Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

DIGITAL TRUST

member of
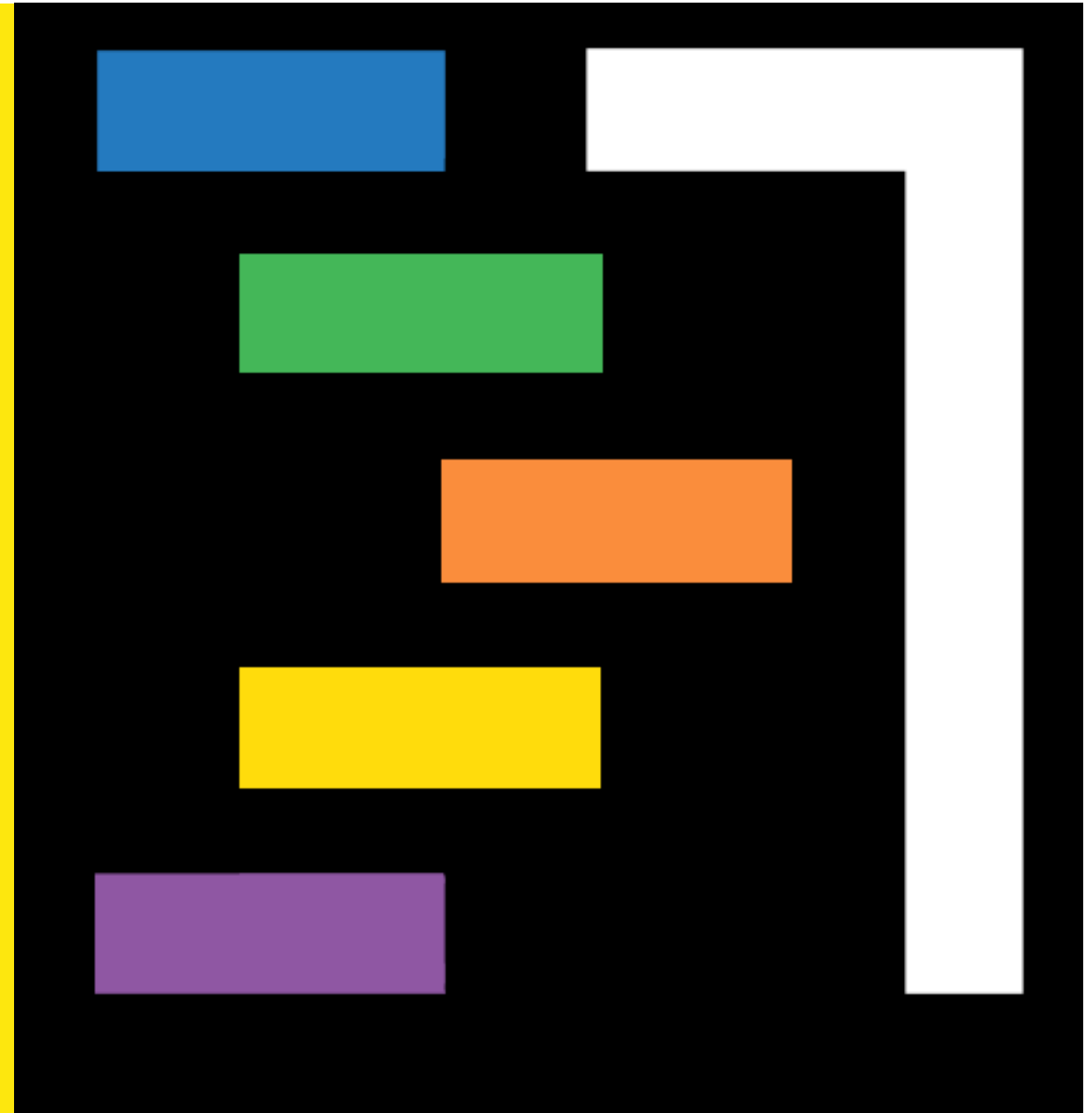swissuniversities

AACSB ACCREDITED

- **The Cultural Factors in Cybersecurity**

- **Swiss-Africa Cybersecurity Community**

