A Framework for Developing Information Security Awareness Measures

Mattia Mossano
Karlsruhe Institute of Technology

Anne Hennig
Karlsruhe Institute of Technology

Fabian Lukas Ballreich
Karlsruhe Institute of Technology

Benjamin Maximillian Berens
Karlsruhe Institute of Technology

Filipo Sharevski
DePaul University

Angela Martina Sasse
Ruhr University Bochum

Melanie Volkamer
Karlsruhe Institute of Technology

Abstract

We present a work-in-progress on a framework for developing effective security awareness measures. The framework provides a systematic process to support practitioners, defining the relevant aspects to design an awareness measure for their target audience, and how to determine the security assumptions. Our work merges existing proposals from several disciplines with our practical expertise in developing and evaluating different types of security awareness measures.

1 Introduction

The existing awareness measures landscape offers multiple, sometimes conflicting recommendations (shown in, e.g., [11, 15]). Users are forced to navigate this fragmented landscape on their own, leading to both *security fatigue* (defined in Stanton et al. [16]), and disinterest towards security (shown in Haney & Lutters [4]). Thus, the awareness landscape would greatly benefit from standardization. There are already guidelines and frameworks on how to develop awareness measures, e.g., [2, 5, 11, 13, 18], but they lack key aspects such as how and when the target population influences the measure, e.g., accessibility needs, cognitive load, or time investment.

Here, we present a work-in-progress on a framework for developing security awareness measures. Our proposal addresses the standardization issue by merging frameworks from different disciplines [1–3, 7–10] with the authors' expertise in developing and evaluating security awareness measures. Further, our work complements and extends existing standards, such as the Cyber Kill Chain [6], the Unified Kill Chain [14], and the NIST Cybersecurity Framework 2.0 [12]. Namely, the framework not only helps practitioners developing effective awareness measures, but also selecting the security assumptions. Clear security assumptions are important because they give an overview of the rationale behind the measure content, clearly showing what is covered, what is missing, and why that is the case. The last point means that the justifications for why certain assumptions are taken should be transparent.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

2 Framework Description

In the following, we present a step-by-step description of our framework for developing information security awareness measures. The framework can be seen in Appendix A.

Step 1 – Preparation. A developer identifies the domain of interest, the target population, the context of use, and the awareness goal. For example, an awareness measure to support the general public (target population) by providing recommendations to detect (awareness goal) phishing through QR codes (domain) in everyday life (context).

Step 2 – Attack techniques in general. A developer collects all the attack techniques within the selected domain, and makes an initial selection by considering the time available to the target population, and the context. This then informs the security assumptions. For example, the developer conducts a literature review of all attack techniques through QR codes, and excludes those that 1) would be too complex to explain to the general public in a limited time, and 2) do not apply to the mobile context. The exclusions are added to the assumptions.

Step 3 – Mitigation measures in general. A developer collects all the mitigation measures in the selected domain, and identifies which attacks lack mitigation, adding them to the security assumptions. In parallel, the mitigation measures are compared against the time available to the population and

its constraints to identify which ones are actionable by the target population. For example, all mitigation measures against attack techniques through QR codes are collected. Those attacks without mitigation are added to the assumptions. The developer also identifies those mitigation measures that 1) do not require significant time investment, and 2) are applicable without a strong technical background.

Step 4 – Attack techniques mitigation and misconceptions to be covered. The developer determines the list of attack techniques to consider by comparing the attacks that have a mitigation, with the mitigation measures actionable by the target population, and the awareness of the target population. The developer adds the excluded attacks to the security assumptions. In parallel, the developer investigates the target population's misconceptions on both attack techniques and mitigation measures. For example, the developer decides to only consider attacks through QR codes that have mitigation measures relatively quick to apply and not requiring a technical background, excluding attacks not fitting these criteria. Yet, the developer sets the awareness level as none, due to the variability in the general population, excluding no attack based on it. The developer then conducts a literature review of misconceptions about phishing, selecting only those related to the selected attacks and mitigation measures.

Step 5 – Content creation based on target population. The developer creates the content for the awareness measure at this step. The outcome of all previous steps come together to form a cohesive structure: attack techniques with actionable mitigation measures, the mitigation measures, and the misconceptions on attacks and mitigation. The maximum time available also influences the content, which should be adequate for the time available. Then, the developer needs to identify the most effective way to incentivize the target population to invest their time and effort in learning the content. The content also needs to take into consideration the context of use, and be adapted to achieve the awareness goal. Once the content is ready, the developer updates the security assumptions one last time, as some attacks or mitigation could still get excluded. For example, building on the QR code example, an incentive for the general population highlighting how QR codes attacks may target their finances directly. The context of the QR code scanner use influences which attacks, misconceptions, and actionable mitigation measures are considered.

