CybaWay

Human Vulnerability Assessment Report

Scan Reference:	**Q4 - All Users - Scan 03**	Organisation:	**CybaWay**
Scan Window:	**Dec 16, 2025 - Dec 31, 2025**	Duration:	**30 Days**
Total Users:	**4**	Report Version:	**3.0**

CONFIDENTIAL - FOR AUTHORISED PERSONNEL ONLY

Generated on: January 10, 2026 at 9:51 PM

1 Executive Summary

Assessment Overview

This comprehensive human vulnerability assessment reveals the organisation's security posture through behavioural analysis of 4 users. Conducted between December 16, 2025 and December 31, 2025, the assessment identifies critical human-factor risks and provides actionable insights for security improvement.

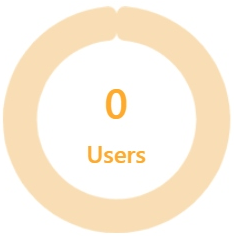
4	30 days	29.3%	0
USERS SCANNED	ASSESSMENT PERIOD	OVERALL VULNERABILITY SCORE	CRITICAL VULNERABILITIES

1.1 - Top Security Concerns

- Password security analysis shows 25.0% of employees use weak passwords and 25.0% reuse passwords across multiple accounts.
- Device security analysis detected 50.0% of employees have poor screen lock habits.
- Knowledge assessment reveals 100.0% of employees have significant cybersecurity knowledge gaps, with weakest performance in baseline training.

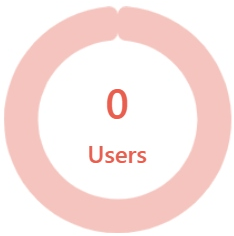
1.2 - Key Risk Indicators

HIGHLY VULNERABLE



MODERATELY VULNERABLE

PHISHING SUSCEPTIBLE



KNOWLEDGE GAPS

2 Introduction

2.1 Assessment Objectives

This assessment aims to identify and quantify human vulnerabilities within the organisation by analysing employee behaviours, security practices, and threat susceptibility. The primary objectives include:

- Evaluate organisational human risk posture
- Identify behavioural patterns contributing to security risks
- Assess susceptibility to common cyber threats
- Provide actionable insights for security improvement
- Establish baseline metrics for ongoing security monitoring

2.2 Key Definitions

TERM	DEFINITION
Human Vulnerability Index (HVI)	A composite score measuring individual susceptibility to security threats based on behavioural analysis
Behavioural Archetypes	Classification of users based on psychological and behavioural patterns affecting security practices
Threat Exposure Index (TEI)	Quantitative assessment of organisational exposure to specific cybersecurity threats
Organisational Human Risk Posture (OHRP)	A holistic measure estimating the organisation's overall risk status by combining human susceptibility (HVI) and threat exposure (TEI)

Assessment Parameters

- Assessment conducted in real-world working environment
- User behaviours observed represent typical work patterns
- All data collection complies with organisational policies
- Findings reflect actual risk exposure under normal conditions

3 Organisational Demographics

3.1 Scan Design & Approach

The human vulnerability assessment employed a comprehensive scanning methodology over a 30-day period, monitoring user interactions across multiple security domains including password practices, email security, device usage, and web browsing behaviours.

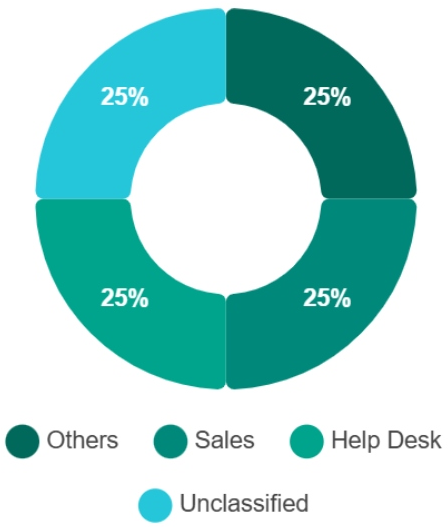
3.2 Compliance Framework Alignment

The assessment methodology aligns with industry standards including NIST Cybersecurity Framework, ISO 27001, and CIS Controls, ensuring comprehensive coverage of human factor security considerations.

