Why should they care? Conceptualizing the challenges of information security training

Sebastian Kurowski [1], Fatma Cetin[2], Rudolf Fischer[3]

Abstract: Most organizations rely on individuals without or with little security knowledge to participate in information security tasks. Intending to enable them, information security trainings are usually used. But their effectiveness is debatable. In this contribution we combine descriptive analysis with the social systems theory and current literature on organizational learning and change management to conceptualize the challenges of information security training. We find that the challenges of security training are rooted within a basic dilemma of security: its value-promise (addressing of risks) is not suitable for communication within an organization. These findings are part of an ongoing research project on trainings for IoT security.

Keywords: Security training, awareness, policy compliance, system theory, change management, organizational learning

1 Introduction

There are many tasks such as identity management, credential management, policy compliance, key management, incident management and several more, where participation of non-security users in the organization is a key to success. If credentials are not handled accordingly by their owner, they become a vulnerability. In order to enable them, information security trainings are usually used. But their effectiveness is debatable. For instance, Bulgurcu [Bu09] showed that the effectiveness of security trainings is moderated by the perceived fairness of the security measures. In our systematic approach, we are using the (social) system theory [Lu84] along with its application to risk [Lu90] and organizations [Lu11] to conceptualize the challenges of information security training (see Section 3) and match these with techniques from literature on change management. These findings are used in an ongoing research project on security training development for IoT security.

[1] Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering, Team Identity Management, Nobelstr. 12, Stuttgart, 70569, sebastian.kurowski@iao.fraunhofer.de

[2] University of Stuttgart, Institute of Human Factors and Technology Management IAT, Nobelstr. 12, Stuttgart, 70569, fatma.cetin@iat.uni-stuttgart.de

[3] University of Stuttgart, Institute of Human Factors and Technology Management IAT, Nobelstr. 12, Stuttgart, 70569, rudolf.fischer@iat.uni-stuttgart.de
https://orcid.org/0000-0003-0783-131X

2 Analyzing social systems in information security

The system theory by Luhmann [Lu84] is a descriptive, communication focused theory on social systems. Its focus on communication hereby allows it to provide a consistent description of a research subject [St20]. In order to describe a social system, system theory uses a subsystem hierarchy [Lu84], meaning that any system can be comprised of subsystems. Patterns and structures that contribute to the description of a social system are constituted by communication between its subsystems. Subsystems however can only communicate, if both subsystems can make the same sense out of what has been communicated. This required sense-making can be achieved by a set of e.g. shared basic elements (in the following referred to as commonalities). If, for instance, two employees, or two business units do not share some common ground for making sense out of a collaboration, it will most likely not be continued, or not be initiated. Collaboration must be hereby regarded with the aspect of time in mind. Structures and patterns in social systems can be produced and vanish again, and thus every association between systems must be continuously reproduced in order to pertain.

If we consider an organization as a system-of-systems whereas the subsystems-of-interest for us are provided by the organizations business units, then the social system of information security in organizations could be reduced down to a primary value generating business unit (user BU) and the information security focused business unit (information security BU). For collaboration between these units to take place, an association must be founded on a common ground for sense making through commonalities [Lu84]. However, there is little common ground between these business units within their goals, foundations for action, and desired outcomes. The user BU for instance acts upon working tasks, with value generating goals in mind, towards the outcomes of its value generating processes. The information security BU on the other hand acts upon the current state of the security architecture, with information security specific goals (mostly risks) in mind, and towards a future state of the organizations security architecture.

This leaves little ground for commonalities to occur naturally within the organization, which yields the question which sense these units should make out of collaborating? However, when looking at organizations one may argue that collaboration between a user BU and an information security BU sometimes take place. A commonality for such a collaboration could lie in the acceptance of information security collaboration as a necessary task to ensure the future of the organization. However, an experiment conducted in 2017 found that individuals may stop participating in information security tasks after enough working stress had been invoked on the participants [Ku18]. This shows that the willingness to participate in information security tasks may as well vanish over time, e.g. when participants start to consider information security as work impeding, and thus a value impeding activity.

A common approach to establish a common ground for sense making is usually found in risk awareness campaigns. These try to raise awareness on the risks that information security is addressing and thus provide the ground for making sense out of information security actions. Risk however is not a naturally occurring phenomenon, but an individual anticipation due to an observed threat [Lu90]. It is thus entangled with its observer [Ba91], and therefore influenced by individual traits such as the affinity or aversion towards certain risks [KT79][Me17], the tendency to weigh known risks heavier than unknown ones [GS89][Me17], and the tendency to underestimate risks that apply to contexts further away from one's personal context [He03][Be09][No83]. With this in mind, findings that individuals with no information security background seem to perceive certain security risks differently than those with security background as found by Albrechtsen and Hovden in 2009 [AH09] seem hardly surprising. This also challenges the communication of risks, as these can hardly be justified without losing credibility either through communicated materialization scenarios that are not believed by the user BU or which seem exaggerated, or which may even be perceived as threats by the user BU [Sk98]. This concludes a basic dilemma of organizational information security. It can hardly objectively justify its actions with its risk posture.

Sometimes legal compliance is referred to as a possible solution out of this dilemma. But this only works of legal compliance is considered for the sake of it[4]. As soon as legal compliance is considered as evasion of sanctions, it becomes a matter of individual risk perception and again leads to described dilemma. This leaves us with the only common ground for associations of the information security BU with the user BU: The trust that this association is in the interest of the user BU. This however also involves that the view on the user BU by the information security BU changes radically from servant to customer.

3 Addressing social challenges of information security training

The change management literature offers a wide range of tangible methods which provide possibilities to bring about changes in personal behavior coming from an organizational logic [Cg19][La21][VW20]. In the everyday professional life of social systems, social-emotional indicators control motivation, action, and "downstream behavioral processes" [Ur08]. Emotional experience and trust affect individual action processes as well as subjective attitudes and perspectives of individuals. Therefore, they play an essential role for the willingness to perform according to the organisational goals [LK02]. Performance for this context can be understood as the BU user's performance of safety-related tasks. Despite the existing formal organizational structures, which according to Luhmann create a basis for trust, the challenge on how to maintain trust in interpersonal communication and interaction remains. In today's debate, managing

[4] In this case legal compliance bears its own meaning, which would distinguish between either being compliant or not being compliant. Communication that bears its own meaning does not require further commonalities and is in the system theory refered to as a succes media [Lu84]

organizational change represents a major challenge for any organization [WQ99]. The successful implementation of change comprises the Organizational (changing structures and processes), Personnel (changing behavior) and Cultural (change in values in norms) level. Amongst these, cultural change plays an essential role, as it triggers the change of values and norms, and thus fosters attitudes and behavioral changes of organizational members [He16].

Simply put, an organization learns by the totality of the organization's members learning. Individuals thus no longer comprehend problems strictly from their own point of view but relate them to the expected actions and perceptions of the organization and thus reorder their own activities in accordance with the organizational specifications [AS06]. Thus, theoretically, a commonality is established between the information security BU and the user BU. However, this contingency develops exclusively through the reproduction of basic elements that create meaning and make it possible to act according to organizational specifications. Nevertheless, it should be noted that an idealistic concept such as this requires a high degree of (intrinsic) motivation to learn on the part of employees and commitment on the part of managers who apply and support this type of learning. The principle of the learning organization includes the participation of all stakeholders through clear definitions of roles and tasks and the training of appropriate competencies. This requires a culture that reminds organizational members daily and promotes learning, especially in everyday organizational life. The following is a brief description of some of the success factors that show the most promise in implementing cultural change in an organization [La21]: **Communication tools** play a key role in terms of a credible and honest internal information policy. Communication should begin before the start of a change process and continue beyond its end. In addition, it must be extremely clear, as it is fundamentally open to interpretation and therefore susceptible to misunderstanding. Openness, empathy and constructiveness are further crucial components of communication and the central signals when resistance to change from within one's own organization must be responded to. **Participation tools** create an acceptance of those affected in the change process - provided that the offer developed for this purpose is credible, transparent integrates feedback and is meant seriously. The people affected can identify more easily with the change, which further creates positive impacts on the other individuals, since increasing participation is accompanied by an increase in motivation. For the implementation of an organizational change, additional skills, competencies and knowledge are needed to cope with the resulting new tasks. A need for **Advanced Training** naturally arises in the field of management. Managers play an essential role as promoters or multipliers, as they recognize the causes of resistance, moderate conflict discussions, increase employee motivation, conduct targeted employee discussions and establish a culture of error.

4 Conclusion

This paper captures the puzzle of needed, but often missing, collaboration among non-security users on critical information security issues. We conceptualized the problem using Luhmann's systems theory and were thus able to break it down to the fact that lack of collaboration between organizational units is based on an absence of meaningful elements which itself is followed by a failing credible communication and ultimately leads to (unintentional) non-compliant behavior. This is rooted within a dilemma of organizational information security: that any risk-based communication is susceptible to failure. In our view it thus makes sense to look at a broader, conceptual view on the organisation. We presented such a view with an insight into possible solution trajectories from change management and organizational learning literature. These include a focus on different communication and participation tools, and trainings. We believe that credible communication can only come from a credible organization that considers itself as a sum of its individuals, focusing on communication as a core piece for fostering participation. We aspire to deliver trainings that provide this in our future research.

Bibliography

[AH09] Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers & Security. 28, 6, 476–490 (2009).

[AS06] Argyris, C., Schön, D.A.: Die Lernende Organisation. Grundlagen, Methode, Praxis. Klett-Cotta (2006).

[Ba91] Baskerville, R.: Risk analysis as a source of professional knowledge. Computers & Security. 10, 8, 749–764 (1991).

[Be09] Benjamin, A.S. et al.: Signal detection with criterion noise: applications to recognition memory. Psychological review. 116, 1, 84 (2009).

[Bu09] Bulgurcu, B. et al.: Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors. Presented at the (2009). https://doi.org/10.1109/CSE.2009.484.

[Cg19] Cameron, E., Green, M.: Making Sense of Change Management: A Complete Guide to the Models, Tools and Techniques of Organizational Change. Kogan Page Publishers (2019).

[GS89] Gilboa, I., Schmeidler, D.: Maxmin expected utility with non-unique prior. Journal of Mathematical Economics. 18, 2, 141–153 (1989). https://doi.org/10.1016/0304-4068(89)90018-9.

[He03] Hermand, D. et al.: Risk target: An interactive context factor in risk perception. Risk Analysis. 23, 4, 821–828 (2003).

[KT79] Kahneman, D., Tversky, A.: Prospect Theory: An Analysis of Decision under Risk. Econometrica. 47, 2, 263 (1979). https://doi.org/10.2307/1914185.

[Ku18] Kurowski, S. et al.: On the possible impact of security technology design on policy adherent user behavior-Results from a controlled empirical experiment. SICHERHEIT 2018. (2018).

[La21] Lauer, T.: Change management: Fundamentals and success factors. Springer, Berlin and [Heidelberg] (2021).

[Le20] Lee, D.: The society of society: The grand finale of Niklas Luhmann. Sociological Theory. 18, 2, 320–330 (2000).

[LK02] Lord, R.G., Kanfer, R.: Emotions and organizational behavior. (2002).

[Lu11] Luhmann, N.: Organisation und Entscheidung. VS Verlag, Wiesbaden (2011).

[Lu84] Luhmann, N.: Soziale systeme. Suhrkamp Frankfurt am Main (1984).

[Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. Organization & Environment. 4, 3, 223–231 (1990).

[Lu15] Luhmann, N.: Theorie der Gesellschaft. [...] Teilbd. 2: Die Gesellschaft der Gesellschaft [...]. Suhrkamp, Frankfurt am Main (2015).

[Me17] Mersinas, K.: Risk Perception and Attitude in Information Security Decision-making. Royal Holloway, University of London (2017).

[No83] Nosofsky, R.M.: Information integration and the identification of stimulus noise and criterial noise in absolute judgment. Journal of Experimental Psychology: Human Perception and Performance. 9, 2, 299 (1983).

[Sk98] Skowronski, J.J. et al.: Spontaneous trait transference: Communicators take on the qualities they describe in others. Journal of personality and social psychology. 74, 4, 837 (1998).

[St20] Stichweh, R.: Systems theory as an alternative to action theory? The rise of’communication’as a theoretical option. Acta Sociologica. 43, 1, 5–13 (2000).

[He16] Svea von Hehn et al.: Der Einfluss der Kultur auf den Organisationserfolg. In: Kulturwandel in Organisationen. pp. 1–23 Springer, Berlin, Heidelberg (2016). https://doi.org/10.1007/978-3-662-48171-4_.

[Ur08] Urban, F.Y.: Emotionen und Führung: Theoretische Grundlagen, empirische Befunde und praktische Konsequenzen. Springer-Verlag (2008).

[VW20] Vahs, D., Weiand, A.: Workbook Change Management: Methoden und Techniken. Schäffer-Poeschel (2020).

[WQ99] Weick, K.E., Quinn, R.E.: Organizational change and development. Annual review of psychology. 50, 361–386 (1999). https://doi.org/10.1146/annurev.psych.50.1.361.