ZiSoft

CYBERSECURITY AWARENESS BASELINE ASSESSMENT Report

Cultivating a Resilient Security Culture for

CUSTOMER NAME

Assessment Conducted:
October 20 - October 24, 2024

This report contains confidential information and is intended solely for the internal use of **CUSTOMER NAME**.

Report Issued
October 27, 2024
Version: 1.0

ZiSoft

TABLE OF CONTENTS

CONTENTS

INTRODUCTION

This report outlines the findings from our recent Cybersecurity Awareness Baseline Assessment conducted in the timeframe between Sunday, October 20th, 2024 and Thursday, October 24th, 2024.

Assessment Purpose

The purpose of this Cybersecurity Awareness Baseline Assessment Report, concluded via services offered by ZiSoft, is to present an analysis of employee knowledge and practices across essential security domains. This report identifies current strengths and areas for improvement, offering actionable insights to guide targeted training and enhance the overall security posture of CUSTOMER NAME.

Assessment Scope and Objectives

This assessment targeted key domains to gauge the cybersecurity knowledge and practices across CUSTOMER NAME, specifically covering the following domains under their respective categories:

ZiSoft Categories and Domains are as Follows:

- **Digital and Online Security**
  - Safe Browsing
  - Mobile Security
  - Online Shopping
  - Email Security
  - Wi-Fi Security
  - IoT Security
- **Information Protection and Data Security**
  - Data Protection
  - Removable Media Security
  - Cybersecurity Hygiene
  - Secure Passwords
- **Social Engineering and threat Awareness**
  - Social Engineering
  - Types of Phishing
  - Social Media Security
  - Executives Awareness
- **Physical and Environmenttal Security**
  - Secure Travelling
  - Meeting Security
  - Physical Security
- **Fraud and Embezzlement**
  - Fraud

THE ASSESSMENT INCLUDED EMPLOYEES ACROSS MULTIPLE LEVELS, INCLUDING THE FOLLOWING LEVELS:

General employees

Department leads

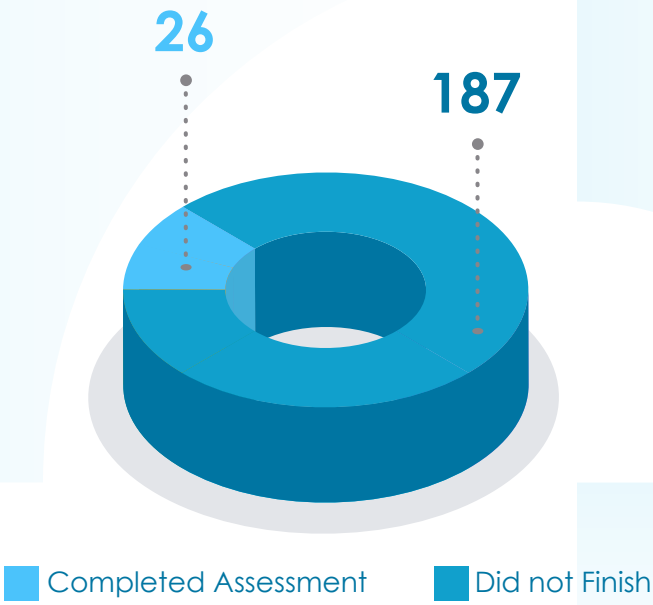
Senior management

Allowing for a comprehensive view of awareness levels and potential areas for improvement.

EXECUTIVE SUMMARY

Assessment Participation

The Cybersecurity Awareness Baseline Assessment engaged a total of **213 employees**, with **187 employees** fully completing the assessment, resulting in a participation rate of **87.79 %.**

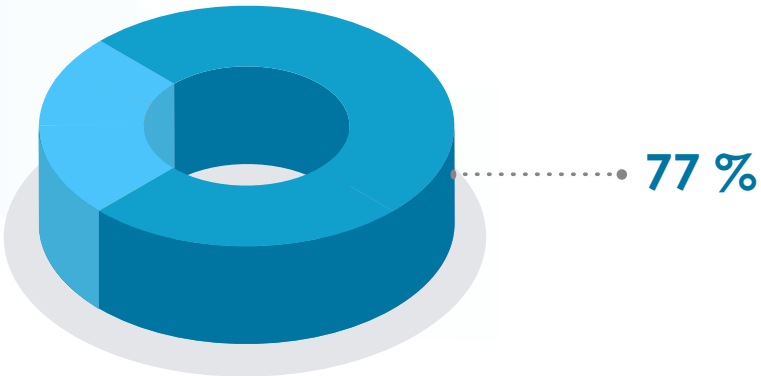


The assessment spanned **16 departments**, with a comprehensive question set of **54 questions** over **18 domains** aimed at evaluating core cybersecurity knowledge and behaviors under 5 key categories.

