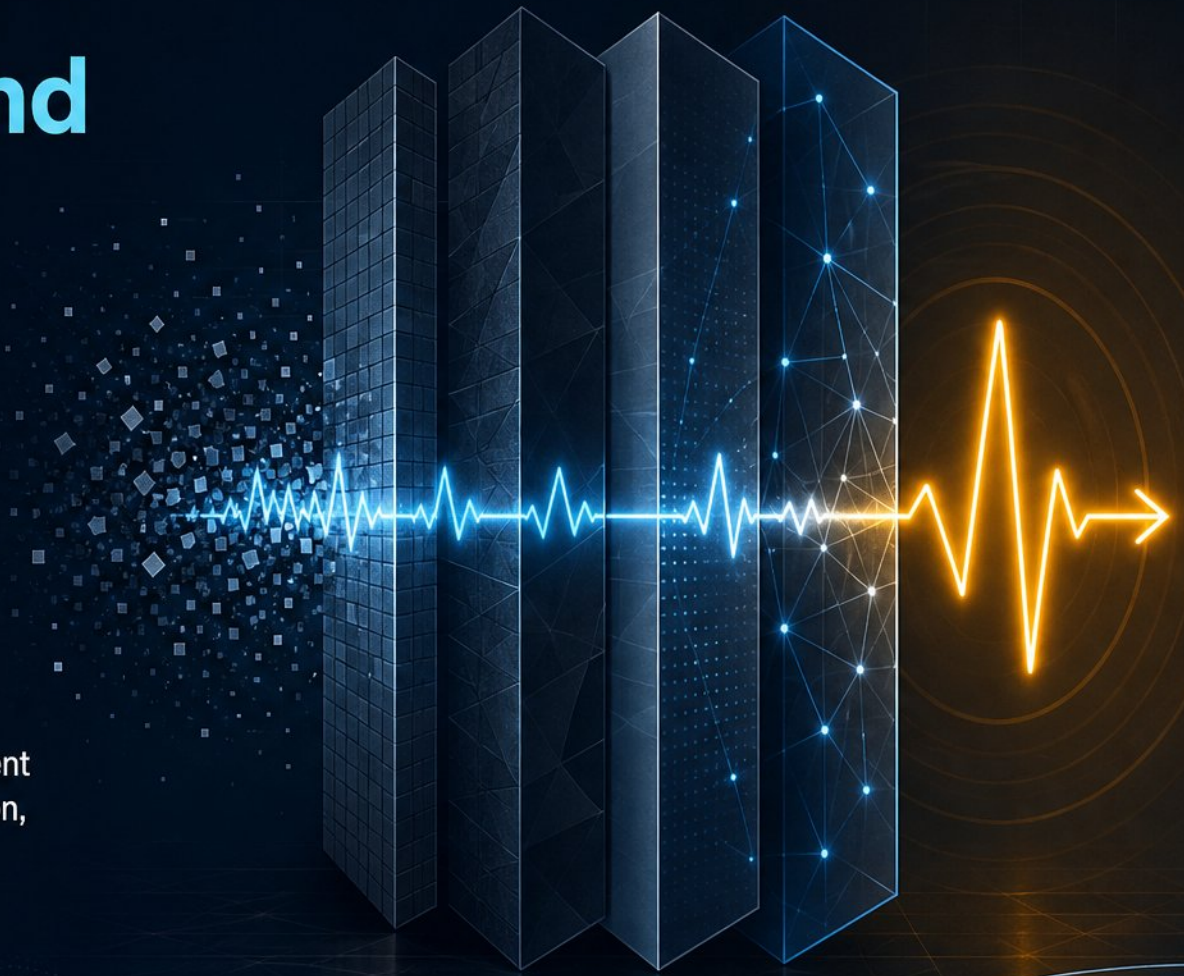
Security Awareness Metrics: Measurement and Interpretation