Franka Ebai

Research Assistant
University of Applied Sciences Northwestern Switzerland
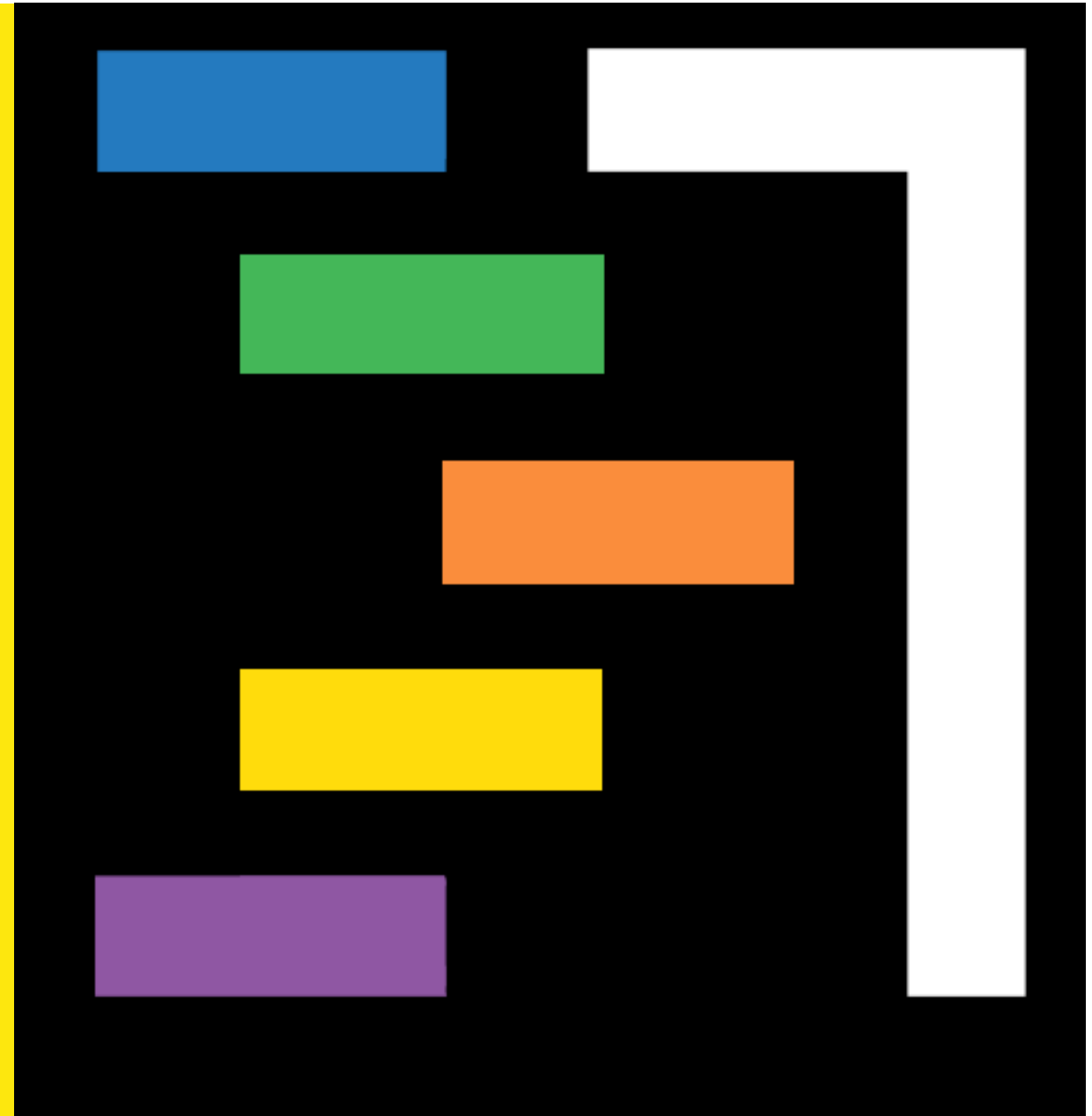
March 25

The Cultural Factors in Cybersecurity

Partnering Institutions:

University of Applied Sciences Northwestern Switzerland

(FHNW) & Biaka University Institute of Buea

Project Sponsor: Leading House Africa

Franka Ebai

March 25

Agenda

➢ Background

➢ Literature review

➢ Research questions and objectives

➢ Theoretical framework

➢ Methodology and data analysis

➢ Results and discussion

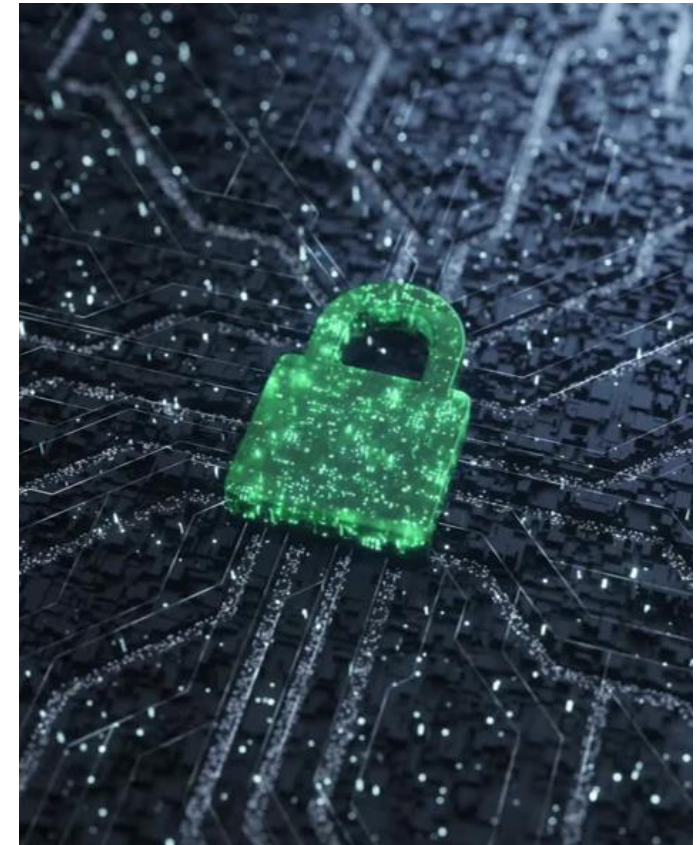➢ Conclusion and areas for further research

➢ Questions & answers

01

BACKGROUND

Background (1/3)

Cybersecurity:

- The preservation of confidentiality, integrity and availability of information in Cyberspace (ENISA, 2015).

- Global security rose by 38% in 2022, and security transcends borders.

- The WannaCry Ransomware affected over 150 countries (SentinelOne, 2024).

- Cybersecurity affects both SMEs and big corporations.

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

BIAKA UNIVERSITY INSTITUTE OF
BUEA -BUIB
Knowledge & Service To Humanity

DIGITAL
TRUST

member of
swissuniversities

AACSB
ACCREDITED

Background (2/3)

The Link to National Culture:

- Past studies show that attention is mainly on the technical aspects of cybersecurity.

- While humans remain the weakest link in the cybersecurity chain, less attention is given to human elements, and worse still, the cultural aspects.

- Every individual is born into a culture.

- Cultural background influences our way of life, beliefs, attitudes, values, decision-making, etc.

- How does cultural background influence individuals' actions and attitudes towards cybersecurity?

Background (3/3)

The Link to Organisational Culture:

- This refers to how people within an organisation relate to each other, their work, and to the outside world.

- It comprises shared assumptions, values, beliefs, and what behaviour is considered appropriate or inappropriate by the members within the organisation.

→ How does organisational culture influence employees' actions and attitudes towards cybersecurity?

02

LITERATURE REVIEW

The Gap in Literature

Human aspects & cybersecurity attitude → Great Coverage	National Culture and Cybersecurity	Organisational Culture and Cybersecurity
e.g., trust, user personality, risk-taking, language, personal initiative	▪ Main focus is on country-level cybersecurity development. e.g., influence of power distance, individualism, uncertainty avoidance, etc	▪ Main focus is on broader organisational culture. e.g. security culture, leadership, training, etc

Identified Gaps:

Limited research on…

✓ culture and individual cybersecurity behaviour

✓ implicit organisational culture and cybersecurity

✓ how to integrate culture into cybersecurity education

03

RESEARCH QUESTIONS & OBJECTIVES

Research Questions & Objectives

1. What cultural factors play a significant role in the field of cybersecurity?

   ✓ The influence of national culture

   ✓ The influence of organisational culture

2. How can these cultural elements be addressed in cybersecurity education?

Objective 1	Objective 2	Objective 3
To investigate the role of national culture in human cybersecurity behaviour in Switzerland and in Cameroon.	To investigate the role of organisational culture in human cybersecurity behaviour in Switzerland and in Cameroon.	To develop guidelines for incorporating the identified cultural elements in cybersecurity education.