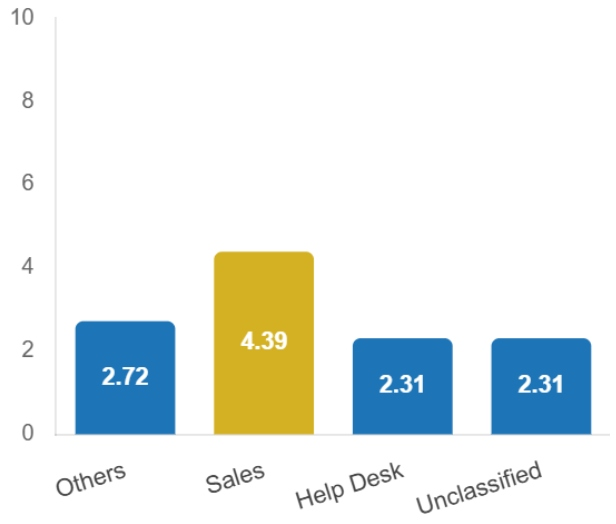
3.3 Workforce Overview

DEPARTMENT	USER COUNT	PERCENTAGE	AVG VULNERABILITY SCORE
Others	1	25%	2.72
Sales	1	25%	4.39
Help Desk	1	25%	2.31
Unclassified	1	25%	2.31

Department Distribution



Avg Score Comparison



4 Detailed Findings

4.1 Human Vulnerability Index (HVI)

The human vulnerability index was calculated using a weighted algorithm considering:

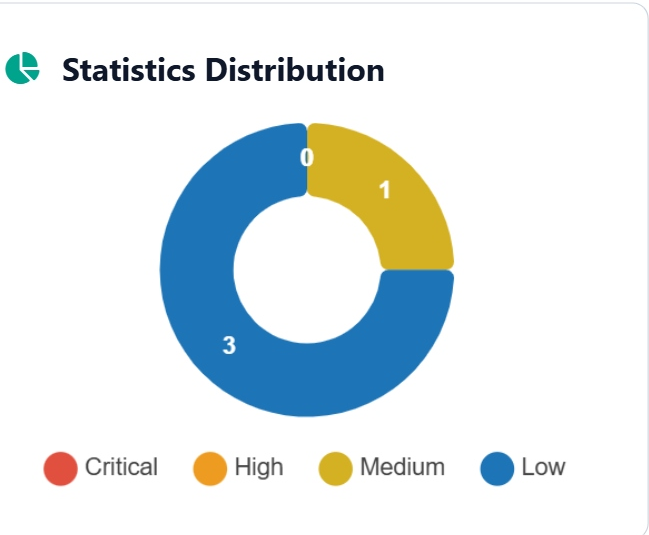
- Behavioural threat (30% weight)
- Online exposure (22% weight)
- Phish susceptibility (27% weight)
- Security knowledge gap (21% weight)

METRIC	VALUE	BENCHMARK	STATUS
Avg Behaviour Rating	2/10	< 4	Good
Avg Exposure Rating	0/10	< 4	Good
Phishing Susceptibility	0 users (0%)	< 10%	Good
Knowledge Gap	4 users (100.0%)	< 10%	Needs Improvement
Human Vulnerability Index (HVI)	**29.3%**	**< 20%**	Fair

4.2 Summary Statistics

The Human vulnerability index of 29.3% reflects a composite measure of users' susceptibility to security threats, based on behavioural analysis.

