



RESEARCH SERIES · HUMAN RISK & ORGANISATIONAL CYBER RESILIENCE

Why Employees Go Silent on Cyber Threats They Recognise

Singapore has made substantial investments in strengthening organisational cybersecurity through the adoption of baseline organisational cybersecurity controls. According to the Singapore Cyber Landscape 2025/2026 report published by the Cyber Security Agency of Singapore (CSA), more than 800 organisations have attained at least one Cyber Essentials certification as of early 2026. The report also highlights continued investment in national cybersecurity capabilities to support Singapore's digital future. Despite these increasing efforts, technical controls, certifications and infrastructure support alone may not be sufficient to ensure strong cybersecurity outcomes.

This raises an important question: Despite cybersecurity awareness and technical safeguards becoming organisational priorities, incidents and breaches continue to be underreported. Why do employees stay silent?



Whistine Chai · Founder & Principal Cyber Psychologist

Shakila Devi · Research Associate

66%

**identified phishing content across messages,
emails, and websites**

CSA Cybersecurity Public Awareness Survey,
2024

50%

**never reported a phishing email across 20
campaigns over 19 months**

Canham et al., 2021

Growing investments in cybersecurity awareness have produced measurable gains in threat recognition. Yet human-related cyber risks continue to significantly compromise organisational security — not because employees cannot identify threats, but because they may choose not to report them.

The gap between recognition of phishing incidents and reporting behaviour has been illustrated through contrasting findings in the broader literature of underreporting. In 2024, a Cybersecurity Public Awareness survey was conducted by the Cyber Security Agency of Singapore. The survey found that 66% of Singaporeans were able to correctly identify phishing content across different forms such as messages, emails and websites.

However, a study by Canham et al. (2021) on reporting behaviours questions this statistic due to its contrasting findings. 6,000 employees were studied for their reporting behaviours over a period of 19 months. Despite exposure to 20 different phishing campaigns, 50% of employees still did not report a single phishing email that they encountered.

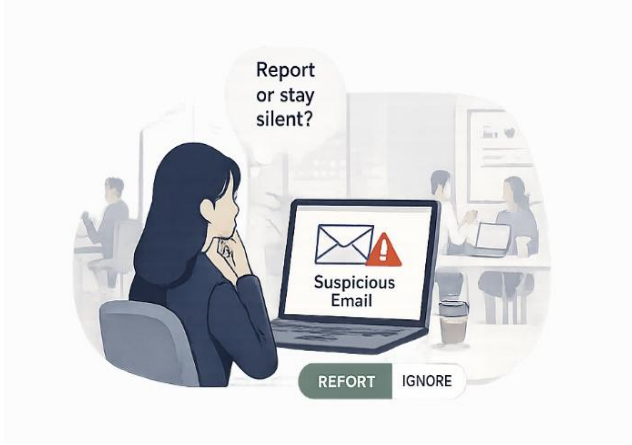
Accurate recognition of a phishing email on its own does not improve organisational cybersecurity. Organisations only benefit when employees translate that recognition into incident reporting — the point at which appropriate follow-up can occur.

Why do employees refrain from reporting phishing incidents despite being aware of the consequences?

Two-thirds of employees can successfully identify a phishing attempt. However, nearly the same proportion knowingly engages in risky behaviour. Why are employees staying silent?

THE REPORTING PROBLEM

Incident reporting could be a psychological safety problem, not a training problem.



An employee's decision to report a suspected cyber incident is not purely a function of knowledge. It could be a function of their assessment of interpersonal risk. Employees who are afraid of being blamed or compromising their professional reputation are less likely to report suspected threats — even when they can recognise them and understand the potential consequences.

"Psychological safety is a shared belief that a team or organisation is safe for interpersonal risk-taking."

Edmondson, 1999

Psychologically safe environments increase the willingness of employees to raise concerns, admit faults, and surface potential threats. This can be attributed to two factors:

1. They can do so without fear of rejection or negative consequences
2. They believe that the information will be taken seriously and acted upon effectively.

Where psychological safety is absent, the mindset shifts. The personal risk of speaking up (being seen as the source of a problem, being blamed for an error, or being dismissed as overly cautious etc) outweighs the perceived benefit of reporting. When the threat goes unacknowledged, the organisation loses the opportunity to respond.

WHAT SHAPES PSYCHOLOGICAL SAFETY

Leadership culture sets the conditions for whether people speak up.



Psychological safety is not a personal trait that employees have or lack. It is a perception shaped by the organisational environment — particularly by leadership behaviours.

1. Leadership culture is the primary driver

Edmondson (1999) established that managers play an integral role in creating conditions where employees feel safe to report errors and ask for help without fearing negative consequences. Although formal policies state the need to report, the response from organisation leaders when a problem arises and errors are discussed serve as an important indication to employees on how they would be treated should they choose to raise their concerns.

Van der Kleij et al. (2025) found that leadership cultures that support instances of reporting by viewing them as opportunities for learning (rather than grounds for punishment), consistently diminish the fear-related barriers that employees face. By giving employees credit for flagging potential cyber incidents, it reinforces their behaviour to do so.

"Non-punitive practices that treat mistakes as opportunities for growth, rather than grounds for punishment, remove the reluctance to speak up due to fear of criticism."