Key metrics and insights

Overall Recorded Awareness

The average assessment score achieved across participating employees was 77 %.

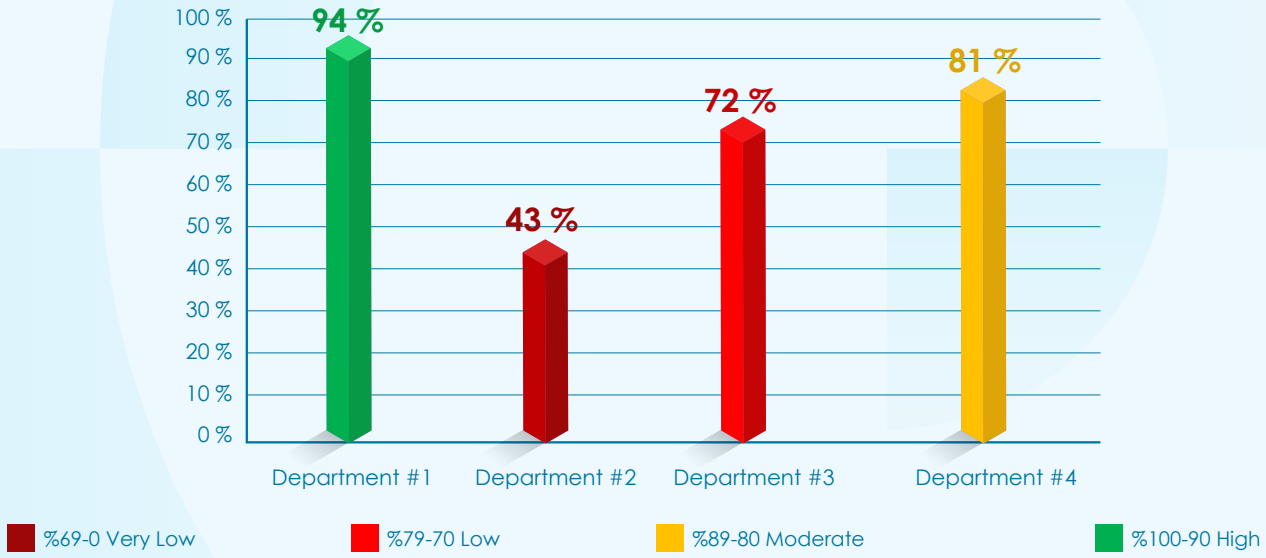


PARTICIPATION INSIGHTS PER DEPARTMENT:

Highest Participation Rate: Department #1 at %100 participation

Lowest Participation Rate: Department #3 at %32 participation.

Awareness Level by Department



This graph shows the average awareness level achieved by all participating employees grouped by their respective departments with their associated risk level.