- 0 users are classified as critical
- 0 users are highly vulnerable
- 1 user is moderately vulnerable
- 3 users are rated as low vulnerability



4.3 Top Vulnerable Users

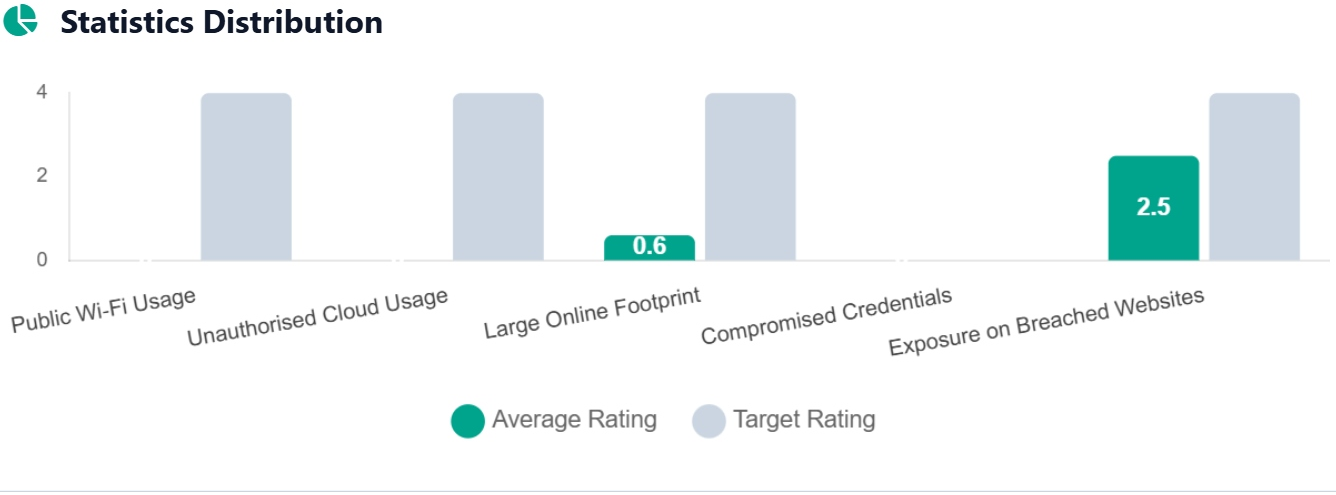
USER ID	VULNERABILITY SCORE	VULNERABLE LEVEL	DEPARTMENT	TOP CONCERNS
divine.chana@cybaway.com	43.9%	Medium	Sales	Knowledge Gap, Poor Screen Lock Habits, Weak Password Usage
admin@cybaway.com	27.2%	Low	Others	Knowledge Gap, Poor Screen Lock Habits
info@cybaway.com	23.1%	Low	Help Desk	Knowledge Gap
support@cybaway.com	23.1%	Low	Unclassified	Knowledge Gap

4.4 Behaviour Rating

The behaviour rating is a quantified measure of how user actions and habits contribute to security risk. It evaluates behavioural factors such as password hygiene, email usage, screen-lock practices, and risky browsing/downloading habits.

4.5 Exposure Rating

The exposure rating is a measure of the extent to which a user's digital footprint and account presence are exposed to external threats. It considers factors like credentials found in breach databases, accounts on compromised websites, use of public Wi-Fi, and large online footprints.



4.6 Phishing Susceptibility

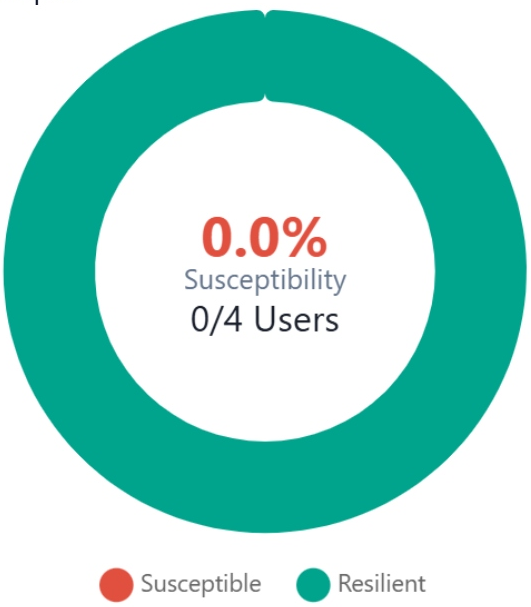
Phishing susceptibility reflects how vulnerable users are to social engineering attacks, measured through their performance in the Phish Challenge simulations and Direct Phishing Tests.

