JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(3), 2684-2692
ISSN: 2589-1316

Shield-Aware: A Practical Roadmap to Elevate SME Cyber Readiness in Line with Saudi Vision 2030

Abdalilah Alhalangy[1*], Khidir Shaib Mohamed[2*], Saleh Abdulrahman Alkhamis[3]

[1] *Department of Computer Engineering, College of Computer, Qassim University, Buraydah, SAUDI ARABIA, a.alhalangy@qu.edu.sa, ORCID: https://orcid.org/0000-0003-2735-8208*
[2] *Department of Mathematics, College of Sciences, Qassim University, Buraydah, SAUDI ARABIA, k.idris@qu.edu.sa, ORCID: https://orcid.org/0000-0001-8309-6121*
[3] *Department of Cybersecurity, College of Computer, Qassim University, Buraydah, SAUDI ARABIA, Khmiess@qu.edu.sa*

*Corresponding Author: a.alhalangy@qu.edu.sa, k.idris@qu.edu.sa

Citation: Alhalangy, A., Mohamed, K. S., Alkhamis, S. A. (2025). Shield-Aware: A Practical Roadmap to Elevate SME Cyber Readiness in Line with Saudi Vision 2030, *Journal of Cultural Analysis and Social Change*, 10(3), 2684-2692. https://doi.org/10.64753/jcasc.v10i3.2825

Published: December 04, 2025

ABSTRACT

Saudi Arabia's rapid digitalization has increased exposure to cyber risks across individuals, organizations, and SMEs. This study consolidates fragmented local evidence into a practical national framework ("Shield-Aware") that couples security awareness and behavior with regulatory compliance (ECC-1:2018). We employed an evidence-synthesis methodology: coding quantitative and behavioral findings from Saudi studies and a national dataset (N=1,230), then operationally mapping them to ECC-1:2018 domains to design measurable intervention packages and a monitoring dashboard. The findings reveal recurring individual gaps (public Wi-Fi use, weak/password reuse, limited phishing literacy), demographic disparities in awareness, and shortfalls in policy and periodic training within some organizations—especially SMEs. Shield-Aware prescribes multilevel interventions: microlearning, phishing simulations, and 2FA enablement for individuals; enforceable policies, role-based training, and compliance monitoring for organizations; and lightweight ECC readiness checks and enablement pathways for SMEs at the governance layer. The framework delivers dual scientific and practical impact: it translates awareness/behavior indicators into measurable, actionable decisions and provides a direct operational alignment with ECC-1:2018 controls—ultimately strengthening national cyber readiness and supporting Vision 2030 priorities.

Keywords: Cybersecurity Awareness; Security Behavior; ECC-1:2018; Phishing Simulations; SMEs; Saudi Arabia; Vision 2030

INTRODUCTION

Saudi Arabia's fast-paced digital transformation and the expansion of remote/hybrid work have enlarged the attack surface and sharpened the "human factor" as a determinant of enterprise cyber resilience. A Saudi empirical study of digital workplaces in the post-pandemic era shows that password/email management, policy support, and periodic training are pivotal to translating awareness into routine secure behaviors [1], aligning with Vision 2030 priorities for a digitized economy and services [2]. At the governance layer, the National Cybersecurity Authority (NCA) established the Essential Cybersecurity Controls (ECC-1:2018) as a mandatory baseline for organizations. In 2024, the Authority updated the framework and announced ECC-2:2024 as an assessment/compliance tool, signaling policy evolution to match a changing threat landscape and national transformation goals [3,4]. The NCA's 2024 sectoral reporting further evidences the growth and maturation of the Saudi cybersecurity ecosystem [5].

Local evidence reveals salient gaps in individual awareness and behavior: in a representative survey (N=1230), 31.7% used public Wi-Fi, 51% created passwords from personal data, 32.5% had no idea about phishing, and 21.7% had suffered cybercrime with low reporting (~29.2%) [6,7]. Among female secondary school students in Eastern Makkah, social media usage approached universality (~98%), alongside weak password-update and incident-response practices [8]. Saudi Arabia's work on social media security awareness also documents gender-linked differentials, motivating context-sensitive interventions [9]. Inside organizations, Saudi evidence indicates that employees do not consistently perceive all security constructs (e.g., infrastructure/email management) as critical, creating behavioral gaps that require enforceable policies and periodic refreshers [1]. In the private sector, a survey of approximately 230 IT managers reported under-investment, reliance on outsourcing, and uneven risk perception for the coming year [10]. For SMEs, a practical, cost-aware route is to align interventions with the ECC and leverage Monsha'at programs, especially the Thakaa Center (AI, data, IoT, and cybersecurity), to accelerate maturity [11].

