Human Factors in Cybersecurity, Vol. 53, 2022, 49–57
https://doi.org/10.54941/ahfe1002201

Information Security Awareness and Training as a Holistic Key Factor – How Can a Human Firewall Take on a Complementary Role in Information Security?

Erfan Koza

Clavis Institute for Information Security, Niederrhein University of Applied Sciences, Germany

ABSTRACT

Human elements have been identified as a factor in over 95% of all security incidents. Current technical preventive, corrective, and defensive mechanisms address intelligent and practical approaches to increase the resilience of information technology (IT) systems. However, these approaches do not fully consider the behavioral, cognitive, and heterogeneous motivations that lead to human failure in the security causal chain. In this paper, we present the Awareness Continuum Management Model (ACM2), which is a role-based and topic-based theoretical approach for an information security awareness and training program that uses Boyd's observe–orient–decide–act (OODA) loop as a framework. The proposed ACM2 is based on the situational engineering method and regards the human firewall as an integral, indispensable, and complementary part of the holistic approach to increase IT systems' resilience. The proposed approach can be applied to different types of organizations and critical infrastructure and can be integrated into existing training programs.

Keywords: Information security, Human factors, Awareness, Training, CISO

INTRODUCTION

According to the interpretation of its holistic approach, information security consists of three interactive and coherent elements, namely, technical security, organizational security, and human factors; the interaction of these elements is propagated in a variety of differentiated models (NIST 2018; DIN, 2017). Moreover, the interaction of these elements trivially leads to the interpretation that an adequate level of information security can only be achieved if all three factors are planned and executed in a complementary view. Consequently, human factors can be defined as an essential subfield of information security that is aimed at ensuring and maintaining system security continuously and evolutionarily. Human factors act in interactive environments. Such interactive environments are collectively embedded in a global network with 24/7 availability (always on status) and a bi- or multidirectional communication network. In addition to traditional human–computer

interactions, automated processes and communication paths are set up and executed in machine–machine interactions. The increasing progression of system complexity, heterogeneity, and interactivity leads to increasing internal and external interfaces and attack vectors, which can be attacked by exploiting human vulnerabilities. As a result of the deep penetration of information technology (IT) in almost all areas of an organization's value chain, human aspects of information security can be defined as the core elements of security-related considerations (Widdowson et al. 2015). Given this interpretation, an adequate level of information security can only be achieved if the conceptual thought processes of strategists and cybersecurity experts take up such collective point of view and they interpret the weighting of the sociological characteristics of system users in relation to their specialist knowledge and risk awareness in the same way as they do for technical system characteristics (Bhahari et al. 2019; Jeong et al. 2019). Therefore, the goal of the current work is to conceptualize a model in the context of information security awareness based on the observe–orient–decide–act (OODA) loop, which supports sustainable and efficient information security awareness and training. The conceptualized model focuses on the role- and topic-based interactivity, dynamics, and diversity of cyberattacks and is intended to enable efficient information security awareness. The goal of this work is to conceptualize the Awareness Continuum Management Model (ACM2) based on Boyd's OODA loop so that the "human firewall" can take on a complementary role in information security. Herein, practice-oriented approaches should be conceptualized as their integration can optimize general and specific information security awareness so that the role of human factors is defined not as a weak point but as an efficient pillar in the information security chain. Therefore, this work focuses on the conceptualization of a new theoretical awareness management model to contribute to the sustainable, dynamic, and efficient assurance of an adequate level of information security while considering a holistic approach. This research stream includes the design of the ACM2 to define strategies and frameworks for identifying, remediating, and monitoring human vulnerabilities and disseminating this information to relevant strategic stakeholders. At the core of the ACM2 is the development of efficient strategics approaches to eliminate relevant remediating vulnerabilities in terms of a continuous awareness program and effective strategies with which CISO seek to prioritize the human vulnerabilities they address and ensure that the human firewall actively contributes to the holistic improvement of the resilience of IT systems. Thus, this research area addresses human factors and the ways in which managers and CISO can be motivated to engage in behavior that is compliant with information security. The aim is to get CISO to apply their theoretical knowledge of information security in practice and convince them of the importance of their actions.