Phish Challenge

During scan Q4 - All Users - Scan 03, up to 1 Phish Challenges were sent. 25.0% of users completed at least one challenge. The average score among completed users was 26.7.

Direct Phishing Test

During the scan period, 4 users received phishing emails. 0 users interacted with malicious payloads, representing 0% susceptibility. The assessment shows 0 link clicks, 0 attachment downloads, and 0 credential submissions were involved in the phishing attempts.



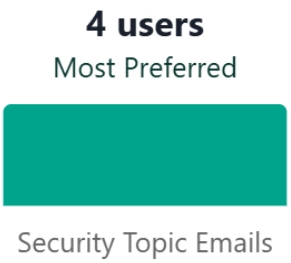
4.7 Knowledge Gap

Knowledge gap assessment covers three core categories: baseline training (users' understanding of everyday security best practices), cyber-skills training (users' grasp of specialised cybersecurity modules), and policy training (users' awareness of organisational cybersecurity policies).

Training Analysis

Training analysis shows Security Topic Emails is the most preferred training channel (4 users), while None is the least used.

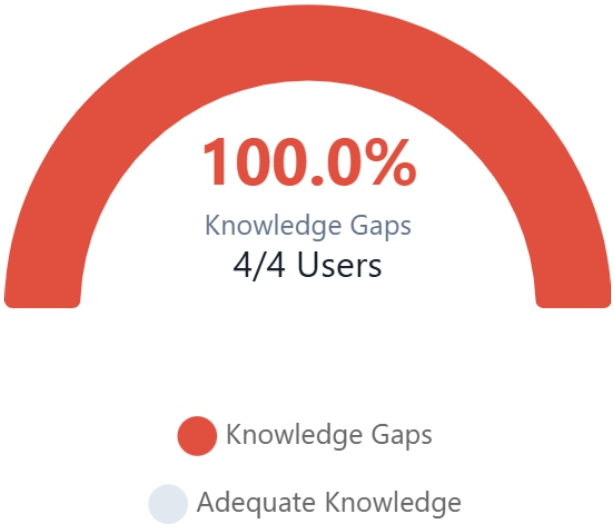
Most Common Channel	Security Topic Emails
Least Common Channel	None
Most Common Learning Style	Traditional Learner



Knowledge Assessment

Knowledge assessment reveals 100.0% of employees have significant cybersecurity knowledge gaps, with weakest performance in baseline training.

Baseline Training	Below Average	4 users /4 total
CyberSkills Training	Below Average	4 users /4 total
Policy Training	Below Average	4 users /4 total



4.8 Behaviour Archetypes

During the scan, users were profiled into four distinct behavioural archetypes, reflecting psychological tendencies and everyday security habits.

25% of users

Convenience-Seeker

Users who prioritise efficiency over security, often reusing passwords and ignoring alerts. Their main barrier is motivation.

25% of users

Overconfident

Users with strong knowledge who still take risks, such as ignoring warnings or skipping training. Their key barrier is poor risk perception.

100% of users

Anxious Avoidant

Users highly aware of threats but lacking confidence to act, often avoiding security tasks. Their primary barrier is capability.