04

THEORETICAL FRAMEWORK

Theoretical Framework

1. Hofstede Cultural Dimensions:

- Six cultural dimensions differentiating groups of individuals in one country from another country.

  o Power distance; Individualism; Motivation towards achievement and success; Uncertainty avoidance; Long-term orientation; and Indulgence.

→ **Based on these dimensions, Cameroon & Switzerland are culturally different.**

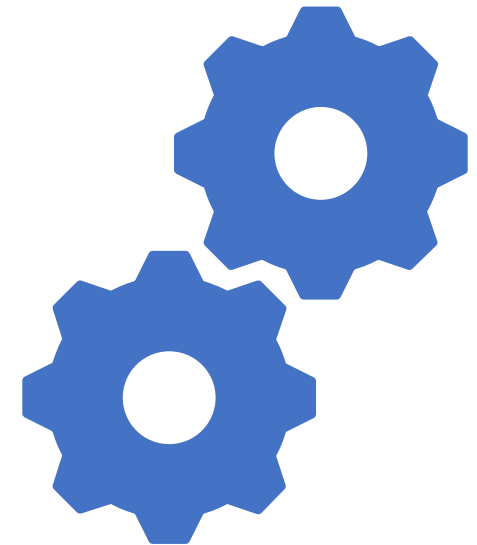   → How do these dimensions relate to cybersecurity human behaviour?

05

METHODOLOGY & DATA ANALYSIS

Methodology

- **Research Design:**

  o Cross-sectional design

- **Data Collection Method:** Qualitative approach

  o Episodic Interviews and Focus groups

    ✓ 9 episodic interviews in Switzerland & 6 episodic interviews in Cameroon

    ✓ 1 focus group discussion in Switzerland & 2 focus group discussions in Cameroon

- **Participants:**

  o CTOs, cybersecurity educators, specialists & students (IT, business, etc)

- **Data Analysis:**

  o In-vivo and descriptive methods of coding → to stay close to participants' words.

06

RESULTS & DISCUSSION

n|w Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

BIAKA UNIVERSITY INSTITUTE OF
BUEA -BUIB
Knowledge & Service To Humanity

DIGITAL TRUST

member of
swissuniversities

AACSB
ACCREDITED

Objective #1 – Based on Interviews in Cameroon

➢ **The influence of national culture on human cybersecurity behaviour:**

Cameroon	
• **Cultural vulnerability:** ✓ Lack of cybersecurity resources in local languages & that match the country's cultural diversity. • **Government policies:** ✓ Lack of stringent cybersecurity policies. • **Resistance to change:** ✓ Unfamiliarity with technology breeds reluctance to embrace digital cybersecurity measures.	• **Attitude to sharing & trust** ✓ A collectivist approach to sharing common knowledge & experience leads to a positive cybersecurity attitude. ✓ Blind trust could be a danger to cybersecurity.

Objective #1 – Based on Interviews in Switzerland

➢ **The influence of national culture on human cybersecurity behaviour:**

Switzerland	
• **State policies:** ✓ The role of the state to enforce cybersecurity policies. • **Attitude towards the unknown** ✓ Some Swiss tend to question unfamiliar cybersecurity policies.	• **Trust** ✓ Cultures that are too trusting could be susceptible to cyberattacks. • **Approach to privacy:** ✓ Keeping digital identities private positively impacts one's cybersecurity attitude. ✓ Some people may hold back from sharing their experiences with cyberattacks.

Objective #2 – Based on Interviews in Cameroon

➢ **The influence of organisational culture on human cybersecurity behaviour:**

Cameroon	
• **Organisational environment:** ✓ Lack of cybersecurity culture in most Cameroonian companies, increasing the likelihood of cyber threats. ✓ Internal envy/jealousy may lead to the breaking of security protocols. • **Organisational policy & governance:** ✓ Limited enforcement of cybersecurity policies and regulations.	• **Training & awareness:** ✓ Some companies fail to provide cybersecurity training. • **Company structure & vision:** ✓ Lower-level employees may hold back from sharing their views in very hierarchical structures. ✓ Unclear vision and objectives hinder employees' commitment to a company's cybersecurity goals.

