CYBER GUARDIAN
Your Online Safety Is Our Priority

POSSE

Personal Online Safety Security Empowerment

E X E C U T I V E R I S K B R I E F I N G

A.N. Other Company

Human Risk Exposure | Q1–Q3 2024

Board-level summary of human-layer security posture, risk reduction, and financial implications

REPORTING PERIOD	EMPLOYEES	DATA PROFILES
Q1–Q3 2024	50	100

info@cyberguardian.ie | cyberguardian.ie | Generated by CyberGuardian POSSE | Confidential

Executive Summary

This Executive Risk Briefing presents the board-level summary of the POSSE Human Risk Exposure programme for A.N. Other Company covering Q1–Q3 2024. It translates raw awareness data into risk language — quantifying the improvement in human-layer security posture, identifying residual exposure, and presenting the financial implications for cyber insurance and breach cost avoidance.

The human layer remains the primary attack surface across all cyber threats. 68% of global data breaches involve a human element. This programme exists to measure, reduce, and evidence that exposure — systematically and continuously.

> ***The organisation's average human risk awareness score improved by 29.7% across both dimensions during the reporting period. 94% of employees showed measurable improvement.***

Programme Performance — Headline Metrics

INDIVIDUAL AWARENESS	EMPLOYEE AWARENESS
9.52 → 12.34	8.26 → 11.04
+2.82 avg | 47.7% uplift | 90% improved	+2.78 avg | 46.7% uplift | 98% improved

COMBINED UPLIFT	PRIORITY COHORT
+280 points	6 employees
Aggregate awareness gain across all 100 profiles	Require targeted re-engagement in next cycle

Risk Reduction Narrative

The data demonstrates a clear, programme-driven reduction in human-layer cyber risk. The following narrative translates the awareness improvement into organisational risk terms:

01	Phishing and social engineering susceptibility: employees with developing-to-high awareness scores are significantly less susceptible to phishing, vishing, smishing, and BEC attacks — the vectors responsible for 68% of all global breaches. With 52–62% of employees now scoring ≥10, the organisation's human attack surface has meaningfully contracted.
02	Behavioural change: the 90–98% improvement rates across both dimensions indicate genuine behavioural shift, not superficial compliance activity. This distinction matters to underwriters and regulators — and it matters to the organisation's actual security posture.
03	Culture indicator: the average score (Individual: 12.34, Employee: 11.04) represents the organisation's collective cyber competence. At Q3, both dimensions sit in the Developing band and are tracking toward High — a trajectory that reduces insurer-assessed risk rating.
04	Residual risk: the 6 employees who showed no improvement across one or both dimensions require structured re-engagement. Unimproved individuals in the Foundational band represent the highest remaining social engineering risk in the organisation.

Financial Implications

The board should note the following financial context when assessing the value of the POSSE programme investment:

$4.88M	Average global cost of a data breach (IBM, 2024). The majority of breaches begin with a human element — the risk the POSSE programme directly addresses.
10–30%	Likely reduction in cyber insurance premium achievable by presenting this report to underwriters at renewal. For context, a 20% reduction on a €5,000 annual premium represents €1,000 saved — against a programme that can cost nothing.
- $2.66M	Average incident response cost reduction where a trained, awareness-mature workforce is in place, compared to an untrained equivalent. (IBM Cost of a Breach, 2024)

Board Recommendations

R1	**Continue the programme**	Sustain quarterly POSSE assessment cycles. The data demonstrates clear, measurable risk reduction — discontinuing the programme would reverse this trajectory and weaken the insurer evidence base.
R2	**Re-engage priority cohort**	Implement targeted re-engagement for the 6 employees showing no improvement. This should be logged, actioned, and reported before the next assessment cycle.
R3	**Present to insurer at renewal**	Submit this report — alongside the Insurance Readiness Report — to your cyber insurance broker as evidence of structured human-layer security controls. This is the documentation underwriters require for premium reduction consideration.
R4	**Track culture trajectory**	Monitor the average score trend across quarters. The objective is migration of the majority toward the Developing band, and a growing proportion into the High band. Set a target score for Q4 and beyond.
R5	**Report the CSR contribution**	Publish the Cyber CSR Report as part of the organisation's ESG and CSR disclosure. The 280-point aggregate awareness uplift and estimated 115-person societal reach represent a tangible, reportable community contribution.

The programme is working. The data is clear. The financial case is compelling. The board's action is to sustain, escalate, and report this progress.

TEMPLATE NOTE: *Recalculate all metrics from the POSSE dashboard at the end of each assessment period. The recommendation text is evergreen; update the specific figures (employee counts, scores, cohort sizes) before each board presentation.*