Van der Kleij et al., 2025

2. Intrinsic motivation matters as much as formal policy

Ebbers et al. (2026) discussed the influence of Organisational Citizenship Behaviours (OCBs), which are behaviours that are not formally required or rewarded by organisations but contribute to effective functioning. The study found that OCBs were a strong independent predictor of employees' intention to report cyber security incidents, alongside psychological safety. This suggests that **policies alone cannot single-handedly support a culture of incident reporting**. Instead, employees' intrinsic motivation exerts a stronger influence on their decision to do so.

Measuring the organisational conditions that shape cyber resilience.

Technological approaches to cybersecurity often overlook vulnerabilities at the level of the human user. ForenSights research addresses this gap by examining the organisational conditions such as governance, culture, and leadership that shape how individuals behave under cyber risk.

Our ongoing research seeks to help organisations move beyond awareness metrics to understand the behavioural and structural factors that determine whether security knowledge translates into security action.

1,600+ participants across two independent ForenSights studies

FORENSIGHTS FINDINGS

Our findings are consistent with this perspective. We conceptualise organisational governance as an organisation's commitment to cybersecurity, including leadership support, governance processes, oversight mechanisms, and broader organisational practices that influence how cyber risk is managed. From our recent study on 801 working adults, we found that governance did not appear to exert its protective effect solely through formal policies or governance processes. Instead, its influence was reflected through broader organisational culture.

Interestingly, although most respondents knew how to report or escalate incidents, 5% felt psychologically unsafe about reporting them.



Source: ForenSights Survey conducted to 810 Working adults from 15 industries and diverse organisational contexts, including SMEs, MNCs, government and non-profit organisations.

This suggests that **governance may contribute to cyber resilience through broader organisational conditions such as culture and psychological safety**, rather than solely through formal policies or controls in shaping cyber resilience. Hence, building technical safeguards alone without fostering a supportive leadership culture towards reporting may continue to limit an organisation's ability to effectively detect and respond to cyber threats.

Building a reporting culture requires more than a reporting system.

01 Improve the usability and accessibility of reporting systems

Reporting mechanisms that are difficult to use, unclear in process, or anonymous in outcome reduce the likelihood of use.

Systems should be straightforward, acknowledge receipt, and communicate what happens after a report is made.

02 Build trust in leadership to handle reported incidents effectively

Employees need confidence that reporting will not result in blame but in action.

Leaders who model transparent responses to security concerns would signal that the organisation treats reporting as a professional contribution, not a liability.

03 Cultivate organisational practices that support proactive reporting

Policy can define what to report and how, but it cannot create the motivation to do so.

Organisations that invest in psychological safety at the team level (through non-punitive norms, visible leadership behaviour, and recognition of proactive security actions) develop the intrinsic motivation that policies cannot mandate.

KEY TAKEAWAYS

Ultimately, training and policies can only teach employees what and how to report. Organisational culture and governance determine who would actually do so.

Cybersecurity awareness programmes have made measurable progress in threat recognition. The evidence suggests that recognition is no longer the primary constraint. The constraint is what happens during moments of decision making — whether the organisational environment makes reporting feel safe enough to act on what employees already know.

Governance structures, leadership behaviour, and organisational climate are not peripheral to cybersecurity strategies. They are, in practice, a significant part of it.

ForenSights Intelligence Brief, Issue 5

This is the fifth in a series of research-informed perspectives from ForenSights. We welcome your thoughts, questions, and perspectives on the findings presented. Please feel free to reach out if you would like to discuss further.

REFERENCES

- Canham, M., Posey, C., Strickland, D., & Constantino, M. (2021). Phishing for long tails: Examining organizational repeat clickers and protective stewards. *SAGE Open*, 11(1), 2158244021990656. <https://doi.org/10.1177/2158244021990656>
- Cyber Security Agency of Singapore. (2024). Cybersecurity public awareness survey 2024. <https://www.csa.gov.sg/news-events/press-releases/csa-s-2024-cybersecurity-public-awareness-survey-shows-an-improvement-in-the-adoption-of-cyber-hygiene-practices/>
- Cyber Security Agency of Singapore. (2026). Singapore Cyber Landscape 2025/2026: *Securing Our Digital Frontiers*. <https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2025-2026/>
- Ebbers, S., Smith, J., Tan, A., & Lee, K. (2026). Predictors of employees' cyber incident reporting intention: A vignette study on TPB, psychological safety, and organizational citizenship behaviour. *Computers & Security*, 167, 104920. <https://doi.org/10.1016/j.cose.2026.104920>
- Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, 44(2), 350–383. <https://doi.org/10.2307/2666999>
- Van der Kleij, R., et al. (2025). *Cultural, Organisational and Individual Factors Contributing to Cybersecurity incident Reporting Behaviour: A Systematic Literature Review*. Social Science Research Network. <https://doi.org/10.2139/ssrn.5634456>

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

Behavioural Risk · Cyber Psychology · Scam Prevention
Organisational Resilience · Human Factors · Singapore

© 2026 ForenSights Pte. Ltd. All rights reserved.

No part of this publication may be reproduced in any form without the prior written permission of ForenSights Pte. Ltd.

For permission or enquiries, please visit forensights.com