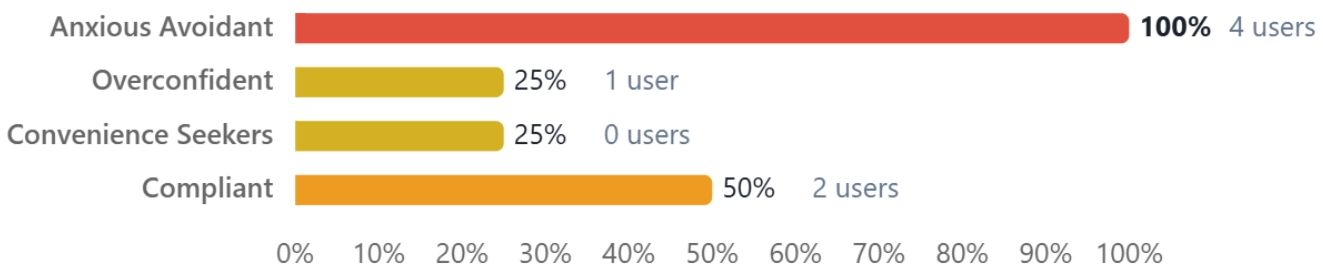
50% of users

Compliant

Users who follow instructions reliably but lack deep understanding, leaving them exposed to unfamiliar threats. They require ongoing reinforcement.

Statistics Distribution

Most Common Archetype	Anxious Avoidant
Urgency Level	High

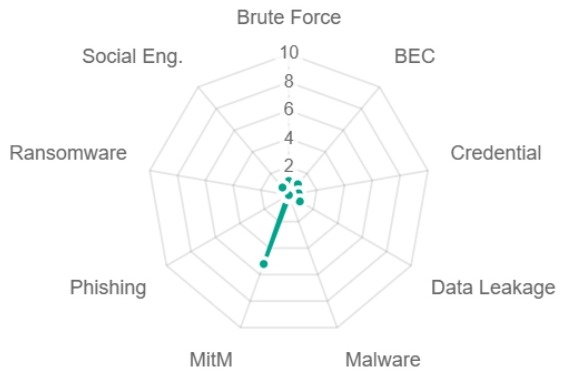


5 Threat Exposure Index (TEI)

The Threat Exposure Index (TEI) is a quantitative assessment of the organisation's exposure to nine major cybersecurity threats, calculated from 43 monitored events and 35 defined use cases.

- **Threat Exposure Index (TEI) 10.78%**
- Target benchmark: **< 20%**
- Status **Good**
- # of threats exceeding 50% severity level: **1**
- Dominant Threat: **Man-in-the-Middle (52%)**

Average Threat Distribution



5.1 Top Threats Summary

THREAT CATEGORY	EXPOSURE SCORE	RISK LEVEL	DESCRIPTION
Man-in-the-Middle	5.2/10	High	Users vulnerable to attacks that intercept, eavesdrop, or manipulate communications.
Brute Force Attack	1.0/10	Low	Users likely to use weak or easy-to-guess passwords, or be targeted due to data breaches.
Business Email Compromise	1.0/10	Low	Users likely to be a victim of company email impersonation in phishing or social engineering.
Credential Stuffing	0.7/10	Low	Users likely to reuse passwords across accounts, or be targeted due to data breaches.
Data Leakage	0.9/10	Low	Users likely to upload sensitive data to cloud services or email confidential documents.
Malware Spread	0.1/10	Low	Users likely to download software from untrusted sources or click on suspicious links.
Phishing Attack	0.1/10	Low	Users likely to click on malicious links or provide sensitive info on fake websites.
Ransomware	0.0/10	Low	Users likely to download and execute malicious attachments or fall for phishing emails.
Social Engineering	0.7/10	Low	Users likely to trust unknown individuals and share confidential information.

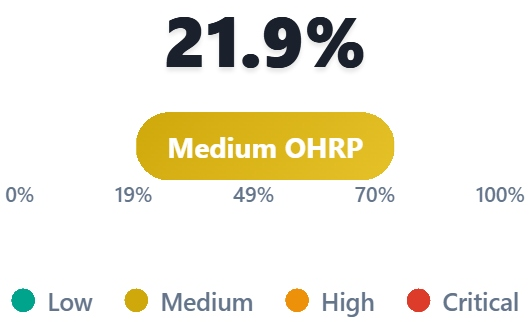
6 Organisational Human Risk Posture (OHRP)

The organisational human risk posture is a holistic measure estimating the organisation's overall risk status by combining human vulnerability index (HVI) and threat exposure index (TEI). It reflects how susceptible the organisation is to real-world cyber incidents based on internal behaviours and external threat landscape.

