Structuring Cybersecurity Hygiene Indicators: Automated Assessment Complexity, Data Privacy and Indicator Prioritisation

Faustas Litvinaitis, Simona Ramanauskaitė

Fontys University of Applied Sciences, Vilnius Gediminas Technical University

Introduction

Cybersecurity hygiene is an essential part of everyday computer use. Interactive tools can complement traditional education by providing guidance when users encounter insecure settings or potentially unsafe practices. Such guidance requires meaningful indicators that can be assessed reliably from an end-user device while respecting privacy.

Existing instruments, including the Security Behavior Intentions Scale and the Cyber Hygiene Inventory, describe multiple dimensions of cybersecurity behaviour. However, translating these concepts into automated endpoint assessment presents a methodological challenge: measurable device conditions do not necessarily reveal users' actions or intentions, and some practices cannot be observed without collecting sensitive information. A structured approach is therefore needed to distinguish directly measurable conditions from indicators requiring behavioural inference. This study develops a framework for evaluating and prioritising cybersecurity hygiene indicators according to their security relevance, observability, assessment complexity, inference reliability, data requirements, privacy sensitivity and explainability.

Research aim

This study aims to identify and prioritise cybersecurity-hygiene indicators suitable for automated endpoint assessment, balancing security relevance, technical feasibility and privacy.

Which cybersecurity hygiene indicators are suitable candidates for automated endpoint assessment, given their observability and privacy implications?

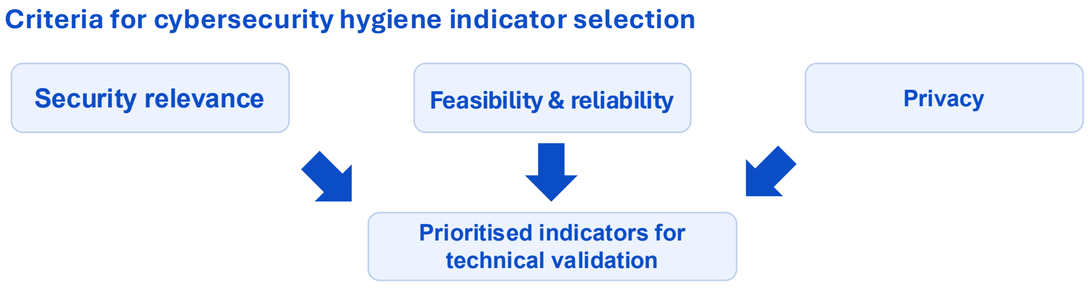

Fig. 1. Key considerations for prioritising cybersecurity hygiene indicators for endpoint assessment.

Methodology

Indicators were compiled from SeBIS and the Cyber Hygiene Inventory development pool, informed by SeBIS behavioural validation [1–3], and supplemented by brainstorming sessions. They were classified by type, observable evidence and assessment requirements. Twelve complete questionnaire responses informed preliminary importance weights using an adapted Analytic Hierarchy Process (AHP) [4]. Individual priorities were calculated and averaged separately for behavioural and environment indicators [5]. Consistency and sensitivity analyses assessed the stability of the resulting rankings.