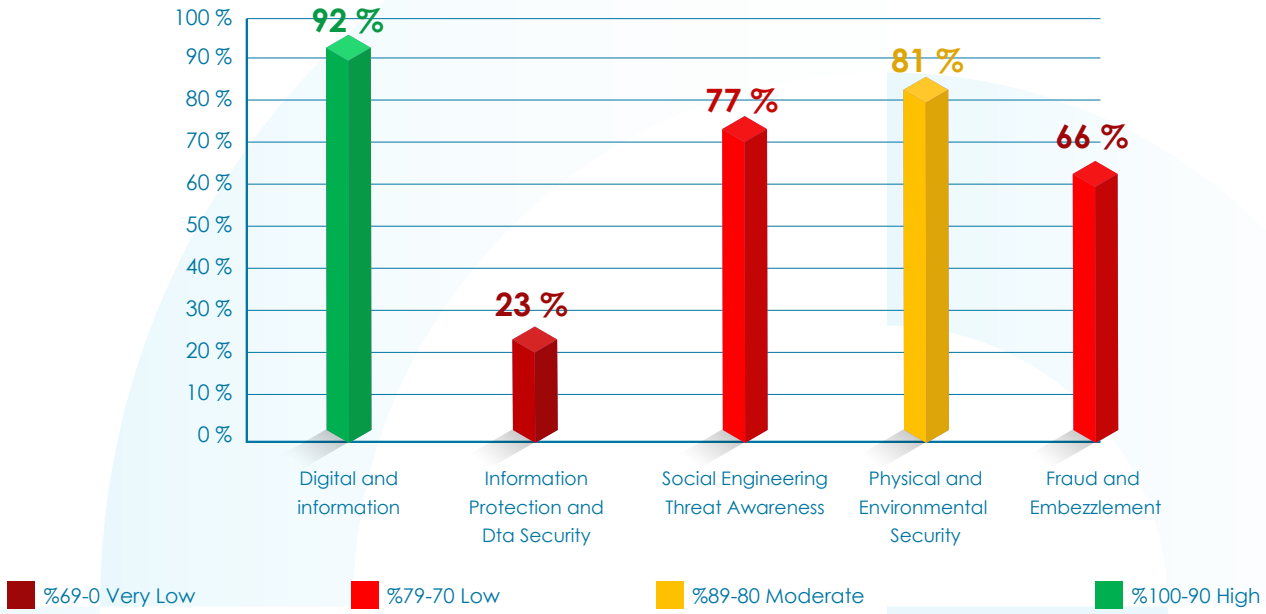
It is made clear that the top three performing departments are:

01 **Department #1 with %94 Awareness Level** — %94

02 **Department #4 with %81 Awareness Level** — %81

03 **Department #3 with %72 Awareness Level** — %72

Awareness Level by Category



This graph shows the average awareness level achieved by all participating employees grouped by category with their associated risk level.

It is highlighted that the two categories "Information Protection and Data Security" and "Fraud and Embezzlement" are the highest categories with an area for improvement.

SUMMARY OF ASSESSMENT RESULTS

Baseline Assessment Score Details

This section outlines the achieved weighted average of all participating employees in each domain.

01 Digital and Online Security

- 44 % Safe Browsing
- 73 % Mobile Security
- 51 % Online Shopping
- 63 % Email Security
- 87 % Wi-Fi Security
- 29 % IoT Security