- Security awareness programs spend heavily, yet leaders report activity, not behavior change or risk reduction

- Metrics should signal human risk and program effect, not just LMS completion records

- Course arc: failure modes, measurement hierarchy, data, baselines, interpretation, reporting, improvement, maturity

- Shared vocabulary for security, compliance, and learning leaders: activity, engagement, learning, behavior, outcome



Why Awareness Measurement Often Fails

- Completion and click rates create false confidence
- Delivery ≠ ability to recognize, resist, or report attacks
- Low click rates hide untested users and high-impact risk
- Data silos block connecting training to behavior
- ISO 27001:2022 and NIST now demand behavior change evidence

From Activity Metrics to Behavior and Outcome Metrics

ACTIVITY METRICS

- Activity metrics: completions, assignments, attendance, attestations

BEHAVIORAL METRICS

- Behavioral metrics: reporting, time to report, credential submission, repeat risky actions, miss rate

OUTCOME METRICS

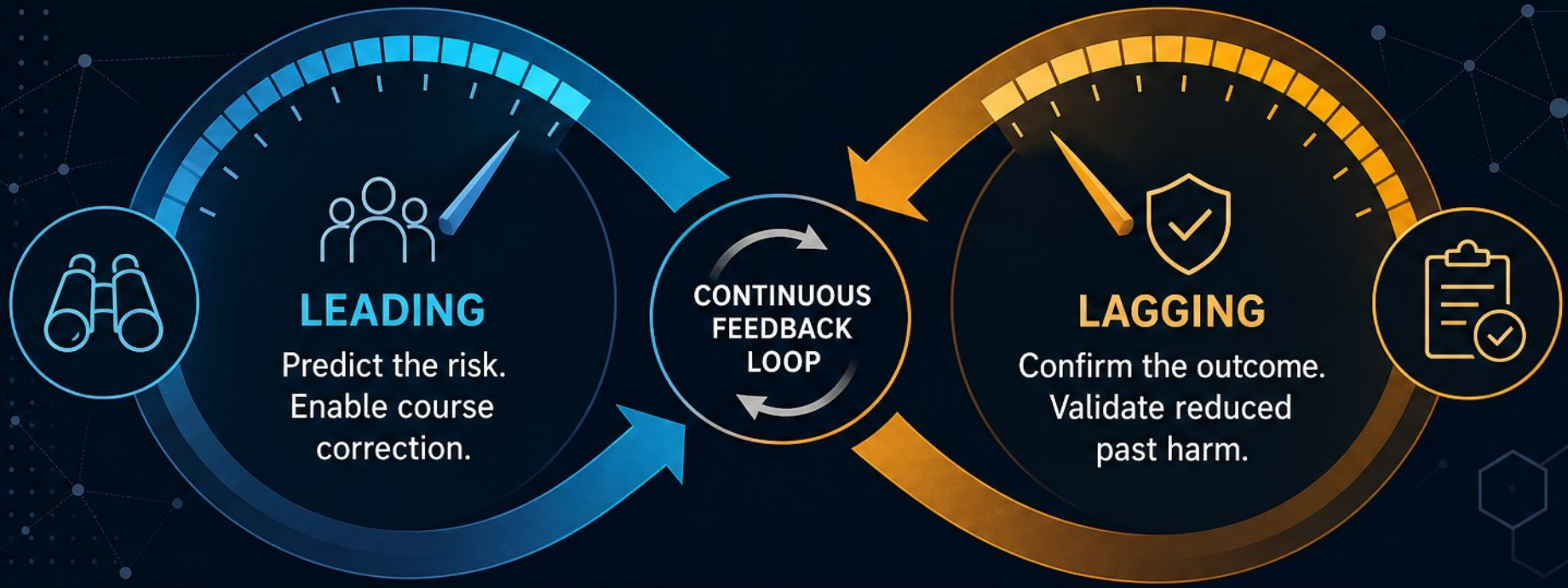
- Outcome metrics: incidents, dwell time, data-loss exposure, remediation results