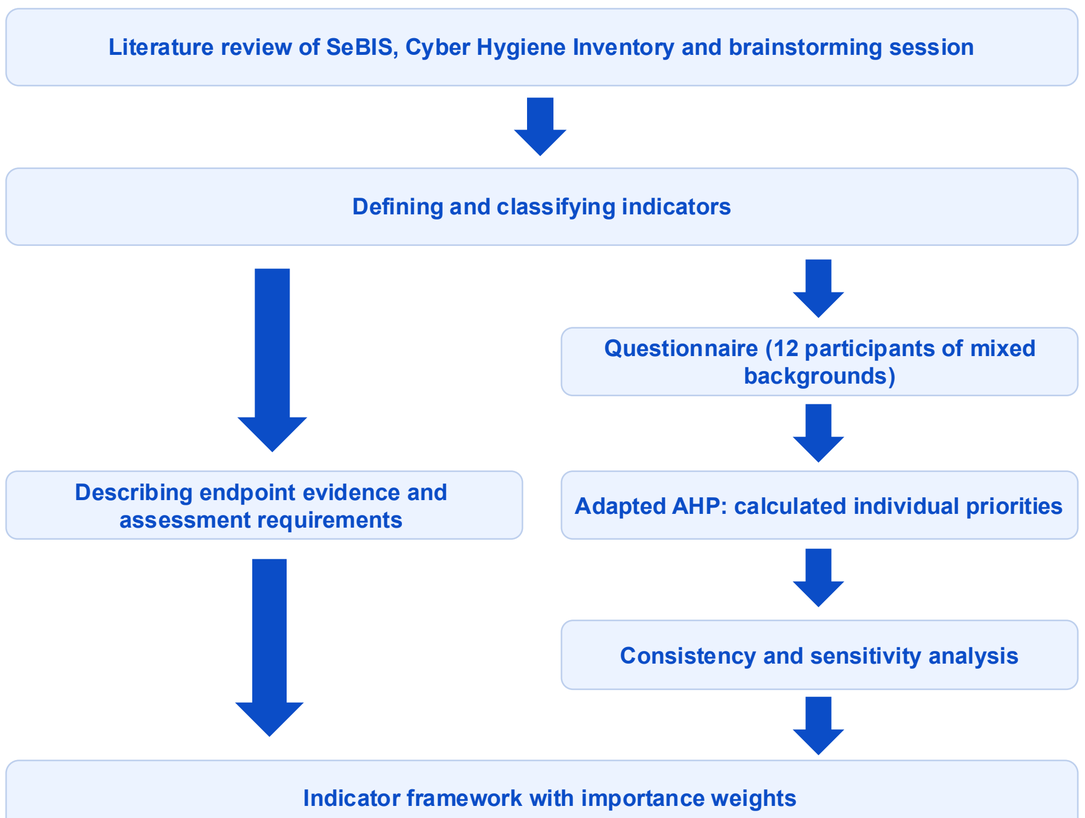

Fig. 2. Methodology for developing and prioritising cybersecurity hygiene indicators.

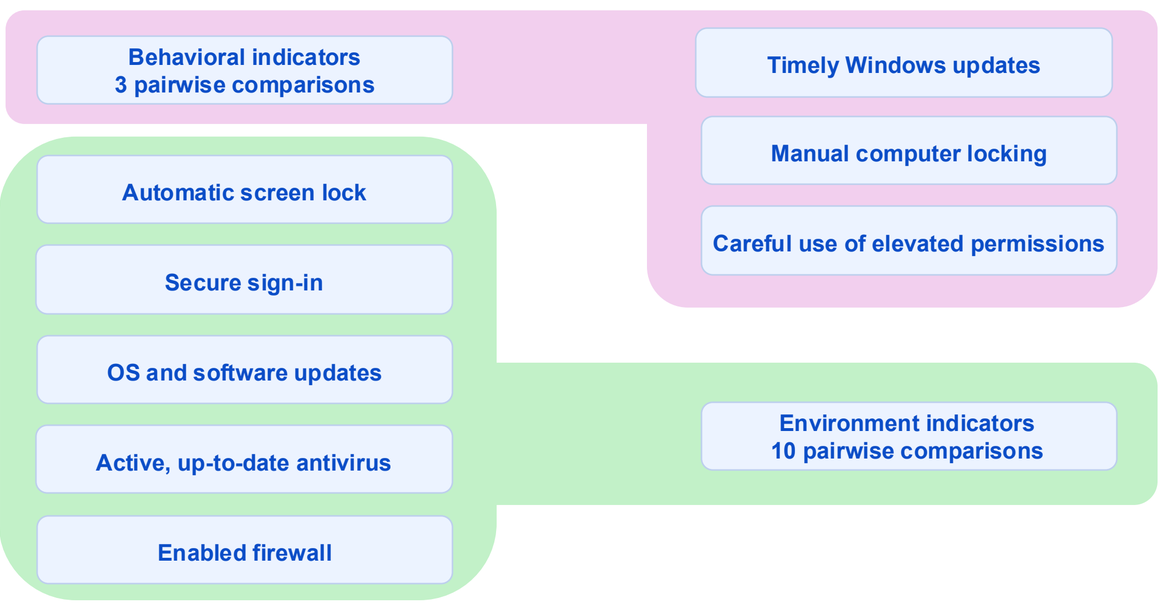

Fig. 3. AHP hierarchies for estimating importance within behavioral and environment indicator groups.

