

**Design and validation of a cybersecurity
research questionnaire: nature of the
data, collection tools, and reliability
testing**

Prepared by

ALI MMADI, PhD student - Midocean University





Research Skills (2)

Task 4

ALI MMADI

PhD student - Midocean University

www.midocean.ae

1. Introduction

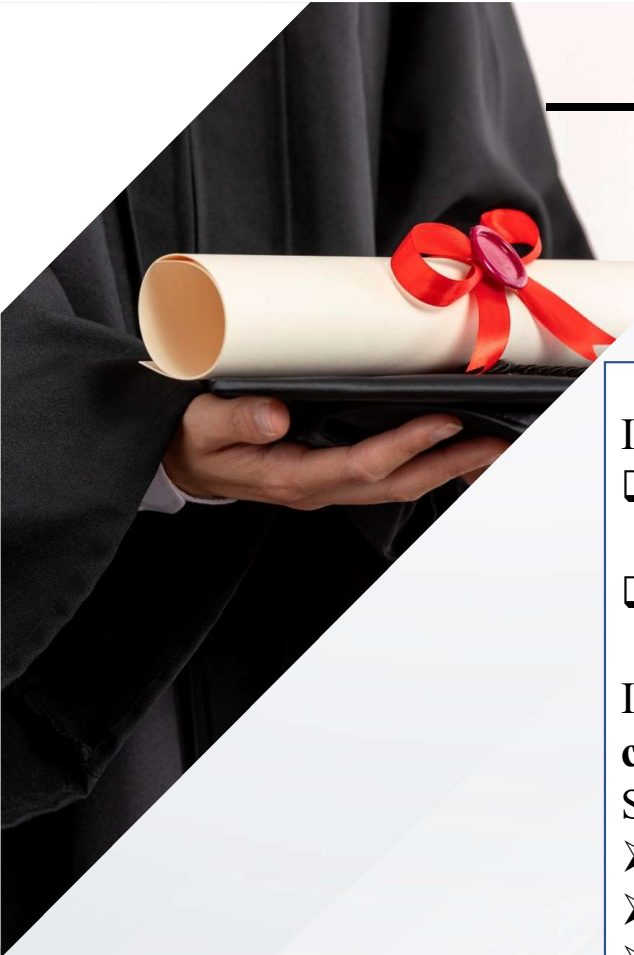
Hello,

My name is Ali Mmadi, a PhD student in Information Technology, specializing in Cybersecurity.

In this fourth task of the Research Skills 2 course, I will present:

- The nature of the data used in cybersecurity research,
- The data collection tools,
- The design of a questionnaire,
- And finally, the statistical tests of reliability and validity applied to the questionnaire.

My example is based on a study on information system security in Cloud environments.



2. Nature of the data and sources of collection

In cybersecurity research, data can be of two types:

- ❑ **Quantitative data, expressed in numbers, for example the rate of detected incidents, the number of vulnerabilities, or compliance scores.**
- ❑ **Qualitative data, expressed in words or opinions, for example users' perceptions of security or attitudes toward risk.**

In my field, data is often **primary**, meaning it is **collected directly from cybersecurity professionals**, system administrators, and Cloud engineers.

Secondary sources can include:

- Incident reports from the CERT,
- Scientific publications,
- And vulnerability databases such as the National Vulnerability Database (NVD).

These two types of sources allow for a comprehensive view, **both technical and human**, of the studied phenomenon.

3. Data collection tool: the questionnaire

The data collection tool chosen for this research is the electronic questionnaire, distributed via Google Forms or **Microsoft Forms**.

The questionnaire is a **practical, cost-effective, and objective instrument**, suitable for surveying a large number of experts or users remotely.

Within the framework of a cybersecurity study, the questionnaire consists of three main areas:

Area 1: Awareness of cybersecurity.

- **Example question: 'I understand the risks associated with social engineering.**
- **'Responses on a 5-point Likert scale: from 'Strongly disagree' to 'Strongly agree'.**

Axis 2: Organizational practices and security policies.

Example question: "My organization has clear password management policies."

Axis 3: User trust and behavior.

Example: "I always check the source of an email before clicking on a link."

These questions help measure cybersecurity maturity within the studied organizations.

4. Questionnaire design and structure

To design a reliable research questionnaire, the researcher follows several methodological steps:

- 1) Define the research problem: for example, "What are the human factors influencing the security of Cloud systems?"
- 2) Identify the main variables (behavior, awareness, internal policies).
- 3) Formulate clear and neutral questions, avoiding ambiguous terms.
- 4) Use a consistent measurement scale (for example, a 5-point Likert scale).
- 5) Conduct a pretest of the questionnaire with a small group of participants to ensure understanding.

This preliminary phase is essential to ensure **the content validity** of the questionnaire, in accordance with scientific research standards.

5. Reliability and validity of the questionnaire

Once the data is collected, the researcher must verify the **reliability** and **validity** of the questionnaire.

- ❑ **Validity refers to the ability of the instrument to measure what it is supposed to measure. It can be verified by:**
 - ❑ **The content validity test, using expert opinions;**
 - ❑ **The construct validity test, through the analysis of internal correlations.**
- ❑ **Reliability is checked using Cronbach's Alpha test, with software such as SPSS or Python (pandas/statsmodels).**

A Cronbach's Alpha value greater than 0.7 indicates good internal consistency of the questionnaire.

For example, in my study on Cloud cybersecurity, the alpha obtained for the questionnaire is 0.82, which demonstrates its high reliability.

5. Conclusion

In conclusion:

The collection of reliable data is essential for any scientific research.

In cybersecurity, primary data through questionnaires allows understanding of human and organizational factors.

The questionnaire design must be methodical, clear, and validated.

Finally, tests such as Cronbach's Alpha ensure the scientific credibility of the research. Thank you for your attention.

Bibliographic reference

1. References (to be mentioned in the written report)NIST (2021). Guide to Intrusion Detection and Prevention Systems (IDPS), SP 800-94.
2. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate Data Analysis (8th ed.). Pearson.
3. Creswell, J. W. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage.
4. ISO/IEC 27001:2022 – Information Security Management Systems — Requirements.
5. Tavakol, M., & Dennick, R. (2011). Making Sense of Cronbach's Alpha. International Journal of Medical Education, 2, 53–55.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