– Completion remains useful for audits as an input, not the headline outcome

A Kirkpatrick-Based Measurement Hierarchy for Security Awareness

- Adapt four levels: reaction, learning, behavior, results
- Reaction: relevance; learning: knowledge and confidence
- Behavior: on-job application; results: reduced incidents
- Lower levels support, but don’t replace, higher evidence
- Knowledge shifts easier than behavior; measure both

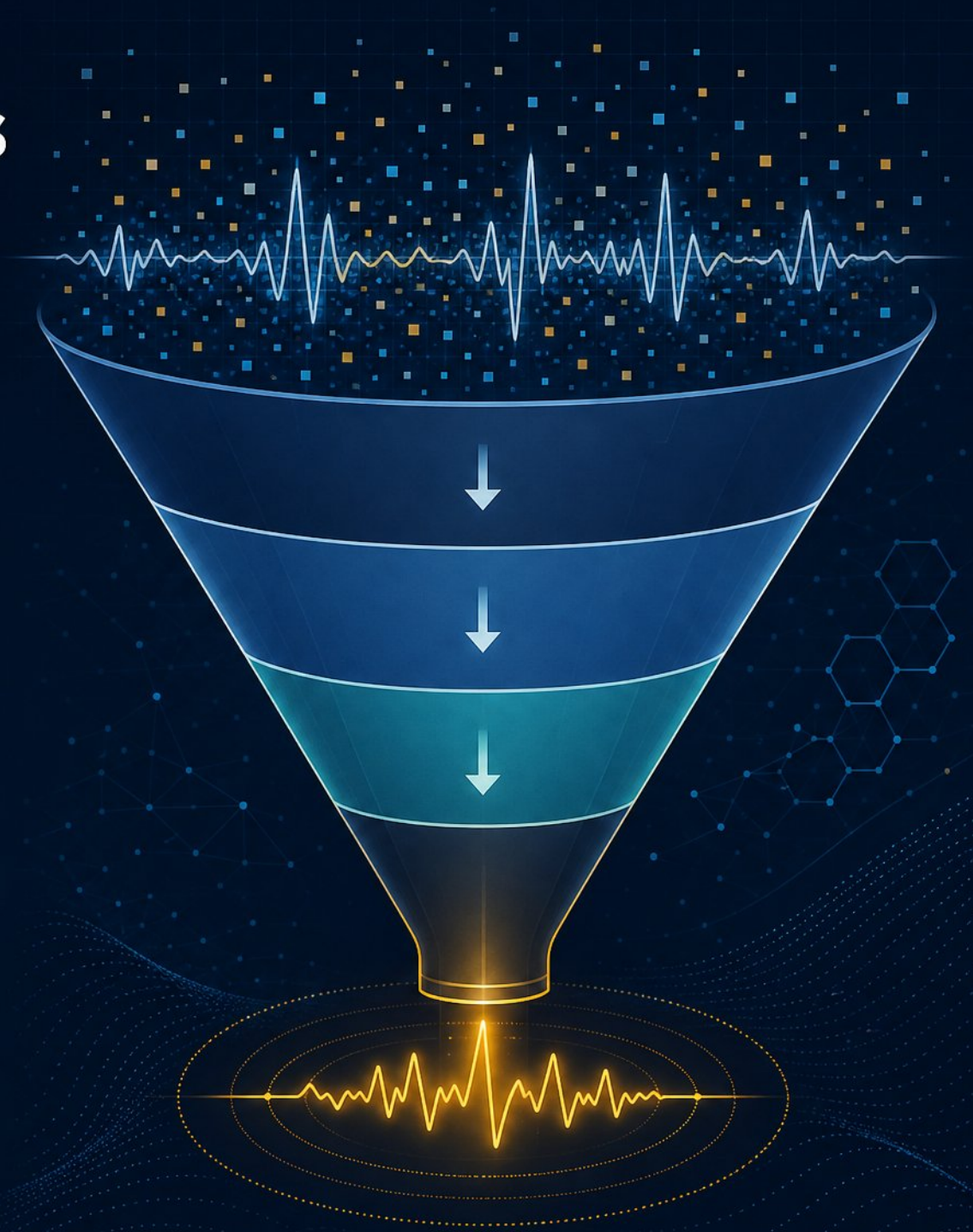
Leading and Lagging Indicators for Human Risk