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

BIAKA UNIVERSITY INSTITUTE OF
BUEA -BUIB
Knowledge & Service To Humanity

DIGITAL TRUST

member of
swissuniversities

AACSB
ACCREDITED

Objective #2 – Based on Interviews in Switzerland

➢ **The influence of organisational culture on human cybersecurity behaviour:**

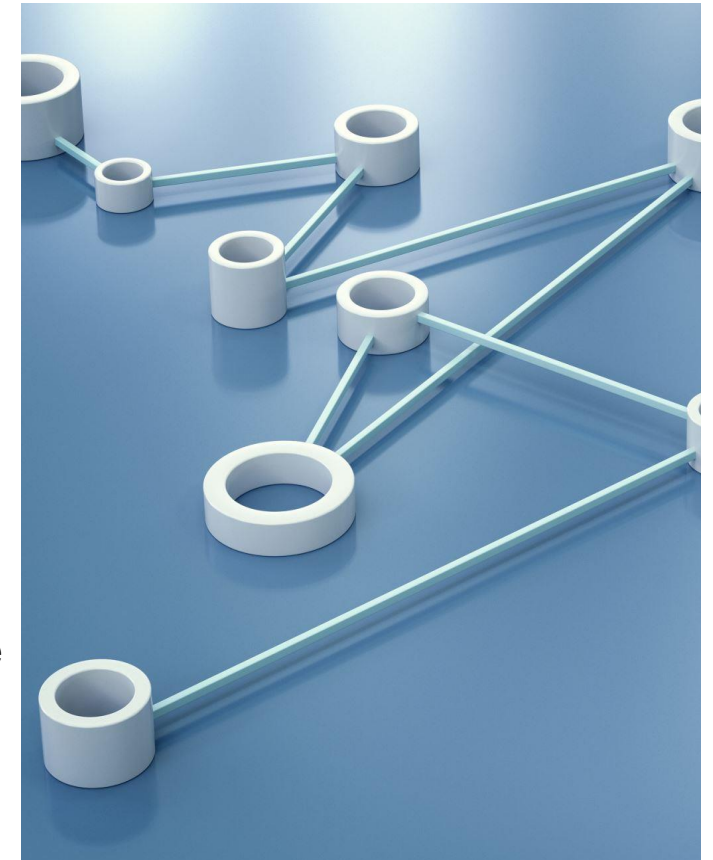| Switzerland	
• **Transparent communication:** ✓ To let employees know the company's stands regarding cybersecurity. • **Maintaining a security culture:** ✓ Physical security measures ✓ Develop a cybersecurity mindset from top to bottom.	• **Authority & hierarchy:** ✓ Hierarchies increase dependency on leaders, hence negative impact. • **Training and development:** ✓ Equips employees with the right tools.

Linking Objectives 1 & 2 to Hofstede Cultural Dimensions

1. **Power Distance**:

- The existence of hierarchies influences people's attitudes to cybersecurity.

    ✓ In high power-distance cultures, people in lower positions may become too dependent.

    ✓ In low-power distance cultures, the need for consensus may slow down decision-making.

2. **Individualism / Collectivism:**

- **Collectivism**:

    ✓ Collectivistic tendencies, such as sharing common knowledge, positively influence people's attitudes toward cybersecurity.

    ✓ Trust, especially blind trust, exposes people to cyber threats.

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

BIAKA UNIVERSITY INSTITUTE OF
BUEA -BUIB
Knowledge & Service To Humanity

DIGITAL TRUST

member of
swissuniversities

AACSB
ACCREDITED

Linking Objectives 1 & 2 to Hofstede Cultural Dimensions

- **Individualism:**
  - ✓ Knowledge of privacy leads to a positive cybersecurity attitude.
  - ✓ Prioritising individual needs above that of the group hinders the building of a cybersecurity culture.

3. Uncertainty avoidance:

- Critically assessing/ questioning the unknown breeds a positive attitude to cybersecurity.

