

Cybersecurity Awareness

Transformation Program

Representative Consulting Scenario

Prepared for: ShopNow Digital

Prepared by: Mustafa Alobaidy

Senior GRC & Cybersecurity Awareness Consultant

March 2026

Table of Contents

1. Executive Summary
2. Human Risk Landscape
3. Security Culture Assessment
4. Awareness Program Strategy
5. Training Framework
6. Phishing Simulation Program
7. Metrics & Reporting
8. Continuous Improvement Model

1. Executive Summary

ShopNow Digital, a leading e-commerce platform with 220 employees operating on Microsoft Azure infrastructure, has engaged Mustafa Alobaidy, Senior GRC & Cybersecurity Awareness Consultant, to design and implement a comprehensive Cybersecurity Awareness Transformation Program. This initiative addresses the critical human element of cybersecurity, recognizing that over 90% of successful cyber attacks involve human error or social engineering.

As an e-commerce platform processing millions of transactions and handling sensitive customer PII and payment data, ShopNow Digital faces significant risks from phishing, business email compromise, and insider threats. This program aims to transform security awareness from an annual compliance checkbox into a continuous behavioral change initiative that builds a security-conscious culture across the organization.

Program Objectives

- Reduce phishing susceptibility from 32% to below 5% within 12 months
- Achieve 100% security awareness training completion across all employees
- Build a measurable security culture with defined behavioral indicators
- Establish role-based training tracks aligned with job responsibilities
- Implement continuous learning through monthly micro-training and simulations

Key Deliverables

Deliverable	Description
Security Culture Assessment	Baseline measurement of current security culture maturity
12-Month Awareness Calendar	Structured program of training, campaigns, and simulations
Role-Based Training Curriculum	Customized training tracks for different employee groups
Phishing Simulation Program	Progressive complexity phishing campaigns with remediation
Executive Dashboard	Monthly reporting on human risk metrics and program effectiveness
Gamification Platform	Employee engagement through leaderboards and rewards

2. Human Risk Landscape

Understanding the human risk landscape is essential for designing an effective awareness program. The following analysis examines threat vectors, employee demographics, and historical incident data to inform program design and prioritization.

2.1 Threat Analysis

Threat Vector	Risk Level	Description
Phishing Attacks	High	Primary initial access vector; 65% of attempts target employees via email
Business Email Compromise	High	CFO/Finance team targeted; \$180K loss in past 18 months
Social Engineering	Medium	Phone-based pretexting; vendor impersonation attempts
Insider Threat (Unintentional)	Medium	Data handling errors; shadow IT; unsecured file sharing
Credential Theft	High	Password reuse; weak passwords; credential stuffing attacks
Physical Security	Low	Tailgating; unauthorized access; clean desk violations

2.2 Employee Demographics

Department	Headcount	% of Workforce	Risk Factors
Executive Leadership	12	5%	High-value targets; board reporting; strategic decisions
Finance & Accounting	18	8%	Payment processing; wire transfers; financial data
Customer Service	45	20%	Customer PII access; high email volume; social engineering targets
Engineering/IT	68	31%	System access; code deployment; privileged access
Marketing & Sales	35	16%	External communications; third-party tools; data sharing
Operations & Logistics	28	13%	Vendor interactions; shipping data; inventory systems
Human Resources	14	6%	Employee PII; recruiting; onboarding processes

2.3 Historical Incident Analysis

Incident Type	Count (12 months)	Impact/Notes
Successful Phishing Clicks	156	32% of workforce clicked at least once
Credentials Compromised	23	Requiring password resets and account remediation
BEC Attempts	12	3 successful, resulting in \$180K financial loss
Data Handling Incidents	34	Sensitive data sent to wrong recipients

Cybersecurity Awareness Transformation Program

Shadow IT Discoveries	45	Unauthorized SaaS applications with company data
Physical Security Violations	18	Tailgating, propped doors, clean desk violations

3. Security Culture Assessment

A comprehensive security culture assessment was conducted using the Security Culture Framework methodology, evaluating seven dimensions of organizational security culture. This baseline assessment enables measurement of program effectiveness over time.

3.1 Culture Dimension Scores

Dimension	Current Score	Target Score	Observations
Attitudes	2.5	4.0	Employees view security as IT's responsibility; limited personal accountability
Behaviors	2.2	4.0	Inconsistent security practices; risky behaviors observed
Cognition	2.8	4.0	Basic awareness of threats; limited understanding of impact
Communication	2.0	3.5	Security messaging infrequent; not engaging or memorable
Compliance	3.0	4.0	Policy awareness exists; enforcement inconsistent
Norms	2.3	4.0	Security not embedded in team culture; peer influence limited
Responsibilities	2.5	4.0	Role responsibilities unclear; security ownership undefined
OVERALL SCORE	2.5	4.0	Developing security culture with significant improvement opportunity

3.2 Key Culture Gaps

- Leadership Visibility: Security messaging from executives is rare; no visible security sponsorship
- Peer Influence: No security champions program; limited peer-to-peer security conversations
- Recognition: No rewards or recognition for positive security behaviors
- Feedback Loop: Employees don't see outcomes of security incidents or near-misses
- Integration: Security not embedded in onboarding, performance reviews, or team meetings

4. Awareness Program Strategy

The Cybersecurity Awareness Transformation Program employs a multi-modal approach combining formal training, experiential learning, continuous reinforcement, and cultural embedding. The strategy is built on behavioral science principles to drive lasting behavioral change.

4.1 Program Pillars

Pillar	Components	Objective
1. Education	Formal training, e-learning, micro-learning modules	Knowledge transfer and skill building
2. Simulation	Phishing campaigns, social engineering tests, tabletop exercises	Experiential learning and risk identification
3. Communication	Newsletters, posters, videos, executive messaging	Continuous reinforcement and top-of-mind awareness
4. Engagement	Gamification, competitions, security champions	Motivation and peer influence
5. Measurement	Metrics, dashboards, culture surveys	Program effectiveness and continuous improvement

4.2 12-Month Awareness Calendar

Month	Theme	Key Activities
Month 1	Program Launch	Baseline phishing test; mandatory security fundamentals training; executive kickoff message
Month 2	Phishing Awareness	Phishing identification training; email security tips; simulated phishing campaign
Month 3	Password Security	Password hygiene training; MFA enrollment drive; password manager rollout
Month 4	Social Engineering	Social engineering awareness; phone-based pretexting simulation; verification procedures
Month 5	Data Protection	Data classification training; secure file sharing; PII handling procedures
Month 6	Mid-Year Assessment	Culture survey; phishing simulation; progress review; program adjustments
Month 7	Remote Work Security	Home network security; VPN usage; secure collaboration tools
Month 8	Incident Reporting	Reporting procedures; near-miss program launch; security hotline awareness
Month 9	Third-Party Risk	Vendor security awareness; supply chain threats; due diligence for business users
Month 10	Physical Security	Clean desk policy; visitor management; tailgating prevention
Month 11	Holiday Security	Travel security; gift card scams; increased phishing awareness
Month 12	Year-End Review	Comprehensive assessment; awards ceremony; program renewal planning

Cybersecurity Awareness Transformation Program

5. Training Framework

The training framework provides role-based curricula tailored to different employee groups, ensuring relevant content that addresses specific risks and responsibilities. Training is delivered through multiple modalities to accommodate different learning styles.

5.1 Training Tracks

Audience	Track Name	Duration	Frequency	Key Topics
All Employees	Security Fundamentals	60 min	Annual + monthly micro-learning	Phishing, passwords, data handling, incident reporting
New Hires	Security Onboarding	90 min	First week of employment	Policies, tools, security culture, reporting procedures
Customer Service	Customer Data Protection	45 min	Quarterly	PII handling, social engineering, verification procedures
Finance Team	Financial Fraud Prevention	60 min	Quarterly	BEC awareness, wire transfer verification, invoice fraud
Engineering/IT	Secure Development & Operations	90 min	Quarterly	Secure coding, privileged access, change management, incident response
Managers	Security Leadership	60 min	Bi-annual	Team security culture, policy enforcement, incident escalation
Executives	Executive Cyber Risk	45 min	Quarterly	Whale phishing, board reporting, strategic risk decisions

5.2 Training Delivery Methods

Method	Platform/Format	Description
E-Learning Modules	KnowBe4 / Proofpoint	Self-paced online courses with knowledge checks
Micro-Learning	Mobile-friendly short videos	3-5 minute weekly reinforcement content
Live Workshops	In-person/virtual instructor-led	Role-specific deep-dives and Q&A sessions
Simulations	Phishing, vishing, physical tests	Experiential learning with immediate feedback
Just-in-Time Training	Triggered by risky behavior	Targeted remediation after failed simulations

5.3 Training Content Topics

Topic	Priority	Sub-Topics
Phishing & Social Engineering	Critical	Email phishing, spear phishing, vishing, smishing, pretexting
Password & Authentication	Critical	Password hygiene, MFA, password managers, credential theft

Cybersecurity Awareness Transformation Program

Data Protection	High	Data classification, PII handling, secure file sharing, data disposal
Email Security	High	BEC awareness, suspicious email identification, email encryption
Mobile & Remote Security	High	BYOD security, public WiFi, VPN usage, home network security
Physical Security	Medium	Clean desk, visitor management, tailgating, secure printing
Incident Reporting	High	Reporting procedures, near-miss reporting, escalation paths
Compliance & Policy	Medium	Policy awareness, regulatory requirements, acceptable use

6. Phishing Simulation Program

The phishing simulation program provides experiential learning through realistic simulated attacks, enabling employees to practice identifying and reporting threats in a safe environment. The program uses progressive complexity to continuously challenge and improve employee resilience.

6.1 Simulation Campaign Schedule

Month	Campaign Name	Difficulty	Scenario	Target Group	Objective
Month 1	Baseline Assessment	Low	Generic vendor invoice	All Employees	Establish baseline metrics
Month 2	Credential Harvest	Low	Password reset request	All Employees	Test credential submission behavior
Month 3	Brand Impersonation	Medium	Microsoft 365 notification	All Employees	Test brand trust exploitation
Month 4	Vishing Campaign	Medium	IT support call	Customer Service	Voice-based social engineering
Month 5	Spear Phishing	Medium	Personalized executive request	Finance Team	Targeted attack simulation
Month 6	Multi-Vector	High	Email + SMS combination	All Employees	Test multi-channel awareness
Month 7	Attachment-Based	Medium	PDF invoice with macro	Finance/Operations	Test attachment handling
Month 8	Current Events	Medium	News-jacking theme	All Employees	Test emotional manipulation
Month 9	Executive Impersonation	High	CEO wire transfer request	Finance Team	BEC simulation
Month 10	Supply Chain	High	Vendor compromise scenario	Operations	Third-party threat awareness
Month 11	Holiday Themed	Medium	Gift card scam	All Employees	Seasonal threat awareness
Month 12	Final Assessment	High	Advanced multi-stage	All Employees	Measure annual improvement

6.2 Simulation Response Framework

Behavior	Classification	Response/Remediation
Report Phishing	Excellent	Recognition in newsletter; points for gamification; reinforcement of correct behavior
No Interaction	Acceptable	No action required; counted as neutral response
Click Link Only	Requires Attention	Immediate just-in-time training (5 minutes); manager notification
Submit Credentials	High Risk	Extended remediation training (15 minutes); tracked for repeat behavior
Repeat Failure (3+)	Critical	One-on-one coaching; additional targeted training; performance discussion

6.3 Technical Infrastructure

Component	Tool/Platform	Purpose
Simulation Platform	KnowBe4 or Proofpoint Security Awareness	Campaign creation, delivery, and tracking
Email Integration	Microsoft 365 integration	Realistic delivery; Phish Alert Button for reporting
Reporting Dashboard	Real-time analytics	Click rates, report rates, department comparisons
LMS Integration	Azure AD SSO	Automated training assignment; completion tracking

7. Metrics & Reporting

A comprehensive metrics framework enables measurement of program effectiveness, identification of areas requiring attention, and demonstration of return on investment. Metrics are reported at multiple levels to serve different stakeholder needs.