Results

Eight indicators were selected for further technical assessment. Their endpoint evidence, inference limitations and qualitative privacy classifications are summarised below.

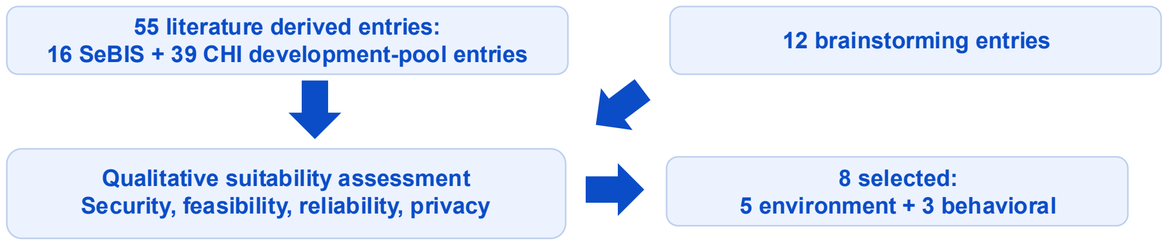

Fig. 4. Selection of cybersecurity hygiene indicators for endpoint assessment. Candidate lists contain overlapping practices.

Indicator	Endpoint evidence	Assessment limitation	Privacy
Automatic screen lock (E)	Lock and timeout settings	Does not establish user absence	Low
Secure sign-in (E)	Sign-in / unlock settings	Password strength remains unknown	Low
OS/software updates (E)	Update status, versions	Coverage varies by application	Low-medium
Antivirus protection (E)	Protection / definition status	Evidence varies by product	Low
Firewall protection (E)	Enabled state, profiles	Rule quality unassessed	Low
Manual locking (B)	Inactivity, lock events	Inactivity does not prove absence	Medium
Administrator use (B)	Elevated process execution	Purpose and necessity remain unknown	Medium
Timely Windows updates (B)	Repeated pending update/restart states	Delay does not prove deliberate postponement	Low

Table 1. Endpoint evidence and assessment limitations for environment (E) and behavioural (B) indicators. Privacy ratings follow the indicator catalogue's qualitative scale.

Indicator priorities within each group

Across 12 complete questionnaire responses, manual locking received the highest weight among behavioural indicators (46.5%), and an enabled firewall received the highest weight among environment indicators (27.6%).

