Making Security Matter: Engaging Non-Security Users Effectively through Empathy

Anne Elisabeth Krueger[1]

Abstract: This position paper highlights the importance of empathetic communication in information security systems, so that cyberattacks can be effectively defended against at the vulnerable points of the security organization, the non-security users. By systematically integrating empathy, trust between non-security users and security users can be enhanced, resulting in increased mutual engagement and commitment, which in turn encourages safer behaviors from non-security users. To this end, initial principles are introduced to guide the systematic integration of empathy into the interactions between security and non-security users. With the overarching goal that organizations can potentially become more resilient and less vulnerable to cyber threats over time, this position paper aims to spark discussions and provide insights for designers of information security systems.

Keywords: Information Security System, Trust, Empathy, Experience Design

1 Introduction

The significant number of security incidents in organizations worldwide underscores the necessity for non-security users within an organization to engage with the topic of information security. Non-security users in departments such as finance, HR, and marketing are often the first line of defense against cyber threats [KCF21]. Many security breaches occur due to human error, such as clicking on phishing links, using weak passwords, or mishandling sensitive data. Therefore, it is essential to equip these employees with the knowledge to recognize and prevent such risks. However, Information Security is often perceived by non-security users as an additional task that interferes with their core productive activities, as potential attacks are viewed as distant and outside their immediate responsibilities.

A promising approach to address these issues seems to promote a trustful relationship-building between non-security users and security users [KCF21]. Establishing trust is essential, as it ensures both parties that they act in each other's best interest. This mutual trust then forms the foundation for upholding agreements and, for instance, non-security users adhering to security policies [KCF21]. In addition to factors such as transparent communication and consistent behavior, empathy seems crucial to building trust [Ra16; WJW22] (see Figure 1). Defined as *the ability to imagine others' emotional experiences while maintaining a clear distinction from one's own [CG11], empathy fosters understanding and creates the foundation for recognizing others' needs and perspectives*. Furthermore, the perceived empathy of the respective other simultaneously makes one feel understood and

[1] Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering IAO, Nobelstr. 12, 70569 Stuttgart, Germany, anne-elisabeth.krueger@iao.fraunhofer.de, https://orcid.org/0000-0002-3472-1186

doi:10.18420/OID2025_12

acknowledged, fostering a deeper, more respectful connection and, in turn, strengthening trust [PK12; WJW22].

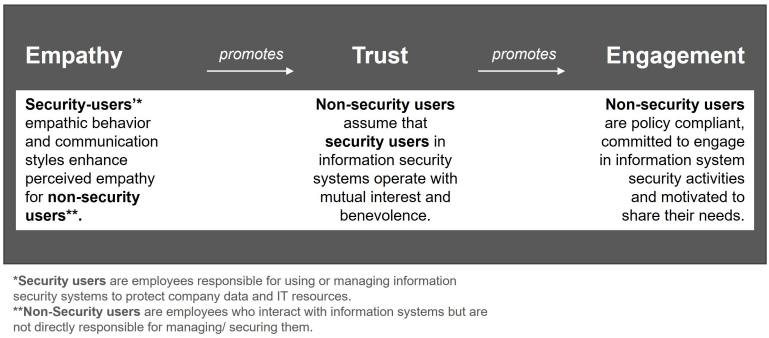

Fig. 1: Empathy builds trust, leading to stronger engagement.

Thus, if security users were supported and actively sought to empathize with the perspective and emotional experience of non-security users, and this was recognized as such, an atmosphere of trust could be established. This, in turn, could lead to safer organizations, as non-security users feel obligated to remain vigilant against potential attacks due to their close relationship with the security department.

Based on these considerations, this paper pursues the following objectives:

- To highlight that empathetic communication in information security fosters trust and promotes safer behavior,'making security matter.'
- To outline key principles for designing security systems that incorporate empathy, strengthening mutual commitment, and long-term cyber resilience.

2 Food for Thought: Design Principles for Information Security Systems to Foster Empathy

Three fundamental principles to systematically introduce empathy are proposed to initiate discussion and provide food for thought for designers and other relevant stakeholders of information security systems. The aim is to support empathy and mutual understanding of their emotional experiences between non-security and security users, fostering a close relationship that encourages commitment and, in the long term, enhances organizational security. Thereby, it has to be noted, that the presented principles do not claim to be exhaustive.

2.1 Principle 1: Establish an Atmosphere of Emotional Safety

Creating an emotionally safe environment [Ed20; Ed99] is key to fostering empathy between security and non-security users. Both stakeholder-groups must feel comfortable expressing their opinions, concerns and emotional experiences without fear of judgment or retaliation. For instance, if a non-security user receives a phishing email and is uncertain about its legitimacy, they should feel comfortable asking security users without embarrassment. Likewise, they should be able to express doubts about the necessity of a security measure without hesitation. Only when prejudices are minimized and active listening is practiced such an open communication is possible, where individuals are willing and able to freely share and connect to their true (psychological) needs to build mutual understanding of the others' experience and thus, to develop empathy. In turn, an emotionally safe environment promotes trust and collaboration, ultimately strengthening the security culture and organization.

Concrete approaches, methods and inspiration on how to create emotional security in organizations can be found in the literature [Ed20; Ed99].

2.2 Principle 2: Enable both Imaginative Empathy Processes

For a security user to genuinely understand the impact of established policies on a non-security user, mere observation and external analysis are not sufficient (cf. [Er16]). Instead, they should actively engage and immerse themselves in the non-security user's experience, linking it to their own emotional perspective to develop a deeper understanding. Thus, to systematically integrate empathy into information security systems, both imaginative processes from empathy research should be considered [Da04]: In the *Imagine-Other* process, people are encouraged to consider what someone else might feel or think in a given situation. In contrast, the *Imagine-Self* process involves imagining how they themselves would feel if they were in the other person's place. While the *Imagine-Self* perspective has a stronger emotional impact on the person adopting it, making it easier to empathize with others' emotional experiences [Er16], the *Imagine-Other* perspective provides an essential level of abstraction to maintain the necessary distinction from one's own experiences (cf. [CG11]).

To support the *Imagine-Other* process, there exist methods and tools in experience design, such as Experience Interviews [Ze16], Experience Probes [Kr20] or the Needs Empathy Map [Fe15; Kr22; OP11]. For the *Imagine-Self* process, the Needs Perspectives, a newer form of the method UX Concept Inspiration [KFP15], can be applied.

2.3 Principle 3: Support the Development of Emotional Sensitivity

For security users to systematically build empathy with non-security users, it is crucial that they are attuned to their own emotional experiences (cf. [YDP13]). To understand another's

emotional experience and differentiate it from one's own, it is essential to connect with one's psychological needs and emotions, thereby developing emotional granularity and sensitivity to one's personal lived experience [CG11; Kr17; YDP13]. Thereby, it is assumed that an individual's emotional experience is based on the fulfillment or non-fulfillment of their psychological needs [Ha03; Ha13], such as for Competence, Stimulation or Connection. For example, the experience of privacy, a fundamental component of information security systems, is subject to varying perceptions based on the underlying psychological needs and associated individual cognitive frameworks [KB24]. Here, the psychological need for *Comfort* might require easy access to privacy settings, while the need for *Connectedness* necessitates the sharing confidential information in a secure environment with the aim of building relationships.

In experience design research, various tools have already been created, which can possibly facilitate this development of emotional sensitivity (e.g. [Bu23; DF20a; DF20b; DF21; DF22; Kr17; YPD15]) and thus can be used and adapted for information security systems.

3 Outlook

The overarching goal of the position paper is to *making security matter* to non-security users in organizations. For this purpose, three initial principles for the systematic integration of empathy into information security systems are introduced. This is done under the assumption that it will, in turn, lead to more trust and ultimately result in safer behavior by non-security users - making organizations less vulnerable to cyberattacks.

Additional research is planned to validate these principles, refine them if necessary, and develop tailored methods to support empathic behaviors in information security systems. For this purpose, the above-mentioned methods and materials from experience design research will be used and adapted accordingly for the context of information security systems.

Furthermore, perceived empathetic behavior can create a positive emotional experience for relevant stakeholders (cf. [WJW22]). Fostering positive emotions promotes motivation, creativity and resilience [Fr04]. Consequently, among non-security users perceived empathetic behavior of security users might lead to an increased motivation to engage in protective behaviors, thereby enhancing overall security compliance. In turn, stimulating negative emotional experiences might have the contrary effect. Thus, consideration should be given to how positive experiences can be incorporated into information security systems.

The objective is not merely to adopt a task-based, technocratic perspective on the relevant stakeholders in the information security system but to shift the focus on their felt-life, communication and relationships. This focus seems essential for effective and equitable collaboration of security and non-security users (cf. [KFR18]). Only by comprehending the entire information security system, its interdependencies and emotional levels organizations can create sustainably secure environments. Thereby, it seems important to understand

that, although the human factor can pose risks for potential security breaches, it should be regarded as an integral and essential part of a functioning information security process.

Acknowledgments. The position paper is part of the activities in the "Mittelstand-Digital Zentrum Fokus Mensch" (MDZ-FM). The MDZ-FM is part of the Mittelstand-Digital initiative funded by the German Federal Ministry for Economic Affairs and Climate Action, funding number: 01MF23003E.

References

[Bu23] Burmester, M. et al.: Bedürfnismaterialien, 2023, https://www.digitalzentrum-fokus-mensch.de/wissen/beduerfnismaterialien, Stand: 01/05/2024.

[CG11] Coplan, A.; Goldie, P.: Empathy. Oxford University Press Oxford, 2011.

[Da04] Davis, M. H. et al.: Cognitions associated with attempts to empathize: How do we imagine the perspective of another? Personality and Social Psychology Bulletin 30 (12), pp. 1625–1635, 2004.

[DF20a] Desmet, P.; Fokkinga, S.: Beyond Maslow's Pyramid: Introducing a Typology of Thirteen Fundamental Needs for Human-Centered Design. Multimodal Technologies and Interaction 4 (3), Number: 3 Publisher: Multidisciplinary Digital Publishing Institute, p. 38, 2020.

[DF20b] Desmet, P.; Fokkinga, S.: Thirteen chairs, thirteen fundamental needs. 2020.

[DF21] Desmet, P.; Fokkinga, S.: The House of Happiness. Inspiration Poster, 2021, https://diopd.org/wp-content/uploads/2021/05/House-of-happiness-screen-scaled.jpg, Stand: 10/17/2022.

[DF22] Desmet, P.; Fokkinga, S.: Thirteen fundamental needs, 2022, https://needtypology.com/.

[Ed20] Edmondson, A. C.: Die angstfreie Organisation: wie Sie psychologische Sicherheit am Arbeitsplatz für mehr Entwicklung, Lernen und Innovation schaffen. Vahlen, 2020.

[Ed99] Edmondson, A.: Psychological safety and learning behavior in work teams. Administrative science quarterly 44 (2), pp. 350–383, 1999.

[Er16] Erle, T. M.: A grounded approach to psychological perspective-taking, PhD thesis, Universität Würzburg, 2016.

[Fe15] Ferreira, B. et al.: Designing Personas with Empathy Map. In: SEKE. Vol. 152, 2015.

[Fr04] Fredrickson, B. L.: The broaden–and–build theory of positive emotions. Philosophical transactions of the royal society of London. Series B: Biological Sciences 359 (1449), pp. 1367–1377, 2004.

[Ha03] Hassenzahl, M.: The thing and I: understanding the relationship between user and product. In: Funology. Springer, pp. 31–42, 2003.

[Ha13] Hassenzahl, M. et al.: Designing moments of meaning and pleasure. Experience design and happiness. International journal of design 7 (3), 2013.

[KB24] Krueger, A. E.; Brandenburg, S.: Learnings from a Guided Method for Experience Design: Psychological Needs in the Context of the Privacy Value. In: Open Identity Summit 2024. Gesellschaft für Informatik eV, pp. 115–126, 2024.

[KCF21] Kurowski, S.; Cetin, F.; Fischer, R.: Why should they care? Conceptualizing the challenges of information security training. In: Open Identity Summit 2021. Gesellschaft für Informatik eV, pp. 199–204, 2021.

[KFP15] Krüger, A. E.; Fronemann, N.; Peissner, M.: Das kreative Potential der Ingenieure–menschzentrierte Ingenieurskunst. In: Stuttgarter Symposium für Produktentwicklung, SSP 2015 Entwicklung smarter Produkte für die Zukunft. Pp. 1–10, 2015.

[KFR18] Kurowski, S.; Fähnrich, N.; Roßnagel, H.: On the possible impact of security technology design on policy adherent user behavior-Results from a controlled empirical experiment. In: SICHERHEIT 2018. Gesellschaft für Informatik eV, pp. 145–158, 2018.

[Kr17] Krueger, A. E. et al.: Needs profile: sensitising approach for user experience research. In: Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17. ACM Press, Brisbane, Queensland, Australia, pp. 41–48, 2017, http://dl.acm.org/citation.cfm?doid=3152771.3152776, Stand: 11/30/2019.

[Kr20] Krueger, A. E. et al.: Guided user research methods for experience design—a new approach to focus groups and cultural probes. Multimodal technologies and interaction 4 (3), p. 43, 2020.

[Kr22] Krueger, A. E.: Two methods for Experience Design based on the Needs Empathy Map: Persona with Needs and Needs Persona. In (Marky, K.; Grünefeld, U.; Kosch, T., eds.): Mensch und Computer 2022 - Workshopband. Gesellschaft für Informatik e.V., Bonn, 2022.

[OP11] Osterwalder, A.; Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer. Campus Verlag, 2011.

[PK12] Pavlovich, K.; Krahnke, K.: Empathy, connectedness and organisation. Journal of business ethics 105, pp. 131–137, 2012.

[Ra16] Rahman, W.: Empathy and trust: Into a better workplace environment. Journal of Business and Economics 7 (12), pp. 2025–2034, 2016.

[WJW22] Wu, Q.; Jin, Z.; Wang, P.: The relationship between the physician-patient relationship, physician empathy, and patient trust. Journal of general internal medicine 37 (6), pp. 1388–1393, 2022.

[YDP13] Yoon, J.; Desmet, P. M.; Pohlmeyer, A. E.: Embodied typology of positive emotions: The development of a tool to facilitate emotional granularity in design. In: IASDR 2013; 5th international congress of international association of societies of design research, Tokyo, Japan. Pp. 1195–1206, 2013.

[YPD15] Yoon, J.; Pohlmeyer, A.; Desmet, P.: Positive emotional granularity cards. 2015.

[Ze16] Zeiner, K. M. et al.: Das Erlebnisinterview–Methode zum Verständnis positiver Erlebnisse: Praktische Einführung und Diskussion von Implikationen zur UX-Gestaltungspraxis. In: UP 2016. Gesellschaft für Informatik eV und die German UPA eV, pp. 10–18420, 2016.