Poster: Experts' Perceptions on Factors Impacting Cybersecurity Culture in Organizations

Hannah Sievers
ETH Zurich
Zurich, Switzerland
hannah.sievers@gess.ethz.ch

Neele Roch
ETH Zurich
Zurich, Switzerland
neele.roch@gess.ethz.ch

Verena Zimmermann
ETH Zurich
Zurich, Switzerland
verena.zimmermann@gess.ethz.ch

***Abstract*—We explored expert perspectives on factors that impact cybersecurity culture in organizations and synthesized the insights into an actionable framework. To achieve this, we conducted an interview study with *N* = 30 experts in the field. We found that important factors impacting cybersecurity culture are leadership, organizational values, cybersecurity risk assessment, policies and regulations, communication, and cybersecurity training. From these factors and their relationships, we derive steps to promote cybersecurity culture.**

I. Introduction

Cybersecurity remains a prevalent issue affecting organizations across industries, with threats targeting the human factor growing in both scale and sophistication [1]. Developing or strengthening the cybersecurity culture is thus considered to be a pertinent measure for organizations to ultimately foster awareness and secure behaviors among their employees [3]. However, enhancing cybersecurity culture to mitigate human-targeted attacks presents a challenge, as the factors and drivers of cybersecurity culture are not well understood, with a multitude of dimensions existing in the literature [4]. The lack of consistent factors contributing to cybersecurity culture makes it difficult for organizations to recognize and implement changes. We draw on expert insights to identify and synthesize relevant dimensions of cybersecurity culture into an actionable framework. Therefore, our objective was to answer the following research questions:

RQ1: What is the experts' understanding of cybersecurity culture and awareness in organizations?

RQ2: Which factors impact an organization's cybersecurity culture from an expert's perspective?

RQ3: How do the factors impact an organization's cybersecurity culture from an expert's perspective?

RQ4: What measures do the experts see as effective in improving an organization's cybersecurity culture and how can they be applied to the factors?

We addressed these questions by conducting semi-structured interviews with experts from the field of information security, as well as other areas that may intersect with cybersecurity culture. In the following, we will describe the study procedure, as well as preliminary findings regarding RQ2 and RQ3.

II. Study Method

The study was carried out in two steps. In a first step, we derived an initial list of factors based on a workshop with industry project partners as well as findings from existing literature [4]–[6]. In a second step, and the main part of the project, we conducted semi-structured interviews, mainly focusing on discussing and extending the previously collected factors as described in the following subsection.

A. Interview Procedure

The semi-structured interviews consisted of three sections.

1) The first section focused on the experts' understanding of cybersecurity culture and awareness in organizations.
2) The second section focused on which factors the experts considered to be impactful with regard to cybersecurity culture, their expressions, their interrelations, and their relative importance compared to each other. This section was accompanied by a card sorting task during which the experts were asked to sort, arrange, and structure cards representing the collected factors, to not only facilitate, but also to visualize and document their responses.
3) The third and final section concerned potential measures to assess and enhance an organization's cybersecurity culture.

B. Recruitment and Sample

The experts were mainly recruited through purposive and snowball sampling and required a minimum of 3 years of working experience or a degree in the fields of either information security, safety, organizational psychology/management, or communication. A total of *N* = 30 experts were interviewed between late January and early April 2025. The study design was approved by the ethics board of ETH Zurich. All participants were fully informed about the content and purpose of the study before participating and willingly provided their consent.

C. Data Analysis

We analyzed the interview data following a grounded theory approach, using memoing and diagramming techniques to aid the analytical process [2]. We analyzed the results of the card sorting task by quantifying the frequency and relative importance (out of 'critical', 'important' and 'nice to have') ascribed to each factor, as well as their relationships to each other.