Step 6 – Design of the measure. Here, the developer adapts the content to the selected format of the measure. The format, as well as the content, must be adapted to the characteristics of the target population and the accessibility requirements. Once this is done, the first version of the measure is created. It is important that every example used (e.g., links) is vetted, as users of the measures might try to visit a link. Hence, no real phishing or malicious examples should be used. For example, the developer decides to adapt the content for a short webpage text, taking care of respecting the W3C [17] guidelines for accessible websites. The developer also makes sure to use no real malicious QR codes, as well as no real phishing URL. Further, they check that the examples used are either under their control or not dangerous.

Step 7 – Evaluation. First, the developer run an informal feedback session with members of the target population and experts. Yet, this is not sufficient to determine the effectiveness of the awareness measure. A formal, empirical evaluation must be designed and carried out, ideally with a representative sample. If the performance is deemed satisfactory, then the process is complete. Otherwise, the developer needs to identify the issues, backtrack, and either modify the content itself, or the way it is presented. For example, at first the developer asks feedback from a focus group of lay users, and from experts of phishing. After implementing their feedback, the developer sets-up a user study with a statistically representative sample to determine if the measure significantly influence the participants' ability to detect phishing QR codes. If the study shows a significantly better detection rate for those participants using the awareness measure, then the process is concluded. Otherwise, the developer will have to correct it and retry the evaluation with a different sample. This process continues until a significant better detection is achieved.

3 Future Work and Conclusion

There is need for a framework for developing security measures that achieve consistent results and support the users navigate the awareness landscape. We propose a framework that merges existing work, while integrating and expanding upon it. Yet , several steps are still open.

Our next step is to develop awareness measures with our framework for different contexts and populations (e.g., employees in a business, or the general public), and then evaluate in user studies the measures' effectiveness, understandability, and users' satisfaction. The effectiveness of the developed and evaluated measures is then used as a key indicator for the effectiveness of the framework itself. Another considerable open challenge is how to achieve acceptance of the framework as a possible standard by the wider security community. To this end, showing that the framework is viable complement to existing standards might be a way worth pursuing.

Acknowledgments

This work was supported by funding from the project "Engineering Secure Systems" of the Helmholtz Association (HGF) [topic 46.23.01] and by KASTEL Security Research Lab.

References

[1] Dialog für Cyber-Sicherheit. Leitfaden des Workstreams „Effektive IT-Security-Awareness: Wirksam ein Bewusstsein für Risiken schaffen". Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2022.

[2] European Union Agency for Cybersecurity. Guideline on Security Measures under the EECC- 4th edition. Technical report, ENISA, 2024.

[3] Arash Ghazvini and Zarina Shukur. A Framework for an Effective Information Security Awareness Program in Healthcare. *International Journal of Advanced Computer Science and Applications*, 8(2):193–205, 2017.

[4] Julie M. Haney and Wayne G. Lutters. "It's Scary... It's Confusing... It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Symposium on Usable Privacy and Security*, SOUPS 2018, pages 411–425, Baltimore, MD, US, 2018. USENIX Association.

[5] Siqi Hu, Carol Hsu, and Zhongyun Zhou. Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, 62(4):752–764, 2022.

[6] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, 2011.

[7] Lennart Jaeger. Information Security Awareness: Literature Review and Integrative Framework. In *Hawaii International Conference on System Sciences*, HICSS 51, pages 4703–4712, Hawaii, US, 2018. AIS.

[8] Mohammed Khader, Marcel Karam, and Hanna Fares. Cybersecurity Awareness Framework for Academia. *Information*, 12(10):417, 2021.

[9] Khando Khando, Shang Gao, Sirajul M. Islam, and Ali Salman. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106:102267, 2021.

[10] Peter Mayer. *Secure and Usable User Authentication*. PhD thesis, Karlsruhe Institute of Technology, 2019.

[11] Mattia Mossano, Kami Vaniea, Lukas Aldag, Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In *European Symposium on Usable Security*, EuroUSEC 2020, pages 130–139, Online, 2020. IEEE.

[12] National Institute of Standards and Technology. The nist cybersecurity framework (csf) 2.0. Technical Report NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, February 2024.

[13] Jethro Oates. *A Qualitative Grounded Theory Study of Employee Interventions to Improve Information Security in Small Businesses*. PhD thesis, Capella University, 2019.