Despite this momentum, measurement tools and study designs remain heterogeneous and mostly cross-sectional, limiting causal inference. A recent Saudi study calls for simplified, locally applicable awareness frameworks and actionable mechanisms that fuse training, phishing simulation, and lightweight governance into institutional routines [12], complemented by vision-aligned knowledge-sharing initiatives to scale capacity [13]. Therefore, this paper proposes "Shield-Aware 2030," a unified, measurable framework that binds local behavioral evidence to national compliance requirements, mapping interventions across individual/organizational/governance levels in line with Vision 2030.

RELATED WORK

Taxonomy of Prior Work

1. ***Individual Awareness and Behavior (National)***
   A representative survey (N=1,230) reported risky practices (public Wi-Fi, passwords from personal data, limited phishing literacy) with a gap between victimization and reporting; the companion dataset documented the instrument/sample, providing a national baseline [6,7].
2. ***Youth/Students (Educational Settings)***
   Among female secondary school students in Eastern Makkah, social media use was near-universal (~98%), while password updates and incident response were weak, supporting age-and gender-sensitive programs [8].
3. ***Social Media Security Awareness:***
   Saudi studies show gender-linked differentials and emphasize sustained education against phishing, malicious links, and social engineering on platforms [9].
4. ***Digital Workplaces and Employee Behavior:***
   A Saudi empirical study showed that converting awareness into repeatable secure behavior requires enforceable policies, organizational support, and periodic training; some constructs (e.g., email/infrastructure management) are not consistently perceived as critical by employees [1].
5. ***Private Sector***/SMEs ***and Governance:***
   A survey of approximately 230 Saudi IT managers indicated under-investment, outsourcing reliance, and uneven risk expectations [9]. At the national level, the NCA set ECC-1:2018 as the minimum baseline and, in 2024, introduced updates, including ECC-2:2024 for assessment/compliance, with SME enablement via Monsha'at/Thakaa (AI/Data/IoT/Cybersecurity) [3,4, 11].
6. ***National Awareness Framework:***
   Recent Saudi studies propose awareness frameworks and call for simplified measurements tied to institutional KPIs and Vision-aligned knowledge sharing [12, 13].

Critical Discussion & Limitations

1. Predominantly cross-sectional designs: descriptive surveys with limited causal inference or longitudinal tracking of post-intervention behavior change [6, 8, 9].
2. Heterogeneous tools; weak compliance mapping: behavioral indicators are rarely mapped to ECC controls or national compliance tooling (e.g., ECC-2:2024) [3,4].
3. SME enablement gap: lack of ready-to-deploy SME packages combining microlearning dosage, phishing simulation, and lightweight governance checklists [10, 11].
4. Demographic/context disparities: Age, gender, and context differences demand tailored content, channels, and cadences [8,9].

5. Limited operational impact metrics: heavy focus on knowledge/attitudes over operational KPIs (phish-sim fall rates, time-to-report, 2FA activation) [6, 12].

Our Contribution Vs Prior Work

1. Unifying measure→decision→action: compact formulas (risk RRR, dosage MMM, impact SSS) plus a 90-day KPI loop to convert measurements into actionable policies.
2. National alignment and SME enablement: bundles mapped to ECC-1:2018/ECC-2:2024 with lightweight checklists; leverage NCA and Monsha'at/Thakaa to cut cost and time-to-maturity [3,4, 11].
3. Context sensitivity: tailored micro-learning and phish-sim cadences; youth/education-targeted modules for observed disparities [8,9].
4. Vision-2030 consistency: moving from individual awareness metrics to measurable compliance/operational outcomes that support a secure digital economy [2,4, 5,13]

METHODS AND MATERIALS

Study Design

We conducted an evidence synthesis and secondary analysis of Saudi datasets and then engineered an operational framework that maps behavioral indicators to ECC controls in alignment with Vision 2030. Three phases:

1. Extraction and double-coding of Saudi studies on individuals and workplaces (target Cohen's $\varkappa \geq 0.80$) [1] and the national dataset (N=1,230) [6,7].
2. Compliance mapping to ECC domains (governance/defense/resilience/third-party and cloud/ICS) using ECC-1:2018 and the 2024 updates, including ECC-2:2024 assessment tooling [3,4].
3. Operational recipes (risk thresholds, dosage, 90-day KPI loop) tailored to SMEs using national enablement programs (Monsha'at/Thakaa). [11].

Data Sources

1. National individual-level dataset (N=1,230): documented measures of risky practices, awareness, and reporting, serving as a national baseline [6, 7].
2. Digital workplaces: Saudi empirical evidence on policy/training/organizational support shaping employee behavior [1].
3. Private sector: Survey of ~230 IT managers on awareness/spend/outsourcing [10].
4. Governance and enablement: NCA documentation/updates on ECC (2018, 2024) and SME enablement programs (Monsha'at/Thakaa) [3,4, 11].

Variable Definitions

$$\text{Behavior index} \quad B \in [0,100]$$

$$B = \frac{1}{3}\ (P_{wifi}+P_{wifi}+P_{wifi})X100$$

$$Policy - practice\ gap\ E\ \in [0,100]: P = \ (1 - A_{2FA})X100$$

$$Exposure\ index\ E\ \in [0,100]: E = \ (W_r R_{remot}+Wr\ S_{sensitivity}) + W_0 O, \sum W = 100$$

3.3 Computation and operational formulas

$$R = 0.40B\ +\ 0.35P\ \ +0.25E, \qquad M = [\gamma R/20],\ \gamma \in [1,1.5]$$

$$S = 0.2A_{2FA} + 0.3IR + (PP - 1)0.5$$

$$\begin{cases} R \geq 70 \\ R < 70 \geq 40 \\ R < 40 \end{cases} \qquad \begin{cases} 95\% \\ 90\% \\ 80\% \end{cases} = TA_{2FA}(R)$$

$$CI\ = \frac{\hat{p}\ +\ z^2/(2n)\ \pm\ z \cdot \sqrt{(\ \hat{p}(1-\hat{p})/n\ +\ z^2/(4n^2)\ )}}{1\ +\ z^2/n}$$

$$z\ =\ 1.96\ ,\ \hat{p}\ =\ x/n$$

Pooling & heterogeneity: Freeman–Tukey double-arcsine transformation and I^2 $+\beta_2$ $+\beta_1 R$ $+\beta\alpha$ = logit(p) Predictive modeling (optional): logistic regression β_3 (exposure)

Statistical Analysis, Software, And Ethics

- ***Software:*** Python 3.11 (Pandas, NumPy, StatsModels, matplotlib).
- ***Significance:*** α=0.05; report estimates with 95% CIs.

- ***Reproducibility:*** The formulas and parameters above enable replication; dosages and thresholds are reviewed on a 90-day cycle.
- ***Ethics:*** secondary analysis of published, anonymized data [5,6]; no direct human subject interaction.
- ***Compliance Alignment:*** KPI dashboard mapped to ECC domains per ECC-1:2018 and 2024 updates (ECC-2:2024) [3,4], with SME enablement via Monsha'at/Thakaa [11].

PROPOSED FRAMEWORK

Aim and Design Principles

Shield-Aware 2030 operationalizes Saudi evidence on cybersecurity awareness and behavior into repeatable ECC-aligned interventions. The framework is simple, applicable, and measurable, spanning three layers.

1. Individual (end-users),
2. Organization (policies, training, controls),
3. Governance/SMEs (lightweight compliance and enablement).

Guiding principles: (i) measurement-to-action, (ii) risk-tiering with explicit thresholds, (iii) 90-day improvement loops, (iv) alignment with ECC-1:2018 (and assessment tools), and (v) context sensitivity across cohorts and sectors.

Measurement Stack

We collected a minimal set of indicators and computed three indices:

- Behavior index $B \in [0,100]$: prevalence of risky practices (e.g., public Wi-Fi use, weak/password-reuse, limited phishing literacy).
- Policy–practice gap $P \in [0,100]$: lack of 2FA activation and incomplete adherence to baseline policies.
- Exposure index $E \in [0,100]$: remote-work share, data sensitivity, and operational exposure, with weights $Wr, Ws, Wo \; and \; Wr + Ws + W0 = 100$
- Unified risk score

$$R = 0.40\,B + 0.35\,P + 0.25\,E.$$

All proportions were reported with Wilson 95% CIs; optional pooling used Freeman–Tukey transformation with $I^2$for heterogeneity.

Decision Policy: Risk Tiers and Targets

The risk tiers guide the bundle selection as follows:

- High: $R \geq 70$
- Moderate: $40 \leq R < 70$
- Low: $R < 40$

A piecewise 2FA target enforces a minimum control strength.

$$T2FA(R) = \begin{cases} 95\% & R \geq 70 \\ 90\% & 40 \leq R < 70 \\ 80\% & R < 40 \end{cases}$$

Intervention Dosage and Content

Training Dosage (per 90-day Cycle)

$$M = \lceil \gamma \;\; 20/R \rceil \;, \qquad \Gamma \in [1,1.5]$$

Bundle components (mapped to ECC domains):

- ***Technical and Policy Controls:*** default 2FA, password manager rollout, password policy enforcement, email/SaaS access policy, and incident-reporting SOPs. (ECC: Defense, Governance).
- Behavioral enablers include micro-learning (5–7 min units), phishing simulations (tiered cadence: monthly/quarterly/semiannual), and role-based training. (ECC: Defense and Resilience).
- ***Governance and Assurance***: lightweight ECC checklists, third-party/cloud hygiene prompts, KPI reviews. (ECC: Governance, Third Party/Cloud, Resilience).

Risk-tier recipes:

- High R: $M \geq 4$ units/quarter; monthly phish-sim; 2FA=95%; immediate password manager adoption; targeted coaching for high-risk roles.
- Moderate R: $M = 2 - 3$; quarterly phish-sim; 2FA=90%; policy refresh and nudges.
- Low R: $M = 1 - 2$; semiannual phish-sim; 2FA=80%; sustainment content and spot checks.

Impact and Kpis

Track operational indicators and a composite impact index

- **PP**: phishing-simulation fall rate (↓ better).
- **IR**: incidents reported within 24h (↑ better).
- $\mathbf{A_{2FA}}$ share of active accounts with 2FA (↑ better).

Impact index

$$S = 0.5(1 - PP) + 0.3IR + 0.2A2FA$$

Targets are reviewed every **90 days**; success criteria can be specified as $\Delta S \geq 0.100$ per cycle or achievement of $T_{2FA}(R)$

Governance Alignment and SME Enablement

- Provide ECC-aligned checklists and a readiness ramp (current state → minimum compliance → continuous improvement).
- Leverage NCA resources and Monsha'at/Thakaa programs to reduce costs and time-to-baseline.
- Maintain a KPI dashboard at the entity level (PP, IR, A_{2FA}A, S) and integrate it with internal audit/risk reviews.

Segmentation And Equity

- Youth/education: game-based microlearning, platform-specific phishing cues, guardian/teacher toolkits.
- Older adults: accessibility-first content, slower cadence, scenario-based rehearsals, assisted setup for 2FA, and password managers.
- Sector tailoring: health, education, and finance modules emphasizing domain-specific threats and governance obligations.

Operating Cadence and Reproducibility

- 90-day loop: Assess R → Decide (tier/bundle) → Act (deliver M, controls, phish-sim) → Measure (PP, IR, A_{2FA}, S) → Improve.
- Protocol: identify sources → extract → double-code (Cohen's K) → analyze → map to ECC → publish dashboard.
- Documentation: All formulas and thresholds are explicit to facilitate replication and controlled evaluations (RCTs or stepped-wedge designs).

One-Page Implementation Checklist

1. Enable default 2FA and deploy a password manager organization-wide.
2. Baseline B,P,E, and compute R; select tier.
3. Schedule M microlearning units and phishing simulations per tier.
4. Stand up the KPI dashboard with PP, IR, A_{2FA}, and S; review at day 90.
5. For SMEs: run the ECC checklist; enroll in NCA/Monsha'at/Thakaa enablement; iterate to baseline, and then improve.

This framework provides a fast, low-overhead path to immediately reduce targetable risks (phishing, password hygiene, under-reporting) while establishing a rigorous, ECC-aligned scaffold for sustained organizational resilience.

RESULTS

This section presents descriptive outcomes only; detailed interpretation is deferred to the Discussion section. Proportions were reported with Wilson's 95% confidence intervals. The total sample (N=1,230) was assessed using the national four-pillar instrument (awareness, risky practices, cyber-crime exposure, and reporting).

Key Proportions (Primary Indicators)

Table 1. Point estimates and Wilson 95% CIs (source: national dataset; see [6,7] in the References).

Indicator (definition)	(x)	(N)	P^ (%)	95% CI (low)	95% CI (high)
Public Wi-Fi use (any)	390	1,230	31.7	29.2	34.3
Passwords include personal info	627	1,230	51.0	48.2	53.8
Limited phishing literacy	400	1,230	32.5	29.9	35.1
Victimization by cybercrime (ever)	267	1,230	21.7	19.5	24.1
Reporting among victims	359	1,230	29.2	26.7	31.9

CI method per Methods: Wilson interval (z=1.96); no continuity correction applied.

Graphics

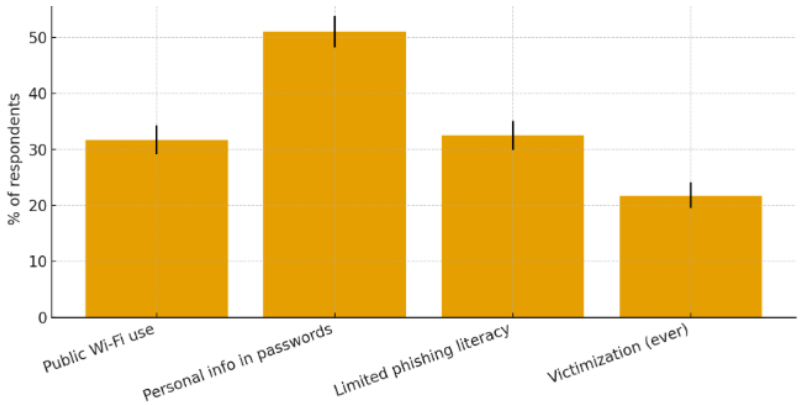

Figure 1. Individual security metrics (95% CI). Bar chart with error bars for the four primary indicators.

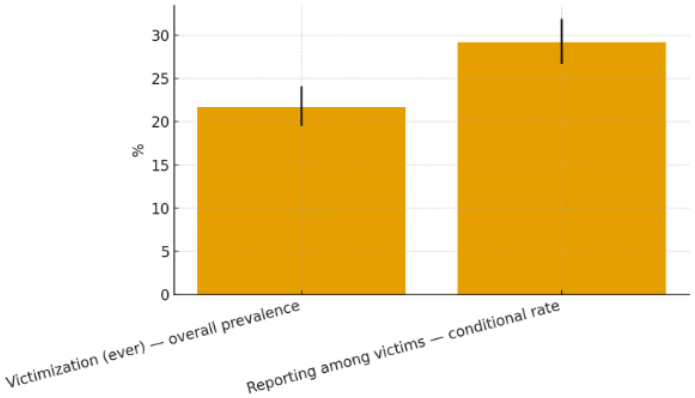

Figure 2. Victimization vs Reporting (95% CI). Paired display contrasting prevalence of victimization with reporting rates among victims.

Derived Analytic Objects (No Interpretation)

- All CIs were computed using the Wilson formula.
- Composite and operational indices (e.g., (R, M, S)) were computed as specified in Section (Methodology); numerical values are withheld here by design and are summarized visually in Figures 1 and 2.

DISCUSSION

Interpretation of Findings

- ***Salient Individual Gaps:*** The indicators point to elevated rates of risk-bearing behaviors—public Wi-Fi use (~31.7%), inclusion of personal information in passwords (~51%), and limited phishing literacy (~32.5%), together with a clear mismatch between victimization (~21.7%) and reporting (~29.2% of victims). These patterns motivate intervention bundles that prioritize password hardening/2FA-by-default, phishing recognition skills, and a culture of early reporting.
- ***Behavior–Policy Duality.*** Risky practices are not consistently counterbalanced by strong institutional policies or routines. This aligns with evidence from digital workplaces, showing that enforceable policies, organizational support, and periodic training are pivotal in converting awareness into repeatable secure behavior.

Comparison with Prior Studies

- Consistency with national evidence. Our individual-level results are consistent with prior national evidence obtained with the same instrument/sample (N=1,230; four measurement pillars), strengthening confidence in the observed trends and offering a standardized baseline for follow-up work.
- Social-media cohorts. Mixed-methods work (e.g., *Tehnički Glasnik*) reports gender-linked differences in social media security awareness and practice, in line with disparities visible in national datasets.
- School settings. Among female secondary school students in Eastern Makkah, awareness and practice were imbalanced (notable 2FA activation in a subset but weak hygiene, such as infrequent password updates), supporting age- and gender-sensitive program design.
- Organizational layer. Digital workplace studies show that role-based policy enforcement and training cadence correlate with better daily security behavior, helping to explain the observed gaps between individual exposure and organizational mitigation.
- Private sector/SMEs. Evidence of gaps in awareness, spending, and reliance on outsourcing underscores the practicality of aligning interventions with ECC-1:2018 and using institutional enablement pathways to raise maturity quickly and cost-effectively.

Explaining Differences and Similarities

- ***Demographic Heterogeneity.*** Differences by gender/age likely reflect usage patterns, exposure channels, and learning preferences, justifying targeted content and delivery by cohort.
- ***Measurement Homogeneity within National Sources.*** Using one validated instrument with four pillars (N=1,230) reduces definitional drift across studies and yields more stable trends for comparison, while still leaving room for controlled intervention trials.
- ***Organizational Convergence:*** Our patterns converge with workplace studies in highlighting policy, training, and institutional support as mediators bridging knowledge and behavior.

Substantive Contributions

- ***From Description to Operation:*** We integrated local evidence into a unified operational framework that links individual behavior with institutional governance and ECC-1:2018 requirements, moving beyond descriptive awareness.
- ***Measurement → Decision.*** We translate measurements into action via compact formulas—risk RRR, training dosage MMM, impact SSS—with explicit risk-tier thresholds that decompose bundles (high/moderate/low).
- ***National KPI Dashboard.*** We propose an expandable dashboard that combines behavioral (phish-sim fall, reporting) and organizational (2FA activation, compliance) indicators to drive a 90-day improvement cycle.
- ***SME Translation.*** We provide ECC-aligned checklists and practical enablement routes that leverage national resources to minimize costs and time-to-baseline.

LIMITATIONS AND FUTURE WORK (SUMMARY)

- ***Limitations:*** Heterogeneity in measurement tools across some studies, predominance of cross-sectional designs with limited causal inference, and incomplete disclosure of workplace contexts in certain surveys.
- ***Future Directions:*** randomized controlled trials to evaluate Shield-Aware bundles; broader sectoral coverage (health, education, finance); longitudinal tracking of phish-sim and micro-learning effects; and development of a lightweight SME maturity index aligned with ECC.

CONCLUSION

We introduced Shield-Aware, a framework that unifies Saudi evidence on cybersecurity awareness and behavior and ties it to national compliance requirements (ECC-1:2018). By packaging interventions across three layers—individual, organization, and governance/SMEs—and translating measurement into action through compact formulas (risk R, dosage M, and impact S) and a 90-day KPI dashboard, the framework is designed to deliver tangible outcomes: lower phishing simulation fall rates, faster incident reporting, and higher 2FA activation—directly improving readiness and resilience.

Scientific contributions: Shield-Aware closes the salient gap between awareness/behavior metrics and institutional compliance. It standardizes the conversion of behavioral proportions into operational decisions (clear bundle thresholds) and unifies KPIs (PP, IR, and A_{2FA} within a single impact index S. The protocol (identify → extract → double-code $\varkappa$ → analyze → ECC mapping → KPI dashboard) is reproducible and suitable as a backbone for randomized and quasi-experimental intervention studies.

Practical and governance implications The framework enables a fast-track, low-overhead compliance baseline for SMEs, leveraging NCA resources and Monsha'at/Thakaa enablement to move from the current state to minimum compliance and continuous improvement, supporting Vision 2030 priorities and trust in the digital economy.

Positioning vs prior literature. Unlike most cross-sectional studies that describe knowledge and attitudes, Shield-Aware operationalizes the measurement→intervention→governance pipeline and introduces a time-boxed dosage (90 days) with quantitative success criteria (e.g., $\Delta S \geq 0.10$) that can be tracked at the institutional level.

Equity and context sensitivity. The framework supports demographic tailoring—youth-focused modules and accessible content for older adults—and prescribes risk-tiered "recipes" to improve fairness and relevance across cohorts.

ACTIONABLE RECOMMENDATIONS (READY FOR IMPLEMENTATION)

- Adopt the 90-day cycle: Assess R → Select bundle → Deliver M + phish-sim → Measure S → Improve.
- Enforce default 2FA and password managers on all enterprise accounts with a binding password policy.
- Run tiered phishing simulations (monthly/quarterly/semiannual) and 5–7 min micro-learning with completion tracking.
- Maintain a unified KPI dashboard (PP, IR, A_{2FA}, S) at the entity level, reviewed every cycle.
- For SMEs: use ECC-aligned checklists and enroll in NCA/Monsha'at/Thakaa programs to reach the baseline and iterate upwards.

in summary, Shield-Aware offers dual value: a fast, practical path to immediately reduce targetable risks (phishing, passwords, under-reporting) and a scalable, testable scientific scaffold for sector-wide deployments—advancing national readiness and sustainable cyber-resilience.

ACKNOWLEDGMENT

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for their financial support (QU-APC-2025).

Funding

The authors did not receive any external grant funding for this study.

Conflicts of Interest

The author declares no conflict of interest

Author's Contribution Statement

Abdalilah Alhalangy: conceived and designed the study, developed the methodology, and writing original draft. **Khidir Shaib Mohame**d: Writing–original draft and editing, Writing – review and editing. **Saleh Abdulrahman Alkhamis:** Writing – review and editing.

REFERENCES

S. Saeed, "Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia," Sustainability, vol. 15, no. 7, p. 6019, 2023, doi: 10.3390/su15076019. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia

Vision 2030 Official Portal, "Vision 2030," Accessed: September 29, 2025. [Online]. Available: https://www.vision2030.gov.sa/en Saudi Vision 2030

National Cybersecurity Authority (NCA), Essential Cybersecurity Controls (ECC-1:2018), Riyadh, Saudi Arabia, 2018. [Online]. Available: https://nca.gov.sa/ecc-en.pdf

National Cybersecurity Authority (NCA), "Essential Cybersecurity Controls (ECC-2:2024) — Assessment & Compliance Tool," 2024. [Online]. Available: https://istitlaa.ncc.gov.sa/en/Scopingnsa/NCA/ECC2/

M. R. Albediwi, K., & Sadaf, "A. Framework for Cybersecurity Awareness in Saudi Arabia. Journal of Engineering and Applied Sciences, vol.10, no. 1, pp. 35–53, Nov. 2023, doi:10.5455/je. 2023050103. 208-1670361683-adt-1.pdf

National Cybersecurity Authority (NCA), "Report on Key Economic Indicators in the Cybersecurity Sector 2024," August 25, 2024. [Online]. Available: f18f6c96-a85c-4e36-80d1-938807c2be6c_Report-on-key-economic-indicators-in-the-cybersecurity-sector-2024-EN. pdf/ (see also the "Studies and Reports" section).

A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," Heliyon, vol. 7, e06016, 2021, doi: 10.1016/j.heliyon.2021.e06016. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia - PubMed

A. Alzubaidi, "Cybercrime Awareness among Saudi Nationals: Dataset," Data in Brief, vol. 36, 106965, 2021, doi: 10.1016/j.dib.2021.106965. Social Media Security Awareness in Saudi Arabia | Request PDF

M. E. Gharieb, "Knowing the Level of Information Security Awareness in the Usage of Social Media Among Female Secondary School Students in Eastern Makkah," IJCSNS, vol. 21, no. 8, pp. 360–368, 2021. [Online]. Available: http://paper.ijcsns.org/07_book/202108/20210845.pdf (no DOI listed by the journal).

M. Alsulami, "Social Media Security Awareness in Saudi Arabia," Tehnički Glasnik (Technical Journal), vol. 16, no. 2, pp. 213–218, 2022, doi: 10.31803/tg-20220124142802.

Monsha'at (General Authority for Small and Medium Enterprises), SME Monitor — Q3 2022 (including Thakaa Center section), 2022. [Online]. Available: https://www.monshaat.gov.sa/sites/default/files/2022-12/SME%20Monitor%20Q3%202022_0.pdf

E. Shafie, "Vulnerability of Saudi Private Sector Organisations to Cyber Threats and Methods to Reduce the Vulnerability," Pertanika Journal of Science & Technology, vol. 30, no. 3, pp. 1909–1926, 2022, doi: 10.47836/pjst.30.3.08.. http://www.pertanika.upm.edu.my/pjst/browse/regular-issue?article=JST-3288-2021

M. Alshaikh, S. Mehmood, R. Amin and Alsubaei, "The Impact of Cybersecurity Through Knowledge Sharing Practices: Limitations, Analysis of Current Trends and Future Research Directions," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 16, no. 3, pp. 1007–1029, Mar. 2025, doi: 10.14569/IJACSA.2025.0160398. [Online PDF].

