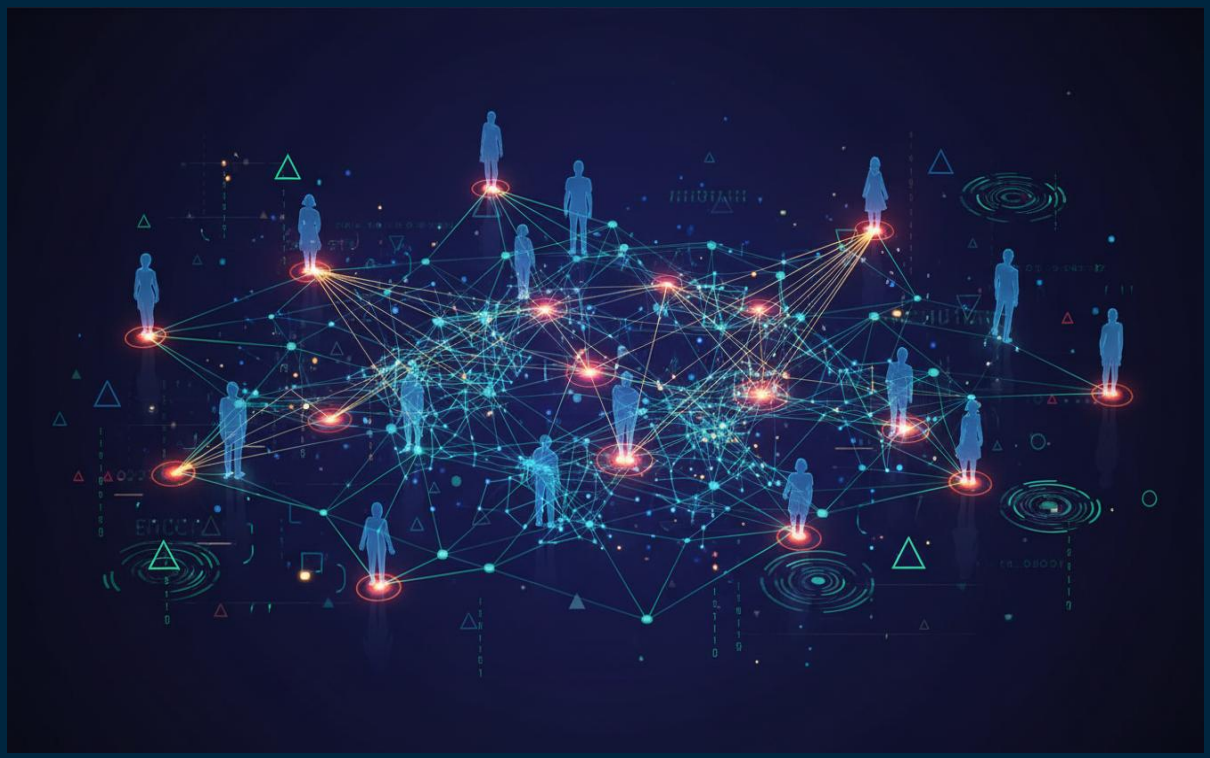
FORENSIGHTS INTELLIGENCE BRIEF
Issue 02 · July 2026

RESEARCH SERIES · HUMAN RISK & SOCIAL ENGINEERING

The Hidden Patterns Behind Scam and Fraud Risk: Why Vulnerability Isn't Random

New research findings from ForenSights reveal that scam and fraud risk may be shaped by both organisational conditions and individual behaviours — suggesting the problem runs deeper than awareness alone.

Whistine Chai · Founder & Principal Psychologist, ForenSights



810

Working adults from 15 industries and diverse organisational contexts, including SMEs, MNCs, government and non-profit organisations.

809

Participants in a second study using a nationally representative sample of Singapore residents to examine scam and fraud risk.

1,600+

Total participants across two ForenSights studies on scam and fraud risk.

9%

ALMOST DAILY

Online financial transactions occur inside the workday.

In our recent study involving 810 working adults in Singapore, representing a diverse range of industries, organisational levels, occupations and sectors, we found that 9% of the respondents conducted online financial transactions at work almost daily.

Among the respondents, one in three (33%) reported that, to the best of their knowledge, their organisation had encountered an attempted or successful fraud or social engineering incident targeting the organisation. 26% reported being unsure whether such incidents had occurred within their organisations.

1 in 3

33% REPORTED INCIDENTS

Their organisations had encountered an attempted or successful scam, fraud or social-engineering incident targeting the organisation.

26%

UNSURE

Reported they were unsure whether such incidents had occurred within their organisations.

Organisations commonly approach cyber and fraud risk by keeping technology secure, training their people, and trusting that these measures are sufficient to contain risk.

Yet many continue to experience scam and fraud incidents despite investing in awareness training, tightening technical controls, and meeting compliance requirements.

Our research suggests that part of what is missing is this: human vulnerability plays a significant role, and that vulnerability may not be randomly distributed across the workforce.