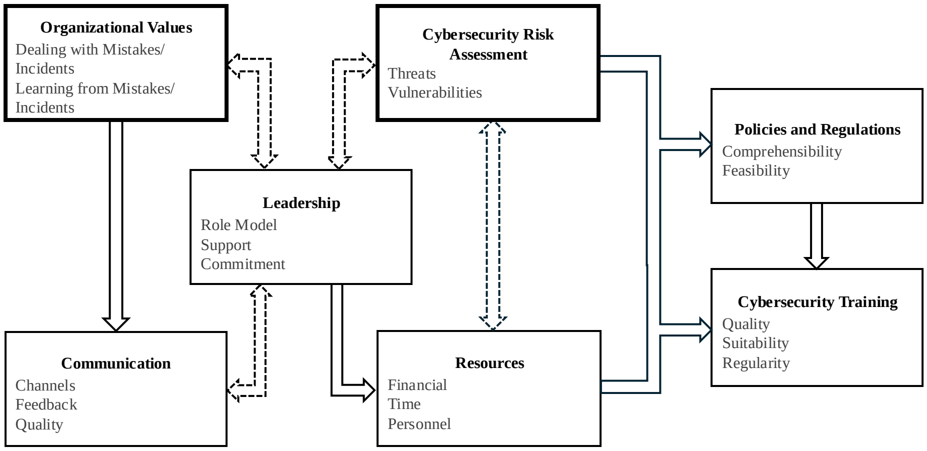


Fig. 1. Derived Cybersecurity Culture Framework

III. Preliminary Results

The majority of the participants identified leadership (*n* = 24), organizational values (*n* = 19), communication (*n* = 26), resources (*n* = 22), cybersecurity training (*n* = 20), cybersecurity risk assessment (*n* = 18), and policies and regulations (*n* = 18) as at least important factors for impacting an organization's cybersecurity culture. Participants highlighted the importance of leadership as role models, their support and commitment to the topic, as well as the presence of clear organizational values. A constructive approach to mistakes and incidents was especially emphasized. Communication should be transparent, comprehensible, and include opportunities for feedback and to exchange information informally. Not only financial resources, but also resources in terms of personnel and time were highlighted. Cybersecurity training should impart useful knowledge, be practical for daily life, customized to the context of the job and organization, and take place regularly to consolidate the knowledge conveyed. Risk assessments serve to identify threats, vulnerabilities, and corresponding gaps in the organization. Finally, clear and comprehensible cybersecurity policies should provide guidance and be able to be implemented accordingly.

The relationships set in the card sorting task, as well as the participants' corresponding statements revealed directions and conditions of action, i.e., which factors presuppose others, and, in turn, form a prerequisite for others. According to the participants, organizational values and risk assessment form the building blocks of an organization's cybersecurity culture. The values, especially the way mistakes and incidents are handled in an organization are "*very, very central. The whole thing more or less stands or falls with them*" (P7). Likewise "*we have to have a risk assessment* [...] *and quite frankly not just for culture or awareness, but* [...] *that we can exist as a company*" (P24). Figure 1 displays the preliminary framework, consisting of the factors outlined above, their characteristics as highlighted by the experts, as well as their respective relationships.

IV. Discussion

The preliminary results allow us to derive a sequence of steps that can be taken to promote an organization's cybersecurity culture. First, the results highlight the need to address *organizational values* and *risk assessment* early on. Second, *leadership* should be informed about the relevance of cybersecurity, the importance of their commitment, and their function as role models. Respective values and risks can be used to communicate these aspects to leadership. Third, structured *communication channels* for information dissemination and feedback opportunities should be created, as well as informal exchange opportunities among employees. Fourth, based on the results of the *risk assessment* and the *resources* made available by *leadership*, *policies and regulations* can be further developed and made available to employees in a simplified form, and appropriate and customized *trainings* can be created.

Our study is limited to Swiss and German experts. Furthermore, the results are based on experts' experience and expertise and are indicative in a first step. More research is needed to further examine the factors and their interrelations.

Acknowledgment

This study is funded by 74818.1 INNO-SBM.ne

References

[1] APWG. (2024). Phishing activity trends report. https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf

[2] Birks, M., & Mills, J. (2023). *Grounded theory. A practical guide* (3rd ed.). SAGE.

[3] ENISA. (2017). *Cyber security culture in organisations*. https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-3-1%20Cyber%20Security%20Cultures%20in%20Organizations.pdf

[4] Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12-22. https://doi.org/10.1016/j.jisa.2018.11.003

[5] Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behavior framework: A rapid evidence review. *Computers & Security, 148*, Article 104110. https://doi.org/10.1016/j.cose.2024.104110

[6] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture. Current practices and future needs. *Computers & Security, 109*, Article 102387. https://doi.org/10.1016/j.cose.2021.102387

ETH zürich

SECURITY
PRIVACY
SOCIETY

Experts' Perceptions on Factors Impacting Cybersecurity Culture in Organizations

Hannah Sievers, Neele Roch, Verena Zimmermann
Security, Privacy and Society, ETH Zurich

1. MOTIVATION

- □ **Strengthening cybersecurity culture is vital** for promoting employee awareness and secure behaviors, yet **inconsistent contributing factors make it challenging for organizations to identify and implement changes.**
- □ We draw on **expert insights to identify and synthesize relevant dimensions of cybersecurity culture** into an actionable framework.

