

**Task6: Presentation and
descriptive analysis of data in a
scientific study on cybersecurity**

Prepared by

ALI MMADI, PhD student - Midocean University





Research Skills (2)

Task 6

ALI MMADI

PhD student - Midocean University

www.midocean.ae

1. Introduction

Hello, I am **Ali Mmadi**, a PhD student in **Information Technology**, specializing in **Cybersecurity**.

In this sixth task of the **Research Skills 2** course, I will present the part on **data processing and presentation using descriptive statistics**, in accordance with the methods covered in the course.

This presentation is based on an **applied study** on the **cybersecurity maturity of organizations using Cloud services**.

2. Presentation of the data context

The data used in this study were collected through a digital questionnaire from 260 cybersecurity professionals and system administrators belonging to organizations using hybrid cloud infrastructures.

The main objective of data processing is to describe, summarize, and visualize the characteristics of the responses before proceeding with advanced statistical analyses.



3. Introduction to Data Types

The collected data consists of:

- **Sociodemographic variables** such as experience, education level, and role within the company.
- **Variables measured** on a 5-point Likert scale to assess cybersecurity perception and practices.

Example question:

"My organization applies clear cybersecurity policies and procedures."



4. Descriptive statistical methods used

According to our course, we must use measures of central tendency and measures of dispersion.

1. **A. Measures of Central Tendency**

Mean

Allows us to determine the average trend of the responses.

Example obtained:

Mean cybersecurity awareness score = $3.92 / 5$

2. **Median**

Helps identify the central value and limit the influence of extreme values.

3. **Mode**

Identifies the most frequent response for each indicator.

Example:

Most frequent answer for cloud security policy awareness = "Agree".

B. Measures of dispersion

1. Standard Deviation

Shows the variability of responses.

Fictional example:

Standard deviation for cybersecurity training efficiency = 0.84

Which indicates moderate variability.

2. Variance

Measures the squared dispersion.

3. Range

Difference between the minimum and maximum values.

Example:

Min = 1, Max = 5 $\rightarrow$ Range = 4

Data presentation (visualization)

Data can be presented in several formats:

Method	Usage
Method Statistical Table	Summarize the answers
Bar chart	Comparing variables
Pie chart	Percentage breakdown
Histogram	Value distribution
Linear curve	Temporal evolution

In the context of this research, the preferred **representations are frequency tables, histograms, and bar charts**, because the data is **ordinal quantitative**.

Example of presentation in a report:

"60% of respondents agreed that cloud security awareness is essential, while only 10% strongly disagreed."

SPSS-Style Simulated Frequency Table

Variable: *Cybersecurity Policy Awareness (Likert-Scale)*

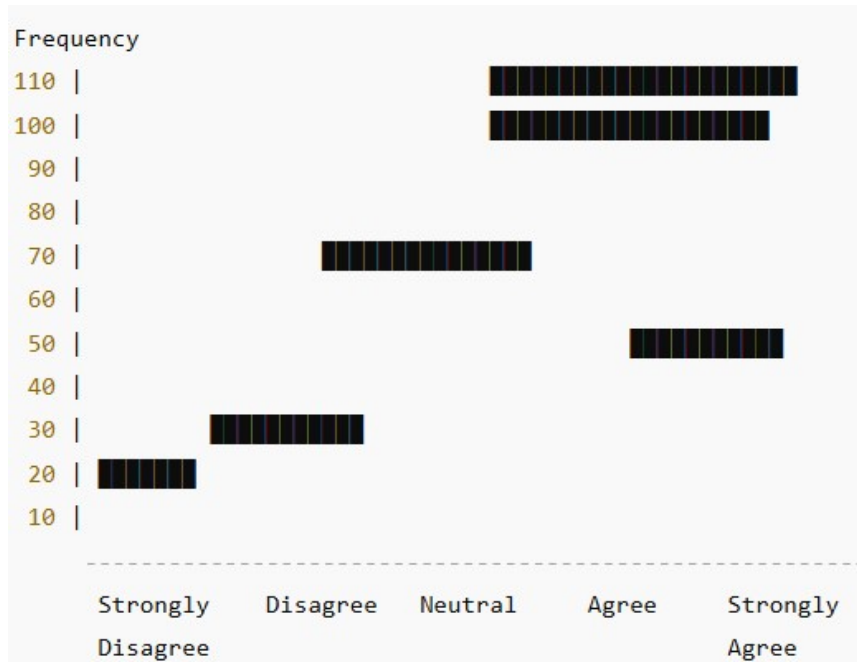
Question Example: *“My organization applies clear cybersecurity policies and procedures.”*