METHODOLOGY

The conception of a metamodel requires the integration of an appropriate methodology that identifies existing methods and tools as best practices, adapts, and applies them step by step to the specific elementary structure of the

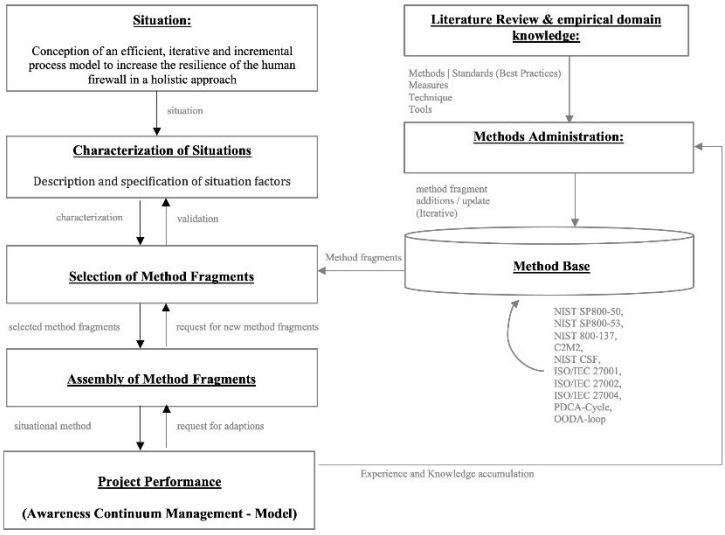

Figure 1: Situational method engineering model for ACM2.

research questions. Thus, the basic idea is based on the concept of a new method that will be implemented through consolidation, optimization, and adaptation of existing methods. This approach deliberately eliminates the need to design a completely new method. Thus, Patel et al. (2004) emphasized that the reuse of existing methods gives method creators the opportunity to adapt other effective benefits from the knowledge and experience already gained. In addition, Mayer et al. (1995) explained that the creation of a new method should only take place if previous methods prove to be incapable of adapting and that this prerequisite must first be verified by adequate expansion and optimization attempts of existing methods. Such expansions and modifications are implemented using metamethods such as method tailoring or situational method engineering from the field of method engineering. Method engineering addresses the research of new methods for the construction, evaluation, and management of the conception of information system development methods through the integration of engineering practices. Method engineering is particularly suitable as a supporting method for the selection and integration of individual method components (Rolland, 2007). To consider the resulting outcomes and the specific procedural properties of previous information security awareness methods, this work draws on the methodical approach of situational method engineering accordingly and uses it for further modeling. Fig. 1 illustrates the intended processes of situational method engineering.

The "Method Base" represents the central component of situational method engineering and integrates the selected method fragments and measures that have already been identified through literature research or empirical domain knowledge in two separate autonomous runs. The main process of situational method engineering is determined by the starting point "Situation." After this process module, the specifics are characterized and documented as situational factors. As a result of the characterization of

situations, suitable method fragments are selected from the method base. In the next step, the selected method fragments are consolidated. Thereafter, the so-called "situation-related method" is implemented, ultimately representing the result (Harmsen, 1996). Based on the defined specific situations, the individual phases are operationalized. In the first phase, the foundation of the metamodel is conceptualized by selecting the relevant question segments from the method base and integrating them into the ACM2. In the second phase, the base model obtains its operational framework. Here, the defined base model ACM2 is integrated into the modified OODA loop. For this modification, the process step selection of method fragments is used; this process reflects situation 1 in terms of content. In the third phase, situation 2, which involves the conception and integration of the role-based threat matrix, is addressed. In the fourth phase, situation 3 is addressed. In this phase, the topic-based threat matrix is integrated. In the last phase, the composition of the individual fragments takes place. At this point, the individual steps of the modified OODA loop are addressed as a framework that defines situation 4.

AWARENESS CONTINUUM MANAGEMENT MODEL (ACM2)

The ACM2 can be divided into four sections (design, development, implementation, and post-implementation). Each section provides a modular design, which is relevant to the next section. Fig. 2 outlines the ACM2.