7.1 Key Performance Indicators

KPI	Baseline	Target	Description
Phishing Click Rate	32%	< 5%	Percentage of employees who click simulated phishing links
Phishing Report Rate	8%	> 70%	Percentage of employees who report simulated phishing
Training Completion Rate	72%	100%	Percentage of required training completed on time
Time to Complete Training	14 days avg	< 7 days	Average time from assignment to completion
Knowledge Assessment Score	68%	> 85%	Average score on post-training assessments
Security Culture Score	2.5/5.0	4.0/5.0	Aggregate score from culture survey
Incident Report Volume	12/month	> 30/month	Employee-reported security concerns (higher is better)
Repeat Offender Rate	18%	< 3%	Employees failing multiple simulations

7.2 Reporting Structure

Report	Frequency	Audience	Content
Executive Dashboard	Monthly	CISO, Executive Committee	High-level KPIs, trends, risk summary, program ROI
Department Reports	Monthly	Department Managers	Team-specific metrics, comparisons, action items
Campaign Reports	Per Campaign	Security Team	Detailed campaign results, click analysis, remediation status
Culture Assessment	Quarterly	All Stakeholders	Culture dimension scores, trends, improvement areas
Annual Report	Yearly	Board of Directors	Program outcomes, risk reduction, investment summary

7.3 ROI Calculation Framework

Benefit Category	Calculation Method	Estimated Value
Breach Prevention	Cost of average breach (\$4.5M) × Probability reduction	Estimated: \$450,000 annually
Incident Reduction	Reduction in incidents × Average incident cost	Estimated: \$125,000 annually
Productivity	Reduced time spent on security incidents	Estimated: \$75,000 annually
Compliance	Avoided regulatory fines and audit findings	Estimated: \$50,000 annually

Cybersecurity Awareness Transformation Program

Total Estimated Benefit	Sum of quantified benefits	\$700,000 annually
Program Investment	Platform, content, personnel, administration	\$180,000 annually
Net ROI	$\text{Benefit} - \text{Investment} / \text{Investment}$	289% ROI

8. Continuous Improvement Model

The program employs a continuous improvement model based on Plan-Do-Check-Act (PDCA) methodology, ensuring the program evolves to address emerging threats, changing workforce dynamics, and lessons learned from ongoing operations.

8.1 PDCA Cycle Application

Phase	Frequency	Activities
Plan	Quarterly	Review threat landscape; analyze metrics; identify improvement areas; plan upcoming campaigns and training
Do	Ongoing	Execute training programs; deliver simulations; run communication campaigns; engage champions
Check	Monthly	Measure KPIs; analyze trends; gather feedback; assess culture; benchmark against targets
Act	Quarterly	Adjust content; refine targeting; update procedures; implement lessons learned; escalate issues

8.2 Security Champions Program

A network of Security Champions embedded across departments amplifies the awareness program, providing peer-to-peer influence and localized security advocacy.

Element	Details
Selection	1 champion per 15-20 employees; nominated by managers; voluntary participation
Training	Advanced security training; monthly champion briefings; early access to threats
Responsibilities	Peer coaching; local security ambassador; feedback collection; event support
Recognition	Quarterly recognition awards; professional development opportunities; visible leadership role
Support	Monthly meetings with security team; dedicated communication channel; resource library

8.3 Gamification & Engagement

Element	Description
Individual Points	Points earned for training completion, reporting phishing, passing simulations
Department Leaderboard	Monthly rankings based on aggregate department performance
Badges & Achievements	Visual recognition for milestones (e.g., 'Phishing Hunter', 'Security Champion')
Quarterly Competitions	Department challenges with prizes for top performers
Annual Awards	Security Awareness Champion of the Year; Most Improved Department; Executive Recognition

8.4 Program Governance

Role	Responsibility	Function
Program Sponsor	CISO	Executive accountability; resource allocation; strategic direction
Program Manager	Security Awareness Lead	Day-to-day operations; vendor management; content development
Steering Committee	Cross-functional leaders	Quarterly review; strategic input; organizational alignment
Champions Network	Department representatives	Local execution; feedback; peer influence

This Cybersecurity Awareness Transformation Program provides ShopNow Digital with a comprehensive framework for addressing human risk, building a security-conscious culture, and measurably reducing susceptibility to social engineering attacks. With committed leadership, consistent execution, and continuous improvement, the organization will achieve significant behavioral change and enhanced security resilience within the 12-month program timeline.