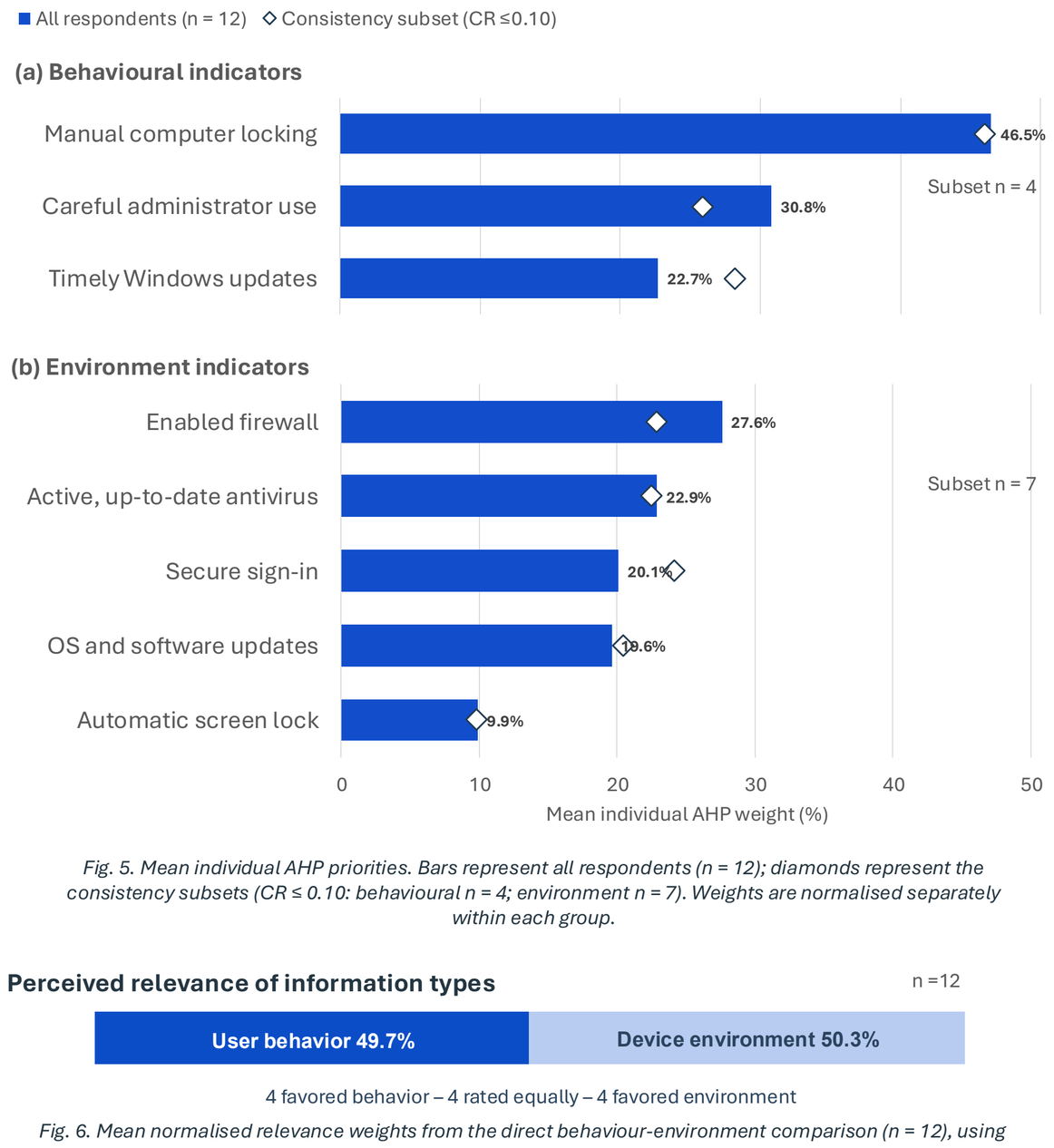

Fig. 5. Mean individual AHP priorities. Bars represent all respondents (n = 12); diamonds represent the consistency subsets (CR ≤ 0.10: behavioural n = 4; environment n = 7). Weights are normalised separately within each group.

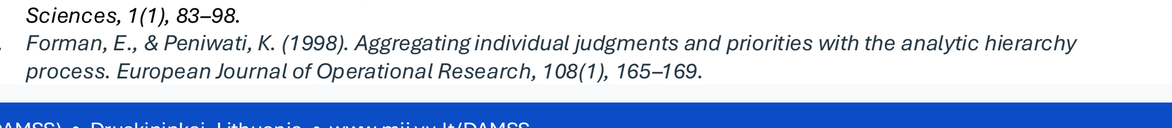

Fig. 6. Mean normalised relevance weights from the direct behaviour-environment comparison (n = 12), using the adapted scale conversion.

Interpretation of results

Across the eight selected indicators, perceived importance and ease of assessment did not always coincide. Manual locking ranked first among behaviours, yet lock events and inactivity cannot confirm that a user left the device unattended. Firewall status can be checked directly with low privacy impact. It ranked first among environment indicators in the full sample, while secure sign-in ranked first in the consistency subset. The 12 respondents gave behavioural and environment information nearly equal relevance overall. These preliminary findings support considering both groups for technical validation, weighing perceived importance alongside observability and privacy.

References

1. *Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). CHI '15, 2873–2882.*
2. *Egelman, S., Harbach, M., & Peer, E. (2016). Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). CHI '16, 5257–5261.*
3. *Vishwanath, A., et al. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 113160.*
4. *Saaty, T. L. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1), 83–98.*
5. *Forman, E., & Peniwati, K. (1998). Aggregating individual judgments and priorities with the analytic hierarchy process. European Journal of Operational Research, 108(1), 165–169.*