[14] Paul Pols. The unified kill chain – raising resilience against advanced cyber attacks through threat modeling, 2023.

[15] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *Conference on Computer and Communications Security*, CCS 2016, page 666–677, Vienna, AT, 2016. ACM.

[16] Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. Security Fatigue. *IT Professional*, 18(5):26–32, 2016.

[17] World Wide Web Consortium. W3C standards and drafts, 2025.

[18] Leah Zhang-Kennedy and Sonia Chiasson. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, 54(1):1–39, 2021.

A Framework representation

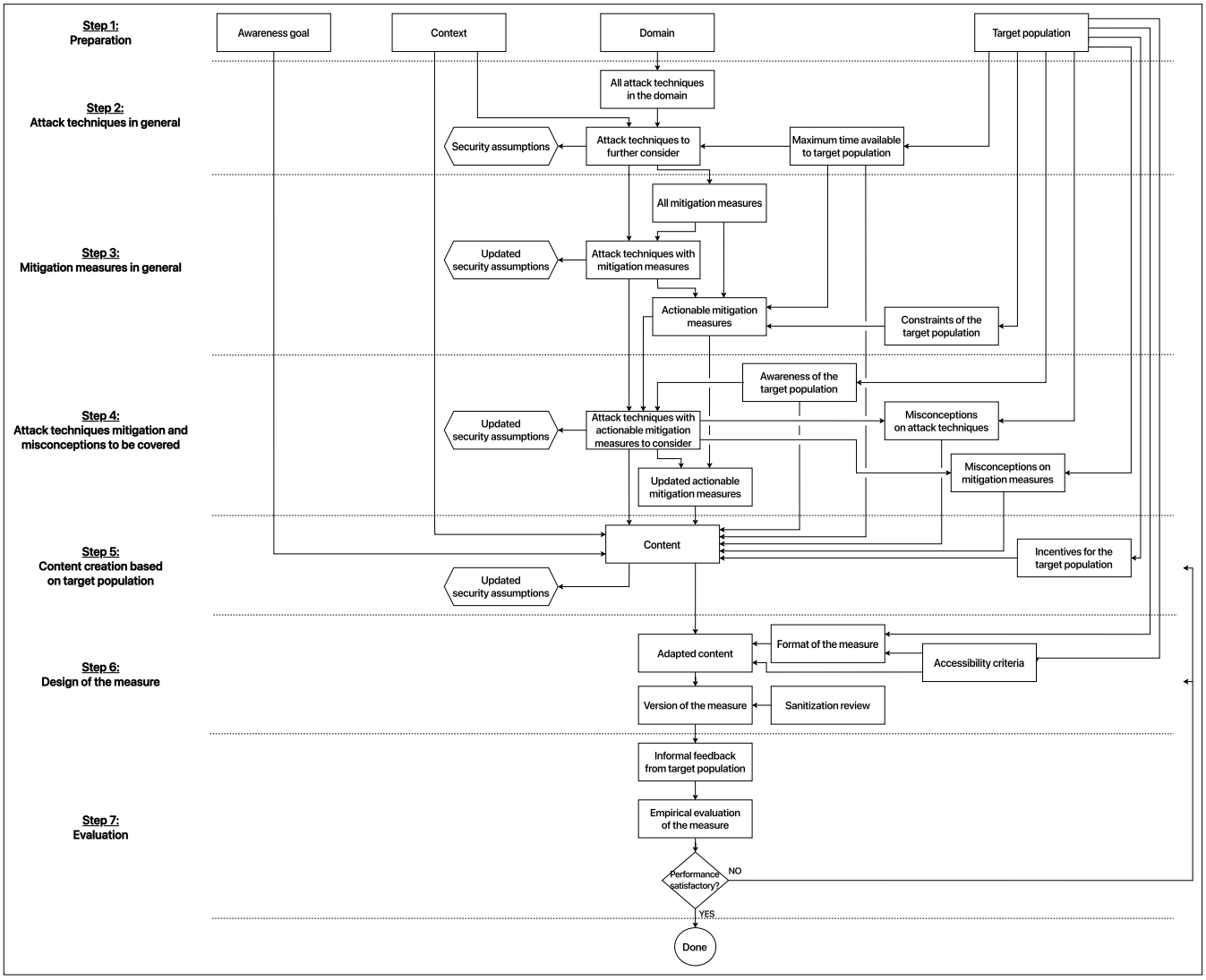

Figure 1: Our framework for developing information security awareness measures.