02 Digital and Online Security

Data Protection

Removable Media Security

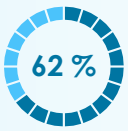
Cybersecurity Hygiene

Secure Passwords

03 Social Engineering and Threat Awareness

Social Engineering

Types of Phishing



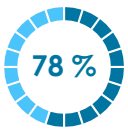
Social Media Security

Executives Awareness

04 Physical and Environmental Security

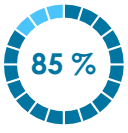
Secure Traveling

Meeting Security



Physical Security

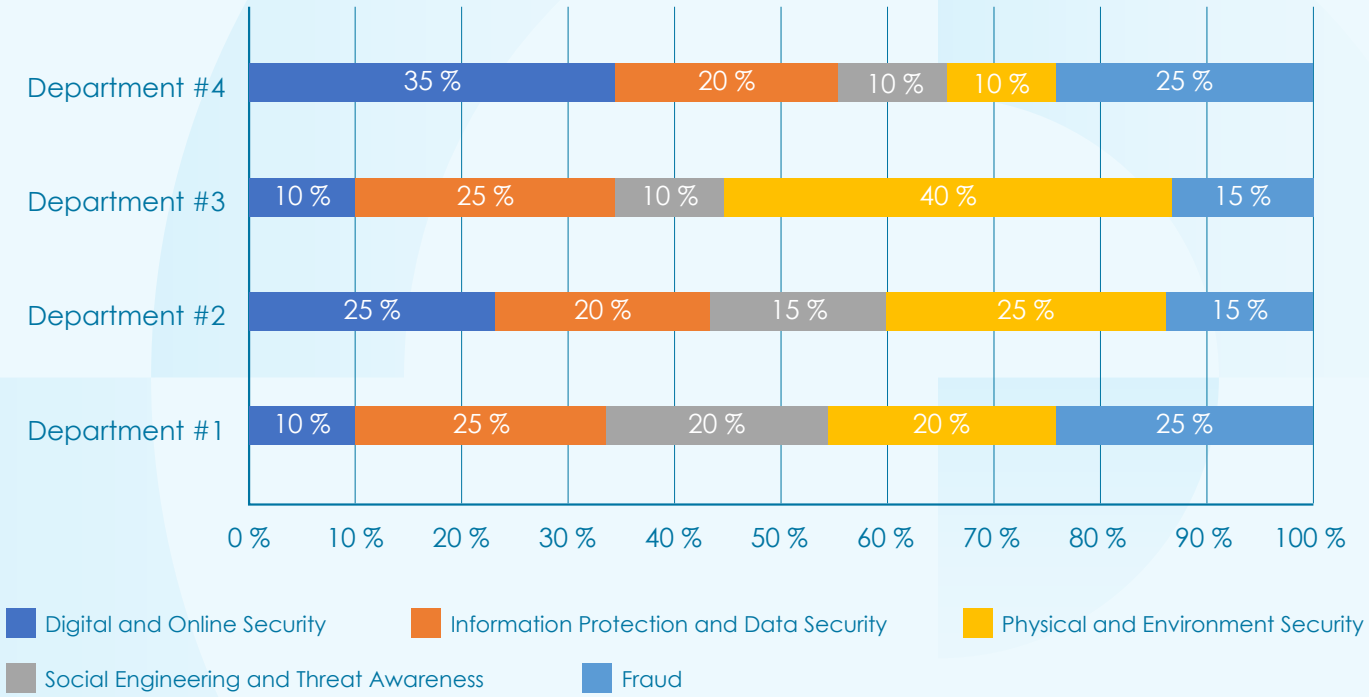
05 Fraud and Embezzlement



Fraud

RELATIVE AWARENESS DISTRIBUTION ACROSS CYBERSECURITY CATEGORIES BY DEPARTMENT

Department Awareness Distribution per Relative Category



This graph shows the relative distribution of correct answers by departments over the 5 categories covered by ZiSoft.

GRAPH FOR DEPARTMENT AND AWARENESS LEVEL (GREEN AND RED).

Category Breakdown

01 Digital and Online Security

Total Number of Questions

Total Number of Incorrect Answers

Total Number of Correct Answers

Overall Score				
Department	Department #1	Department #2	Department #3	Department #4
Safe Browsing				
Mobile Security				
Online Shopping				
Email Security				
Wi-Fi Security				
IoT Security				
Risk	Low	Very High	Moderate	Moderate

02 Information Protection and Data Security

03 Social Engineering and Threat Awareness

04 Physical and Environmental Security

05 Fraud and Embezzlement

DETAILED RESULTS

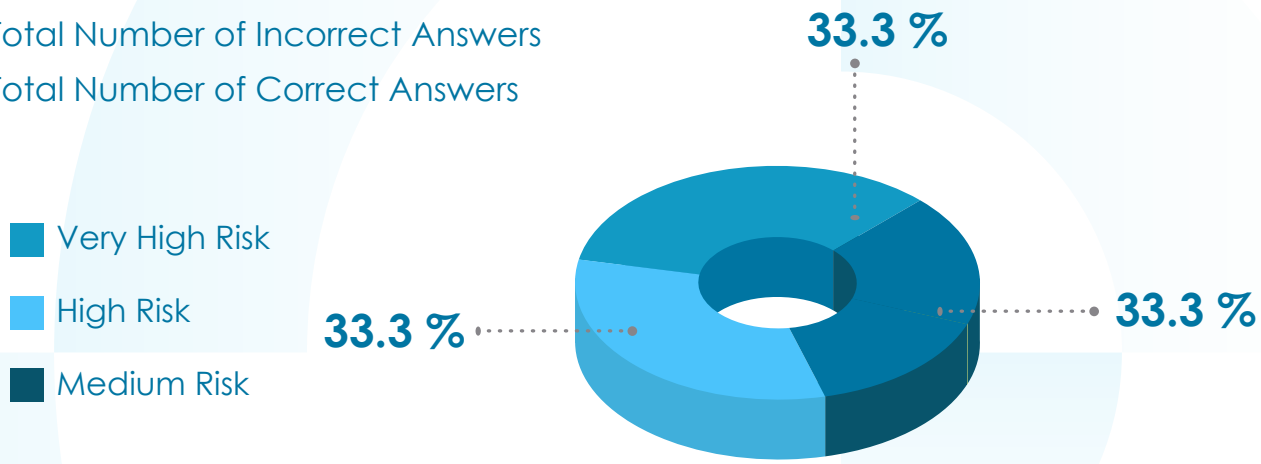
This section performs both a **domain breakdown** and a **departmental analysis** of the assessment results. Each domain is highlighted alongside its associated risk level (average incorrect results), and the average department result.