Before the operationalization of the ACM2, the fundamentals must be defined in the design section. The overall strategy for information security awareness and training programs must also be documented. For this purpose, the goals, objectives, roles, responsibilities, and measurement of the program must be described (NIST, 2003). The use of the ACM2 ensures a uniform training strategy in the organization, whereby the overriding goal can be defined equally for all instances. This application enables the comparison of different areas, departments, and roles. The possibility of direct comparison allows those responsible to define the best practices within their own structures and optimize their processes. In this way, the relationships, incentives, and reasons that are vital to the successful implementation of programs can be identified. The definition of objectives must not contain any generally valid formulations. Therefore, a specific, measurable, achievable, realistic, and time-bound (SMART) formulation should be used to define objectives. Objective definitions that are not measurable and specific enough cannot be monitored quantitatively and qualitatively even after operationalization. Here, a content-related reference to the Integrated Behavior Model (IBM) can also be made. The factors defined in IBM, such as attitude or behavioral intention, are in a coherent relationship with the actual behavior of a person. However, this correlation increases when the factors are at the same level of generalization. The better the correlation effect is, the more specific it is. For the processes to be measurable and thus generate real benefits from IBM, the objectives must be specifically instantiated (topic-based or role-based) to a particular security-compliant behavior (NIST, 2003). In this definition, objectives are ultimately defined in terms of employees or topics (e.g., compliance with a clean desk policy). Accordingly, an appropriate SMART formulation

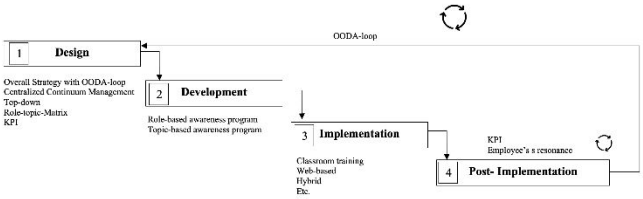

Figure 2: Awareness continuum management model (ACM2).

can be defined for system operators in a virtual power plant (Koza et al., 2021) as follows: "With the awareness program, all system operators should be sensitized (measurable) regarding the clean desk requirements (specific) at least once (achievable) in the next 12 months (realistic)." For objectives to be fine-tuned and specific in granularity, the roles and the corresponding training needs must first be identified through a requirements analysis. First, a requirements analysis is conducted by the CIO as a central element; here, the necessary topics and relevant employees must be identified. In this process step, all roles that have a direct and indirect impact on the basic values of information security, namely, "availability," "integrity," and "confidentiality," according to the failure criticality (e.g., executives and managers, IT security staff, system/network administrators as superuser, normal user, externals with access to critical assets) are defined using a top–down methodology. Thus, the integration of internal and external roles takes place systematically and hierarchically from top to bottom along the organizational landscape. By assigning people to individual roles, one can form homogeneous groups or clusters in which employees with equivalent task profiles and technical knowledge levels can be integrated. Another advantage of this clustering is reduction of complexity, which ultimately allows the principle of "setting the bar" to be implemented efficiently and in a targeted manner. After clustering, requirements analysis can be used to assign the identified training and awareness needs to individual clusters (NIST, 2003). The merging of topics and roles into clusters can be documented and visualized in a roles–topics-based threat matrix (Figure 3). In principle, the annex to ISO/IEC 27001 with its controls can be used to determine technical and organizational topics. The matrix specifies an assignment of involved systems and roles to the threats and is mapped in homogeneous clusters. The previous results can be visualized in a portfolio. The present example shows how such a classification can be defined as an instantiable model. Individual details can be specifically changed, modified, and executed in an organization-and system-specific manner.

The matrix is classified as instruments in the observe and orient phase. Each volatile and dynamic change at the internal personnel level, system level, hazard level, and probability of occurrence level triggers a new observation and orientation. Thus, the information and especially the threat situation are visible in a transparent and dedicated way so that any remaining vulnerability or incident can be immediately assigned to its relevance and importance. This scenario gives cybersecurity engineers an order in their perception and orientation processes. In addition, cybersecurity engineers can now update

	Threats (T)						
Role	T 1	T 2	T 3	T 4	T 5	T 6	Cluster
Role 1	x	x			x	x	HR - Cluster
Role 2	x	x			x	x	
Role 3		x	x		x	x	OT-Cluster
Role 4		x	x		x	x	

Cluster	Employee information	
	Department	Business Impact
RC 1	HR	High
RC 2	OT	Critical

System	Threats (T)						
	T 1	T 2	T 3	T 4	T 5	T 6	Cluster
System 1	x	x		x	x	x	Exchange Server
System 2	x	x	x		x	x	SCADA
System 3	x	x	x		x	x	