Overall, cyber and fraud risk was significantly associated with specific organisational conditions and behavioural patterns ($p < .05$). Organisational conditions that are often

overlooked by conventional security programmes may play an equally important role in shaping cyber and fraud risk. Consequently, relying solely on staff awareness is unlikely to be adequate.

> ***"What if the greater risk is not what employees don't know about threats — but the environment in which they make decisions?"***
>
> ForenSights · Intelligence Brief Issue 02

OUR RESEARCH

ForenSights recently conducted two studies involving over 1,600 respondents on scam and fraud risk in Singapore. The first study involved 810 working adults across Singapore, representing diverse industries, organisational levels, occupations and sectors. The participants ranged from junior employees to senior leaders across public, private and non-profit organisations. It was designed to examine patterns associated with cyber risk, scam susceptibility and organisational exposure. This diversity allows ForenSights to examine how scam and fraud risks may vary across different organisational contexts, job functions and seniority of roles. The current article is based on this study.

WHAT WE FOUND

Three patterns. One structural conclusion.

1. Behavioural risk patterns differ across organisational contexts

Employees from different sectors did not show the same patterns of vulnerability. There were clear differences that appeared across industries, occupations, organisational levels and sectors. These suggest that work conditions are associated with exposure to cyber and fraud risk in ways that are patterned, and not coincidental.

This also implies that a security programme calibrated for one organisational context may be systematically under-protected or over-trained for another.

Given that generic approaches obscure the variation that matters, security programmes need to examine the organisational context.

> **If vulnerability differs by organisational context, then the one-size-fits-all training does not just miss the mark — it misses a different mark for every part of the organisation.**

2. Organisational culture shapes risk more than many organisations realise

Our recent study of working adults found clear associations between specific organisational factors, behavioural risk exposure and risky behaviours. These factors include how concerns are raised, how reporting processes are perceived by staff, and how clearly management communicates and models expectations around security.

Culture is not peripheral to cybersecurity. Instead, culture is a core determinant of employee behaviour.

Culture can shape whether employees in organisations would flag anomalies actively, hesitate before acting, or remain silent instead of raising concerns.

Each of these responses has important risk implications for cybersecurity.

> ***"Reporting culture is not simply a function of policy. It reflects the psychological safety employees perceive when something feels wrong but is not yet clearly wrong."***
>
> ForenSights · Intelligence Brief Issue 02

3. Uncertainty, not ignorance — creates an exploitable moment

Having knowledge of fraud, scam and cyber-enabled threats is not sufficient.

Many respondents in our study understood these risks in general terms. However, the vulnerability did not arise from ignorance. Instead, vulnerability may arise from moments of uncertainty. These include

- When something felt unusual but not clearly wrong.
- When procedures or processes were ambiguous.
- When a quick decision was required etc.

Fraud and scam attempts are frequently designed to create these conditions of uncertainty, ambiguity, urgency, and hesitation. They exploit the gap between knowing a rule and being able to apply it under pressure.

Scams are engineered to work in the space between knowing the risk exists and being certain enough to act on that knowledge.

Actors are increasingly targeting this gap.

IMPLICATIONS FOR ORGANISATIONS

The organisation is part of the risk model.

01 **The organisation shapes the individual**

Organisational culture and daily practices not only shape the environment in which employees work but also the risks that environment creates.

02 **Vulnerability may be rooted in both organisational systems and human behaviour**

Systemic vulnerabilities can quietly increase exposure long before an incident occurs. They are not routinely measured by conventional security audits.

03 **Raising awareness alone is unlikely to be sufficient**

While knowledge is important, effective resilience building also depends on understanding how organisational culture affects risk.

KEY TAKEAWAYS

From "Are our staff aware?" to "What shapes how they behave?"

Holistically, these findings suggest that cyber and fraud risk is not only a technology issue, but also a behavioural systems concern.

Vulnerability does not appear to be evenly distributed.

It appears to be associated with specific organisational conditions, roles and decision environments in ways that conventional cybersecurity measures often miss.

If these patterns can be identified, vulnerability can potentially be measured and managed before incidents occur.

FORENSIGHTS — WHERE MIND MEETS DATA

Measuring what conventional security programmes often overlook

Technological approaches to cybersecurity often overlook vulnerabilities at the level of the human user. ForenSights research addresses this gap by identifying organisational behavioural risk patterns that existing security frameworks normally do not capture.

Our ongoing research examines the full suite of behavioural vulnerabilities to scams and fraud with the aim of augmenting present-day security safeguards by unravelling what underlies human error prior to incidents.

This is the second in a series of research-informed perspectives from ForenSights. Future issues will present additional findings from our ongoing research on behavioural risk. We welcome your thoughts, questions, and perspectives on the findings presented. Please reach out if you would like to discuss further.

ForenSights Pte. Ltd.
https://forensights.com

Behavioural Risk · Cyber Psychology · Risk Prediction
Organisational Resilience · Human Factors · Singapore

© 2026 ForenSights Pte. Ltd. All rights reserved.