01 Secure Travelling

Total Number of Questions

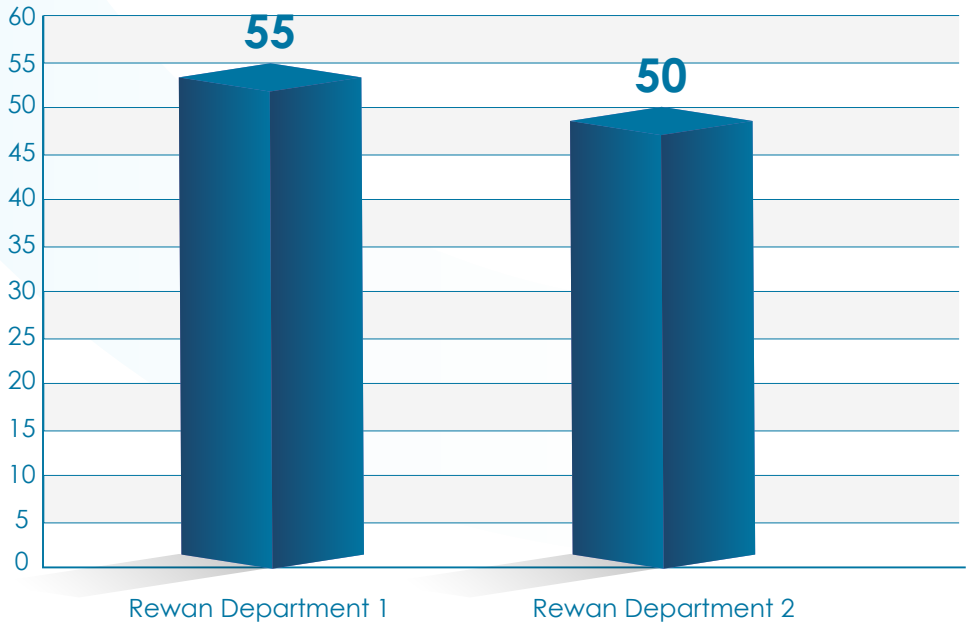
Total Number of Incorrect Answers

Total Number of Correct Answers



This graph displays the average risk levels across all participants for the **'Secure Travelling'** domain, indicating the percentage of incorrect responses. Higher percentages suggest greater risk and potential need for focused training.

Average Result by Department



The average performance of each department in the 'Secure Travelling' domain is shown here, providing insights into areas where additional support may be needed to strengthen awareness.

02 Meeting Security
03 Removable Media Security
04 Safe Browsing
05 Mobile Security
06 Social Media Security
07 Data Protection
08 Online Shopping
09 Cybersecurity Hygiene
10 Fraud
11 Email Security
12 Wi-Fi Security
13 Secure Passwords
14 Physical Security
15 Social Engineering
16 Types of Phishing
17 IoT
18 Executives Awareness

RECOMMENDATIONS

01 Instant Training Campaigns for High-Risk Users
Assign high risk profile users to Instant Training Campaigns covering the most failed domains.

02 Targeted Training on High-Risk (Low-Awareness) Domains
Provide immediate, focused training sessions on domains with the highest risk levels, such as "Secure Travelling" and "Social Engineering."

03 Department Specific Workshops
Organize workshops tailored to departments with lower performance scores in critical areas (e.g. departments with high incorrect answers in "Information Protection and Data Security" category).

04 Create Reference Materials for Common Risks
Develop reference materials (e.g. newsletters, email tips, posters, rollups, infographics, ...etc.) on domains with moderate awareness/risk such as "Physical Security", "Removable Media", and "Secure Passwords."

05 Enhance Participation in Future Assessments (In case of overall participation <%70)
To improve participation in future assessments, implement targeted engagement strategies, such as personalized reminders, departmental incentives, and flexible scheduling options to encourage broader employee involvement.