Cluster	Employee information	
	Department	Business Impact
SC 1	Exchange Server	High
SC 2	SCADA	Critical

Cluster	Matrix - Classification		
	Damage-Classification	Probability of occurrence - Classification	Matrix (3 x 3)
RC 1	2	2	4
RC 2	3	3	9
SC 1	2	1	2
SC 2	3	3	9

Figure 3: Itemization of a roles-topics-based threat matrix.

their threat situation in terms of monitoring in a time- and event-oriented manner. "He who writes, stays" is the essential advantage here because only information that is recorded and documented in a structured manner can be evaluated, analyzed, successively optimized, and supplemented. In the development and implementation phase, role-based and topic-based trainings are conducted. Depending on their relevance, different operational plans should be developed. However, as mentioned previously, this planning is dependent on the individual results from the observe phase. In the post implementation phase, the effectiveness of the training is verified. Feedback methods (survey, questionnaire, benchmarking, etc.) play a relevant role here. The awareness and training program must be updated regularly to keep pace with technological progress. Network landscapes are changing and must be considered accordingly. Change management processes should also be applied. In addition, the OODA loop is used to record resonances dynamically and promptly. In the following Fig. 4, the individual phases of the OODA loop are transferred to the context of information security awareness.

For this purpose, we use the defined "Relationship of objects in an information security incident" of ISO/IEC 27035-1 and conceptualize the OODA loop. The OODA loop adopts in this context the logic of Boyd's OODA loop, but the two crucial phases, namely, observe and orient, are modified to implement the specific aspects of information security awareness in the loop. The primary modification concerns the observe phase and is performed by integrating the principles of SA. In addition to the existing technical and organizational monitoring mechanisms, two instruments are integrated for this purpose. The topic-based and role-based threat matrix serve as a technical framework in this context and play a central role in 360-degree monitoring. The secondary modification concerns the orientation phase to determine the orientation criteria that are relevant to information security awareness. The first factor group comprises the threats and vulnerabilities and is integrated as an orientation criterion for the weighting of the recorded internal and external information. The second factor group includes assets,

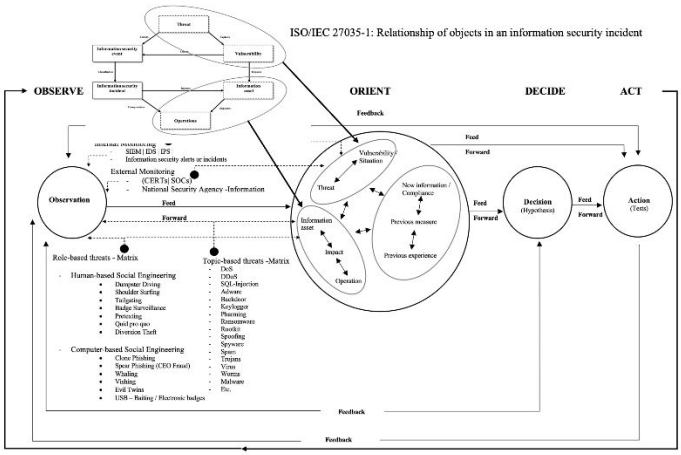

Figure 4: Modified OODA loop.

impacts, and operations and is used as an orientation criterion for the weighting of the captured information from the matrix as well as for the evaluation of the internal and external information captured. Thus, security awareness training and programs can be developed. The last factor group takes over the unchanged logic of the OODA loop to supplement the mental security models with proven models and experiences. To ensure the planning, implementation, and monitoring of the awareness and training programs in terms of continuity, the overall strategy uses the modified OODA loop methodology. This approach allows the integration of the basic aspects of the information security awareness and training program with four sections: design, development, implementation, and post-implementation. The advantage of the OODA loop over the Deming cycle (PDCA cycle) is its dynamic and highly efficient responsiveness. Situational Awareness (SA) enables a fully comprehensive consideration of relevant topics because security experts consider not only internal factors but also external factors and influences. Within the framework of the OODA loop, operationalization can take place through the concept of SA. The basic idea is the strategic advantage that one would like to achieve over attackers (time critical) to be able to use the opportunity to act (preventive planning) and react (corrective planning in the sense of business continuity management) in a meaningful way. In this context, the actions and movements of attackers are continuously observed in the first step (observe). A change or modification of the attack vectors, methods, targets (role- and topic-based attacks), one's overall strategy, compliance requirements (changes in the legal situation), and impact ultimately provide the immediate reason for planning strategic and operational actions and reactions (orient). Further observations must be triggered from external information sources, for example, to obtain verified and industry-specific information. To this end, the relevant information on current vulnerabilities and attack vectors is collected via the interfaces of computer emergency response teams, security operation centers, and the National Security Agency. However, for the completion of the observe phase, employee responses and the quantitative