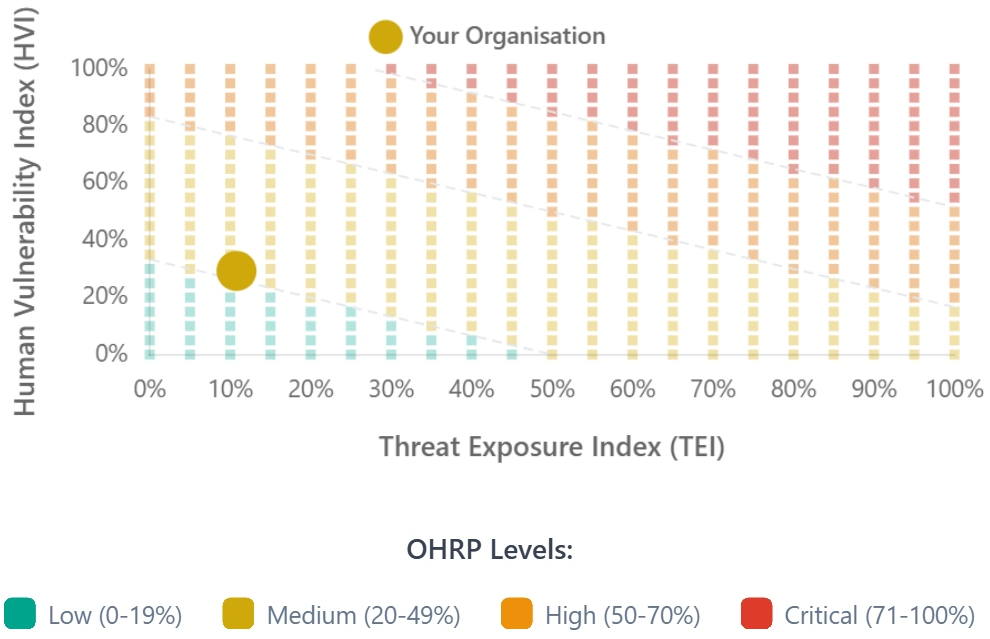
How OHRP is Calculated

OHRP = (HVI × 0.6) + (TEI × 0.4)

HVI	**29.3% × 0.6 = 17.6%**
TEI	**10.78% × 0.4 = 4.3%**



OHRP Matrix Visualisation



OHRP Levels:

Low (0-19%) Medium (20-49%) High (50-70%) Critical (71-100%)

7 Intervention Roadmap

This Human Vulnerability Assessment provides a comprehensive analysis of organisational security posture from a human factors perspective. The findings highlight both strengths and areas requiring immediate attention.

TIMEFRAME		ACTION ITEM	PRIORITY
Short-term	(1-2 months)	Add Targeted Password Security Topics to Queue (Topic of the Week)	Medium
Short-term	(1-2 months)	Enable Weak Password Behaviour Intervention for Affected Users	Medium
Short-term	(1-2 months)	Enable Same Password Behaviour Intervention for Affected Users	Medium
Short-term	(1-2 months)	Mandatory Password Policy Challenge for Affected Users	Medium
Short-term	(1-2 months)	Add Targeted Device Security Topics to Queue (Topic of the Week)	Medium
Short-term	(1-2 months)	Enable Screen Lock Behaviour Intervention for Affected Users	Medium
Short-term	(1-2 months)	Mandatory Device Security Policy Challenge for Affected Users	Medium
Short-term	(1-2 months)	Enable Security Best Practice Intervention for Affected Users	Medium
Long-term	(2+ months)	Add Targeted Email Security Topics to Queue (Topic of the Week)	Medium
Long-term	(2+ months)	Enable Personal Email Behaviour Intervention for Affected Users	Medium
Long-term	(2+ months)	Add Targeted Internet Security Topics to Queue (Topic of the Week)	Medium
Long-term	(2+ months)	Enable Social Media Behaviour Intervention for Affected Users	Medium

By implementing the recommended actions, the organisation can significantly reduce human-factor security risks and build a more resilient security posture against evolving threats.