3. STUDY METHOD

- □ We conducted **semi-structured interviews** with ***N* = 30 experts** in the field between late January and early April 2025.
- □ Interviews were accompanied by a **card sorting task** to discuss and enhance pre-collected factors.
- □ **Topics discussed:** Impactful factors, their expression, interrelations, and relative importance.

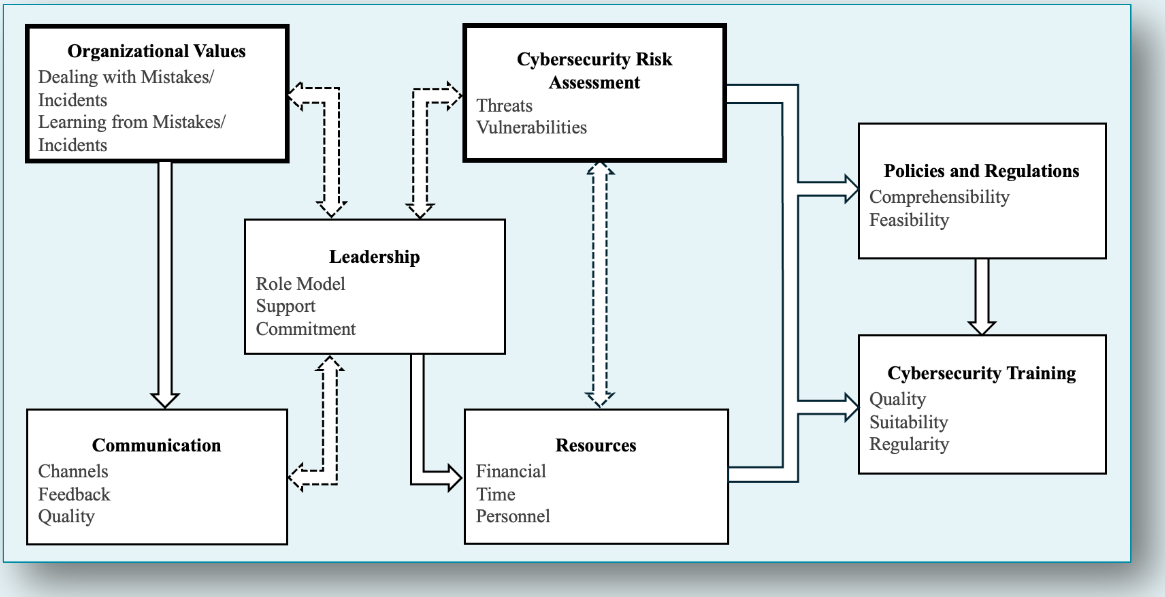
2. SELECTED RESEARCH QUESTIONS

- □ Which factors impact an organization's cybersecurity culture from an expert's perspective?
- □ How do the factors impact an organization's cybersecurity culture from an expert's perspective?

4. PRELIMINARY RESULTS

- □ **Derived framework** of important factors and their interrelations, with **organizational values** and **risk assessment** forming the **building blocks.**
- □ From the framework, **a sequence of steps** can be derived **to promote cybersecurity culture:**

1. Addressing **values and risk assessment**
2. Obtaining **leadership support and resources**
3. Establishing **communication channels**
4. Further **developing policies and trainings** based on the results of the risk assessment and resources available



Organizational Values
Dealing with Mistakes/ Incidents
Learning from Mistakes/ Incidents

Cybersecurity Risk Assessment
Threats
Vulnerabilities

Leadership
Role Model
Support
Commitment

Policies and Regulations
Comprehensibility
Feasibility

Cybersecurity Training
Quality
Suitability
Regularity

Communication
Channels
Feedback
Quality

Resources
Financial
Time
Personnel

5. FUTURE DIRECTIONS

- □ **Validation of the framework in different settings**, e.g., company sizes, industries, and countries.
- □ **Assessing the cultural impact** on which factors are considered important regarding cybersecurity culture.

Contact:
Hannah Sievers
hannah.sievers@gess.ethz.ch

More information here: