Human Factors in Design, Engineering, and Computing, Vol. 159, 2024, 315–324
https://doi.org/10.54941/ahfe1005596

Human-Centric Security Engineering: Towards a Research Agenda

Rick van der Kleij[1,2], Dianne van Hemert[1], Bert Jan te Paske[1], and Thomas Rooijakkers[1]

[1]Netherlands Organisation for Applied Scientific Research TNO, The Netherlands
[2]Avans University of Applied Research, The Netherlands

ABSTRACT

While the importance of designing for user experience has long been acknowledged, there has been relatively little exploration of the actual processes involved in constructing usable and cybersecure systems. In many conventional projects, cybersecurity and usability are not considered primary goals, making them likely candidates for sacrifice in the rush to meet project deadlines. Unfortunately, designing systems with both cybersecurity and usability in mind is easier said than done and typically requires a change towards an organizational culture more conducive of human-centric designing. This position paper advocates for expanded research to explore the connection between culture and engineering practices, highlighting their impact on advancing a cyber-secure society. We explore ways in which the behavior of software development team members towards designing software and products that are both usable and cybersecure can be influenced through organizational culture. We conclude that initiating change within culture requires additional knowledge that future research must seek to provide. Three of these areas are discussed in the paper for immediate attention. The practical implication of this paper is that it encourages research in the field and provides some propositions to guide future empirical investigations.

Keywords: Security-by-design, Human-computer interaction and security (HCISec), Cybersecurity, Software development

INTRODUCTION

The increased dependence on digital systems and processes, coupled with an increased threat level and a rising number of cyber incidents stress the importance of raising the cybersecurity bar. Cybersecurity has transformed into an essential prerequisite for a secure and digitalizing society. The European Commission has proposed new cybersecurity regulations for safer and more secure products through the EU Cyber Resilience Act (CRA). The proposed CRA imposes cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network. Furthermore, it introduces cybersecurity by design and by default principles and demands a duty of care for the full product lifecycle[1].

[1]See EPRS Briefing on the EU Cyber Resilience Act (14-12-2022).

This paper argues in support of further research in the field with a view to establishing the link between organizational culture and engineering practices and their implications for growth towards a cyber-secure society. It highlights the need for designing for user experience in security engineering: the practice of constructing secure systems. In particular, it deals with the role of culture in promoting *human-centric security engineering* in software development teams. We explore ways in which behavior of software development team members, towards designing software and products that are both usable and secure, can be influenced through organizational culture. The practical implication of this paper is that it encourages research in the field and provides some propositions to guide future empirical investigations.

ENGINEERING USABLE AND SECURE SYSTEMS

Some years ago media reported on a hack of security cameras and video baby monitors due to inadequate built-in security, causing live images from these cameras to be shared *en masse* on the internet. More recently, a group of hackers breached a massive trove of security-camera data collected by tech startup Verkada, gaining access to live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, prisons and schools (Turton, 2019). Companies whose footage was exposed include carmaker Tesla. Hackers were able to view videos from inside women's health clinics, psychiatric hospitals and the offices of Verkada itself.

This example shows the importance of designing software and products with cybersecurity in mind from the start rather than bolting it on after products have been deployed. Software developers therefore ideally take security into account from the start. A security mindset among developers is a good step forward. But it is certainly not a panacea for more cybersecurity, for it does not automatically lead to improved security (Sasse & Flechais, 2005; Furnell, 2005), especially when the products and applications that include the software are intended to be used by end users. Too often, the security settings in these products and applications make it too difficult for people to simply use them as intended, causing more, rather than less, insecurity (Van der Kleij, 2022).

While the importance of designing for user experience has been long acknowledged, there has been relatively little exploration of the practical tasks involved in constructing usable and secure products and applications (Faily, Lyle, Fléchais, & Simpson, 2015). This gap was underscored by Birge (2009), who pointed out that although there has been significant research in Human-Computer Interaction and Security (HCISec) in recent years, much of it has focused on studying the usability of security controls and exploring abstract concepts like 'trust' and 'privacy', rather than the actual processes involved in system design or software development. Specifically, a considerable portion of this research in HCISec caters to the needs of end-users rather than addressing the concerns of designers and developers. Few studies have attempted to tackle the question of how designers should approach both usability and security as integral components of the design process. Unfortunately, designing systems with both security and usability in

mind is easier said than done. In many conventional projects, security and usability are not considered primary goals, making them likely candidates for sacrifice in the rush to meet project deadlines (Faily et al., 2015).

Faily et al. (2015) describe a three-year study where security and usability techniques were used in a research and development project. They describe the difficulties faced in applying security and usability techniques. For instance, they discovered that technique misappropriation may hinder the adoption of usability and security techniques. Detailed guidelines, examples, and references were provided for team-members to help apply security and usability design techniques. Although these were written with the limited usability expertise of team members in mind, cases were still found where techniques were misappropriated unintentionally. Faily et al. (2015) also describe lessons that can be learned trying to build usability and security into software systems. Important lessons learned are that designing for usability and security takes time and that, even when security and usability are pushed to the front of a design process, it may be necessary to accept that high quality empirical data may either be unavailable, or not available in the quantity designers would like.

While the approach of designing for user experience has long been recommended, it is however still under-implemented in security engineering practice (Prudjinski, Hadar & Luria, 2024). Recent studies have pinpointed the organizational climate as a significant contributor to this discrepancy (Arizon-Peretz, Hadar & Luria, 2022). Organizations are complex and their goals are multiple, and thus, software developers sometimes face conflicting demands stemming from competing organizational goals. Developers' activities in implementing security and usability techniques may often be perceived as less important than those related to other organizational facets or demands, such as meeting functional requirements, production schedules (time), and cost (Prudjinski et al., 2024). Furthermore, developing secure and usable software, requires strategies, technical knowledge, and resources, that are often not at hand (Glasauer, Maurer, Spreitzer, & Alexandrowicz, 2024).

THE LINK BETWEEN CULTURE AND SECURITY ENGINEERING

It is not surprising then, in the light of what has been said before, that several studies have confirmed a relation between organizational culture and security engineering. For instance, Glasauer (2023) outlined 13 key elements of organizational culture that foster the creation of secure systems. These include structured processes, company values, resource allocation, participation, and a culture that embraces constructive feedback and learning from errors. Experts highlight how these factors positively influence the security posture of systems in development. In a study on secure software development challenges, Tomas, Li, and Huang (2019) explored the intersection of development, security, and operations. They uncovered barriers to a strong security culture, such as management's lack of emphasis on security, conflicts between risk management and cost considerations, limited opportunities for developer involvement, and overlooking security at the project's outset. This underscores the importance of cultivating various

aspects of software security culture to ensure the development of robust and secure systems.

Although there are not many studies on the relation between organizational culture and security engineering, there is research showing a positive relationship between employees' security behavior and organizational information security culture. For instance, Parsons, Young, Butavicius, McCormac, Pattinson, and Jerram (2015) surveyed 500 Australian employees and found a significant, positive relationship between information security decision making and organizational information security culture. This suggests that improving the security culture of an organization will positively influence the behavior of employees, which in turn should also improve compliance with security policies. Similar results were found by Wiley, McCormac, and Calic (2020), Arizon-Peretz et al. (2022) and Da Veiga and Eloff (2010).

Apparently, the type of organizational culture is important for employees' information security policy compliance (Karlsson, Karlsson, Åström, & Denk, 2021). Therefore, researchers and practitioners should be aware that the different organizational cultures in an organization matter for the extent to which employees uptake information security measures. For example, Karlsson et al. (2021) mention a development toward customer orientation and marketization, i.e., the opposite of an internal focus, that may have negative ramifications for the information security of organizations.

Types of Cultures

Researchers identify different ways to describe organizational cultures. One way is through using models or typologies such as the Cameron and Quinn model of cultural archetypes in organizations. This model identifies team cultures (characterized by trust, belonging, participation, and teamwork), entrepreneurial cultures (growth, resource acquisition, adaptivity, innovation, and risk taking), hierarchical cultures (with high internal efficiency, homogeneity, methodical ways of working, and policy enforcement), and rational cultures (goal-oriented, market competition, and productive; Denison & Spreitzer, 1991). In recent years theoretical developments linking the cultural archetypes with IT security behaviors have been made (see for example Fernandes, Pereira, & Wiedenhöft, 2023). Also, empirical evidence showed that some cultural archetypes are more effective at fostering positive security behaviors. A study by Kam, Mattson & Kim (2020) showed that perceived organizational cultures in favor of stability and control promoted more positive security-related behaviors. They found no such effect for organizational cultures that valued flexibility (i.e., perceived entrepreneurial and team cultures). Karlsson et al. (2021) did a survey across different companies in Sweden and they found 'that organizational cultures with an internal focus are positively related to employees' information security policy compliance. Differences in organizational culture with regards to control and flexibility seem to have less effect. The analysis shows that a bureaucratic form of organizational culture is most fruitful for fostering employees' information security policy compliance'. Therefore, we should be

cautious about generalizing the effects of organizational culture on security-related actions across different contexts and industries. Also, different departments in organizations have different goals and therefore might have different cultures (Mintzberg, 1991).