- Resisting the unknown, especially digital security measures, increases the risks to cybersecurity.
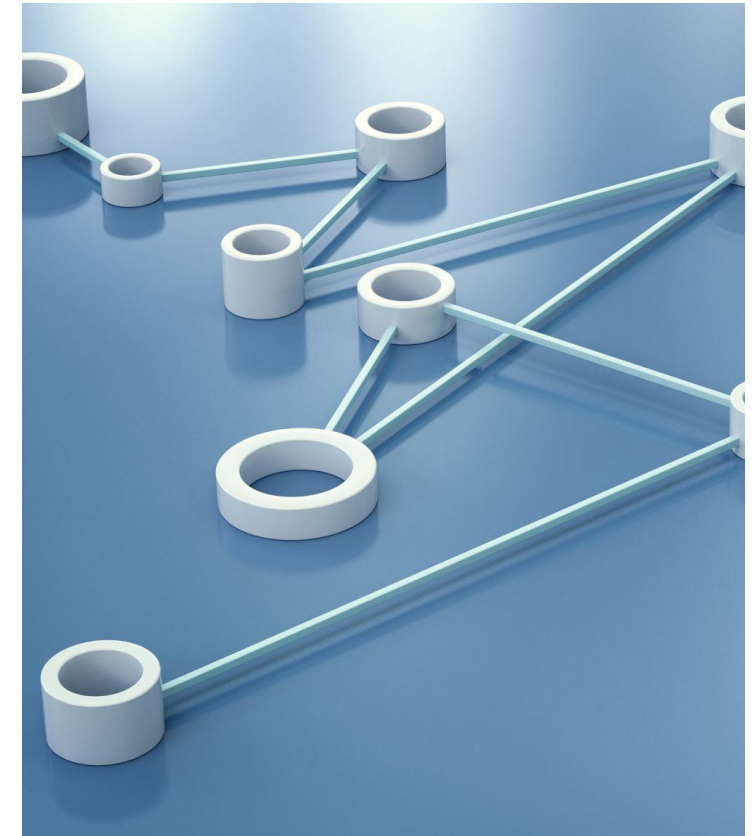
Objective #3 – Recommendations

➢ **Integrating Cultural Elements into Cybersecurity Education**

Recommendations to Educational Institutions:

✓ Expose cybersecurity/IT students to cultural modules and other cultures.

✓ Design an elective or sub-module covering culturally influenced cyberattacks, incidents, and solutions.

Recommendations to Educational Institutions & Companies:

✓ Recognise the role of culture in the field of cybersecurity.

✓ Train (cybersecurity) leaders on the cultural aspects of cybersecurity.
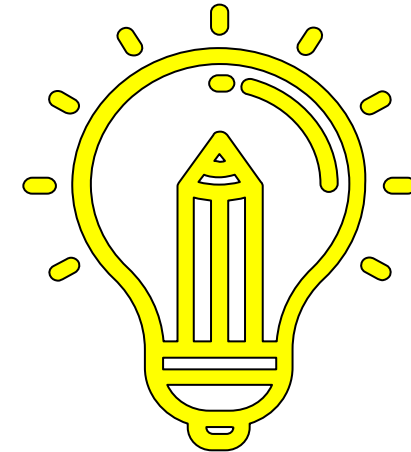
Recommendations to Companies

✓ Provide intercultural training to security/IT staff.

✓ Match cybersecurity training to the cultural norms influencing your organization.

CONCLUSION & AREAS FOR FURTHER RESEARCH

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

BIAKA UNIVERSITY INSTITUTE OF
BUEA -BUIB
Knowledge & Service To Humanity

DIGITAL
TRUST

member of
swissuniversities

AACSB
ACCREDITED

Conclusion

- Addition to the discussion on cybersecurity and culture

  - ✓ New findings relating to culture and individual cybersecurity behaviour.

  - ✓ Recommendations on how to integrate culture into cybersecurity education and training.

- Policymakers can use our findings when designing and enforcing cybersecurity policies.

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

BIAKA UNIVERSITY INSTITUTE OF
BUEA -BUIB
Knowledge & Service To Humanity

DIGITAL
TRUST

member of
swissuniversities

AACSB
ACCREDITED

Areas For Further Research

- **Focus on the same topic and research questions**

  ✓ Adopt a quantitative approach to test the findings.

  ✓ Consider participants from more regions in Cameroon and
    Switzerland.

  ✓ Research the applicability of the recommendations and how to
    design a module that links culture and cybersecurity.

March 25