- Leading indicators predict risk and enable course correction
- Reporting rate, time-to-report, and culture signals
- Lagging indicators confirm interventions reduced past harm
- Breach counts, quarterly click trends, repeat offenders
- Time-to-report predicts breach impact and proves training effect

Selecting Metrics That Matter

- Align metrics to top human risks and the behaviors that manage them
- Define purpose: diagnose, compare, predict, or prove value
- Start with a stable, small KPI set; retire ineffective metrics
- Balance quantitative signals with qualitative evidence
- Segment by role, privilege, and risk profile, not averages



Data Sources and Collection Challenges

- - Core sources: LMS, phishing platforms, surveys, DLP, help desk, SIEM, IAM, and endpoint logs
- - Assess data quality, freshness, ownership, and integration constraints
- - Standardize definitions and collection cadence across security, compliance, learning, and HR
- - Address privacy, ethics, and employment considerations for behavioral data
- - Watch for survivor bias: untested or non-engaging employees stay invisible

Building Baselines and Setting Realistic Targets

- Establish credible baselines before launching new interventions
- Combine unannounced simulations, knowledge assessments, and culture surveys
- Segment by role, risk, tenure, and contract status for fair comparisons
- Use segmented targets; high-privilege groups need stricter expectations
- Compare like with like: same difficulty, population, and metric definitions

Interpreting Trends and Avoiding False Conclusions

- Single simulations are weak evidence; repeated trends show true signal
- Beware confounders: simulation difficulty, timing, policy shifts, new tools
- Declining click rate may signal disengagement if reporting rates fall
- Require at least 30 employees per segment before drawing conclusions
- Compare against your own baseline, not misleading external benchmarks

DANGEROUS FALSE TREND

A drop may look like progress but hide a blind spot. Investigate before you conclude.

Reporting to Executives and Stakeholders

- Tailor views for security, compliance, and business audiences
- Translate data into business impact: exposure, detection speed, incident trends
- Use concise visuals with a short narrative on changes and next actions
- Present uncertainty and segmentation honestly, not a single green score
- Separate compliance evidence from behavioral evidence

Using Metrics to Drive Program Improvement

- Link metric shifts to training, simulation, and communication changes
- Build feedback loops across security ops, learning, and business units
- Experiment with targeted interventions to prove what works
- Prioritize fixess where human risk and business impact are highest
- Treat failures as teachable moments, not punitive events

Phishing, Reporting, and Repeat-Risk Metrics in Practice

- Track reporting rate and speed, not just failures
- Credential submission reveals higher-risk actions
- Miss rate uncovers silent non-participation
- Measure repeat offenders after coaching
- Resilience ratio balances reports against clicks

Privacy, Ethics, and Governance of Awareness Data

- Treat simulation outcomes and risk scores as employee data
- Restrict access and define a lawful purpose for monitoring
- Aggregate or anonymize when individual identification isn’t needed
- Document definitions, owners, review cadence, and decision triggers
- Keep simulation failures out of employment scorecards without HR review

Maturity, Governance, and Next Steps

- Compliance-driven completion tracking is the baseline
- Progress through behavior change to culture and resilience
- Assign clear roles, owners, and review cadences
- Build phased roadmap: baselines, KPIs, executive reporting
- Embed metrics within broader human risk governance

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/10878118/public