Although these different categorizations can inform the interventions to take towards changing awareness and development, no culture fits one type entirely. Therefore, cultural dimensions to describe cultures are useful. Examples of dimensions of (organizational) cultures are Power Distance and Hierarchy and Individualism (Hofstede, 2001; Trompenaars & Hampden-Turner, 2004). Research about the links between these dimensions and security engineering is scarce, but there are cultural studies focusing on security behavior. For example, Connolly, Lang, and Wall (2019) linked the Individualism Collectivism, Uncertainty Avoidance, and Power Distance dimensions from Hofstede to information security attitudes and levels of compliance. The most relevant findings in this context are that (1) the presence of formalized controls is associated with higher levels of compliant security behavior, (2) high levels of sociability in the workplace can give rise to non-compliant security behavior, and (3) flatter organizational structures with lower communicational barriers between managers and employees are helpful in improving information security. However, other authors question the existence of a relationship between organizational culture dimensions such as Hofstede's and individual attitudes towards information security (McCoy, Stephens, & Stevens, 2009). Like the types of organizational cultures discussed before, these cultural dimensions can help to disentangle the role of organizational culture in human-centric design, but should never be considered in isolation or in a deterministic fashion.

There seems to be some invariance in the use of the terms organizational culture and information security culture. Solomon and Brown (2021) developed a theoretical model of the relationships between organizational culture, information security culture and employee compliance. Using survey data and structural equation modelling, they showed that organizational culture and information security culture indeed have significant, yet similar influences on employee compliance, and that organizational culture has a strong causal influence on information security culture. Thus, organizational culture and information security culture should be explicitly viewed as two separate, but interlinked entities, both having an influence on individual behaviors.

It is evident that, in designing for secure and usable engineering, culture plays a role in the sense that organizational culture shapes policy, management, leadership, and employees' behavior. As such, culture should be identified early on. However, aspects of the current organizational culture may hinder the promotion of the desired behavior of the engineering team members. To what extent can organizational cultures, or aspects of these cultures, be changed in order to facilitate security engineering? The next section describes research on cultivating cultures and organizing change.

CULTIVATING CULTURES AND ORGANIZING CHANGE

Generic theories about organizational change are abundant. One of the most influential models of organizational change is Lewin's Change Management Model (Lewin, 1946). This model involves three stages: Unfreeze, Change, and Refreeze, making it easier to manage and implement changes incrementally. Over the years many researchers have built on this model, resulting in a large body of research on so-called planned organizational change models (e.g., Kotter, 1996). Another much-used model, Schein's 3-Level Model (2009), identifies three levels of culture: artifacts, values, and assumptions, emphasizing addressing and aligning all three levels for effective cultural change. Further, the McKinsey 7-S Framework (Waterman, Peters, & Phillips, 1980) focuses on seven interdependent factors: strategy, structure, systems, shared values, style, staff, and skills, to ensure comprehensive organizational change. More explicitly focused on cultural change are Cameron and Quinn's Competing Values Framework (2006), seeing culture as dynamic and multidimensional, and Cultural Transformation Theory (Eisler, 1987), contrasting egalitarian and cooperative values with hierarchical and competitive values, suggesting societies can shift towards more egalitarian structures. A model of learning and communication that is much used among practitioners (Bateson, 1972) distinguishes six logical levels, arguing that, in order to change the culture (both organizational and in terms of information security), one should focus on convictions and skills, rather than the behavior itself. The assumption would be that mission or goal and identity of an organization are more or less stable and fully ingrained in the organization culture. A cultural shift starts with identifying the desired change in behavior and corresponding skills and convictions, and targets the skills and convictions.

However, when cultivating cultures in order to facilitate change in security engineering, the distinction between organizational culture and information security culture is crucial. Our take is that organizational cultural change requires an intensive process that may span years to achieve. Information security culture on the other hand might be somewhat easier to achieve as it has more limited focus. However, in changing information security culture, dimensions of the overarching organizational culture should be taken into account. For example, control-oriented organizational cultures are found to be conducive to information security compliant behavior. For an information security subculture to be effectively embedded in an organization's culture, the dominant organizational culture would have to be considered first.