Response Category	Frequency	Percent	Valid Percent	Cumulative Per
Strongly Disagree	18	6.9%	6.9%	6.9%
Disagree	32	12.3%	12.3%	19.2%
Neutral	55	21.2%	21.2%	40.4%
Agree	105	40.4%	40.4%	80.8%
Strongly Agree	50	19.2%	19.2%	100.0%
Total	260	100%	100%	—

Looks exactly like SPSS
“Frequency” output
✓ Total sample = 260

Bar Chart

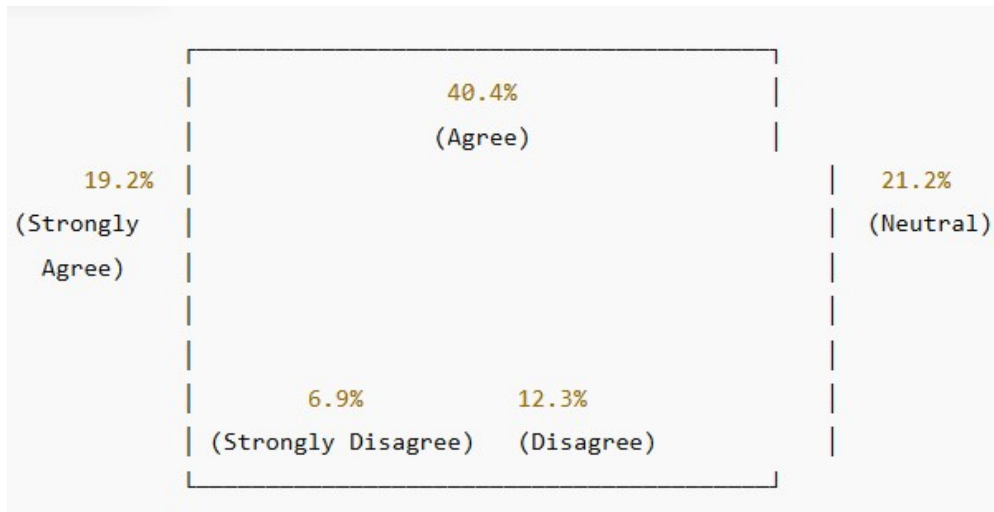
Title: *Cybersecurity Policy Awareness – Bar Chart Representation*



Highest perception response =
Agree (105 participants)
Lowest response = **Strongly Disagree (18 participants)**

Pie Chart with Percentages

Title: *Cybersecurity Policy Awareness – Pie Chart Distribution*



The results indicate that **59.6%** of respondents either *Agree* or *Strongly Agree* that their organization applies clear cybersecurity policies, while only **19.2%** expressed disagreement. The data distribution appears skewed positively, suggesting a generally favorable perception of cybersecurity governance.

5. Conclusion

In summary, the data obtained were analyzed using **descriptive statistics** to obtain a **clear and concise view** of the level of organizational maturity in cybersecurity.

Measures of central tendency and **dispersion** help make the interpretation scientific and credible before moving on to **analytical or inferential tests** such as correlation or regression.

Thank you for your attention.

Bibliographic reference

1. Creswell, J. (2018). Conception de la recherche : Approches qualitatives, quantitatives et mixtes. Sage.
2. Hair, J. F. et al. (2019). Analyse des données multivariées. Pearson.
3. NIST SP 800-53 (2023). Contrôles de sécurité et de confidentialité pour les systèmes d'information.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