Although the link between culture and engineering practices has long been confirmed, only few studies show how to cultivate organizational cultures that are friendly to human-centric security-by-design. For instance, Alshaikh (2020) identifies and explains five key initiatives that organizations have implemented to improve their respective cybersecurity cultures. The five key initiatives are: identifying key cybersecurity behaviors, establishing a 'cybersecurity champion' network, developing a brand for the cyberteam, building a cybersecurity hub, and aligning security awareness activities with internal and external campaigns. Although this research was focused

on promoting cyber-secure behaviors by employees, these key initiatives could help organizations exceed minimal standards-compliance in software development teams to create functional cybersecurity cultures.

Alhogail and Mirza (2014) summarize the most important guidelines and models that have been proposed in this domain, e.g., Kotter's Eight-Step Model, Schein, and Ulrich's Seven-Step Model. They conclude that there is a scarcity of culture change models targeting information security culture. Therefore, they highlight the main change management principles that could be used in the field of information security culture. In addition, they propose a multistep framework to help professionals and researchers to achieve a successful information security culture change within organizations. In a more recent overview, Uchendu, Nurse, Bada, and Furnell, (2021) identify the most important factors in creating information security culture change, i.e., top management support, policy and procedures, and awareness.

Overall, at least three major factors are agreed upon across the literature (see, for example, Da Veiga & Eloff, 2007). First, leadership plays a crucial role. There must be management commitment to invest in a security mindset in the development process. Leaders can shape culture by communicating a clear vision and values that reflect the desired culture. By being consistent in emphasizing these elements in communications and decision-making, leaders can inspire development team members to take responsibility for developing a secure product in all its facets. Second, organizations can exert a powerful influence on culture through policy. By establishing development guidelines that promote desired actions and discourage undesirable behavior in development teams. This can range from ethical guidelines, rules regarding writing secure code and involving end users early in the development process to introducing a reward system that is in line with the desired culture. Finally, by making employees aware of the importance of information security and providing them with training, the desired culture can be promoted. It is important to ensure that training is updated regularly and that development teams stay informed about the different perspectives on security-by-design. In addition, one needs to make sure to appoint people to the teams with knowledge of required perspectives on cybersecurity or to let end users participate in the development teams, for example through working groups in which they can contribute to the development process. Future research should seek to test and validate these principles for application to the information security domain.

TOWARDS AN AGENDA FOR RESEARCH

In this article we have highlighted how research into human-centric security engineering has begun to contribute in significant ways to the standing of a more cyber-secure society. At the same time, we are proposing that human-centric security engineering still requires research. We suggest three of these areas that need immediate attention.

A first area of research would address the balance between usability and cybersecurity; usually security is added at the expense of usability. We claim that future research should not focus on security OR usability, but on

security AND usability. Designing systems with cybersecurity in mind is still a challenge, and continuing efforts are needed to ensure that IT security systems are designed for user experience.

A second component of this research agenda should involve a critical assessment of the impact of culture on human-centric security engineering. Several studies have confirmed a relation between organizational culture and engineering. This underscores the importance of cultivating various aspects of software security culture to ensure the development of usable and cybersecure systems. Culture should be identified early on when designing systems as well as interventions to support human-centric security engineering. However, there is a scarcity of culture change models targeting security culture. An integrated conceptual model is needed as a first step in providing a coherent framework for future research. Such a framework should explicitly address organizational culture, cybersecurity culture, and the role these can play in enhancing security behaviors, and as such, be based on existing models from the domains of corporate anthropology, information security, and behavioral psychology. We also like to stipulate the need for proper and employable definitions of cybersecurity culture and the need to develop tools and metrics for guiding, evaluating and comparing security culture raising programs (see also Karyda, 2017).

The third component of this research agenda, and the one which is most actively underway, would investigate the interplay between organizational elements (including organizational structure, type and management practices) and cybersecurity culture in practice. Culture is not only about behavior, but very much about the why of behavior. Therefore, cybersecurity culture change should focus on convictions, skills, as well as behaviors. We need insight into how culture is changing in organizations and the role that behavior can play to facilitate the process. There seems to be a consensus that, although models and theories are in place, empirical research about the relation between organizational culture, security culture, and behavior is scarce. Therefore, empirical applied research should be an important and integral part of this research agenda.

We recognize that this article raises more questions than it answers regarding future research directions in human-centric security engineering and how such an agenda can enhance our broader understanding of the field. Consequently, we challenge cybersecurity researchers from all disciplines to help develop a coherent research agenda that builds on the progress already made.

REFERENCES

Alhogail, A., & Mirza, A. (2014). A Framework of Information Security Culture Change. *Journal of Theoretical & Applied Information Technology*, *64*(2).

Arizon-Peretz, R., Hadar, I., & Luria, G. (2022). The importance of security is in the eye of the beholder: Cultural, organizational, and personal factors affecting the implementation of security by design, IEEE Trans. Softw. Eng., vol. 48, no. 11, pp. 4433–4446.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98,* 102003.

Bateson, G. (1972). The logical categories of learning and communication. Steps to an Ecology of Mind, 279–308. Birge, C. (2009). Enhancing research into usable privacy and security, in Proceedings of the 27th ACM international conference on Design of communication. ACM, 2009, pp. 221–226.

Cameron, K. S., & Quinn, R. E. (2006). *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework*. Jossey-Bass.

Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information security behavior: A cross-cultural comparison of Irish and US employees. *Information Systems Management, 36*(4), 306–322.

Da Veiga, A. & Eloff, J. H. (2007). An information security governance framework. *Information systems management, 24*(4), 361–372.

Da Veiga, A. & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & security*, *29*(2), 196–207.

Denison, D. R., & Spreitzer, G. M. (1991). Organizational culture and organizational development: A competing values approach. *Research in organizational change and development, 5*(1), 1–21.

Eisler, R. (1987). The Chalice and the Blade: Our History, Our Future. HarperOne.

Faily, S., Lyle, J., Fléchais, I., & Simpson, A. (2015). Usability and security by design: a case study in research and development. USEC, San Diego, CA, USA.

Fernandes, P., Pereira, R., & Wiedenhöft, G. (2023). The Effect of Organizational Cultures on Relationships between IT Governance and Individual Behavior. *Emerging Science Journal, 7*(5), 1602–1635.

Glasauer, C. (2023). The PREVENT-MODEL: human and organizational factors fostering engineering of safe and secure robotic systems. *J. Syst. Softw. 195*, 111548.

Glasauer, C., Maurer, L., Spreitzer, C., & Alexandrowicz, R. W. (2024). Development & psychometrics of the Solid-S–An inventory assessing software security culture in software development companies. *Computers & Security*, *140*, 103753.

Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. Sage publications.

Karyda, M. (2017). Fostering Information Security Culture In Organizations: A Research Agenda. *MCIS 2017 Proceedings*. Http://aisel.aisnet.org/mcis2017/28

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security, 30*(3), 382–401.

Kotter, J. P. (1996). *Leading Change*. Harvard Business Press, Boston, MA.

Lewin, K. (1946). Action research and minority problems. *Journal of Social Issues, 2(4),* 34–46.

McCoy, B., Stephens, G., & Stevens, K. J. (2009). An investigation of the impact of corporate culture on employee information systems security behaviour. 20th Australasian Conference on Information Systems (ACIS), Melbourne.

Mintzberg, H. (1991). The effective organization: forces and forms. *MIT Sloan Management Review, 32*(2), 54.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129.

Prudjinski, M., Hadar, I., & Luria, G. (2024). Exploring the Role of Team Security Climate in the Implementation of Security by Design: A Case Study in the Defense Sector. *IEEE Transactions on Software Engineering*.

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management, 34(4),* 1203–1228.

Schein, E. H. (2009). *The corporate culture survival guide* (Vol. 158). John Wiley & Sons.

Tomas, N., Li, J., & Huang, H. (2019). An empirical study on culture, automation, measurement, and sharing of DevSecOps. In: 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8.

Trompenaars, F., & Hampden-Turner, C. (2004). Managing people across cultures. Chichester: Capstone.

Turton, W. (2019, March 9). Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals. Bloomberg. Retrieved from: https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

Van der Kleij, R. (2022). From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design. In: Tareq Ahram and Waldemar Karwowski (eds) Human Factors in Cybersecurity. AHFE (2022) International Conference. AHFE Open Access, vol. 53. AHFE International, USA.

Waterman, R. H., Peters, T. J., & Phillips, J. R. (1980). Structure is not organization. *Business Horizons, 23*(3), 14–26. https://doi.org/10.1016/0007-6813(80)90027-0

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & security*, *88*, 101640.