metrics determined must also be integrated into the process in the form of feedback loops so that internal personnel and technical and temporal changes can be considered. Findings from the orient phase can then be used to derive effective decisions (decide) that can ultimately be operationalized and executed (act). In the orientation phase, a multidimensional analysis and consideration are conducted to examine the collected information in detail. For this purpose, the factors with their mutual influences must be brought into a coherent form as much as possible. The multidimensional analysis must therefore include the following factors and indicators: impact, current situation, current vulnerability, identified attack or threat, new information (employee response) or change in compliance, and previous action and experience. As a result, the essential goal of the OODA loop is to maintain the awareness of the function's current cybersecurity state across the operational environment. For this purpose, IT and OT systems and cybersecurity information are collected, analyzed, alerted, presented, and utilized to identify anomalous activities, vulnerabilities, and threats to the function to support incident response and organizational risk management decisions. The OODA loop should ultimately be integrated into the ACM2, which can also be understood as a central continuum management model. The goal of the ACM2 is to ensure a learning continuum.

CONCLUSION

Human factors represent a sensible extension in the security chain and can lead to the avoidance of incidents in the sense of prevention, reaction, and detection. Therefore, human factors must be given special consideration. As ICT dependency increases, we also recognize that the threats in the cyber environment are increasing and that human factors are often involved. Although awareness and training models exist, they need targeted and, above all, specific models that can be customized for organizations. Factors from other disciplines, such as health psychology, also play an important role. ACM2 provides the necessary framework to implement a sustainable awareness and considers internal and external influences. The ACM2 is to be understood as a dynamic, interactive, and incremental model, whose core is the OODA loop. An OODA loop can be used to define an iterative and incremental framework in which the dynamics of events in terms of interactivity and the mutual relationships with the environment (cybercriminal activities and their radius of action) can be considered depending on the situation. The main characteristic features are dynamism, interactivity, continuity, and timeliness. The ACM2 reduces complexity. The identified topics (weak points, attack methods, attack vectors, etc.) can be defined by the roles–topics matrix and practically established as a process in terms of continuous improvement. The heterogeneity in the organizational workforce is efficient and sustainable by clustering employees. The focus here is on the role-based or group-specific alignment of awareness activities. This description means that employees who ideally have the same task profile, the same IT skills, and the same work environment can be integrated into the roles–topics matrix and consolidated as a homogeneous cluster. The complexity and diversity of security topics can also

be determined in a role-oriented manner by using a matrix. For a rich understanding and for an efficient approach, reference can be made to the topics of ISO/IEC 27001, which define the state-of-the-art methods. ACM2 also defines a way to set individual goals (SMART goals). However, the measurement and monitoring of individual processes and success steps are complex tasks that are beyond the scope of this work. Nevertheless, the ACM2 provides the OODA loop with the necessary prerequisites and framework to perform such evaluation processes (depending on the defined goals).

REFERENCES

Bhaharin, S. H., Mokhtar U. A., Sulaiman, R., Yusof, M. (2019): "Issues and Trends in Information Security Policy Compliance," in IEEE: Proceedings of the 6th International Conference on Research and Innovation in Information Systems: Empowering digital innovation (ICRIIS), Johor Bahru, Malaysia, pp. 1–6.

Boyd, J. R., (2018): A Discourse on Winning and Losing, edited, and compiled by Dr. Grant T. Hammond, Maxwell, AFB, Alabama, pp. 1–400.

Boyd, J. R. (1976): "Destruction and Creation," pp. 1–8.

DIN EN ISO/IEC 27001:2017-06, (2017): Information Technology-Security techniques- Information security management systems- Requirements, Beuth Verlag, Berlin, Germany, 2017, pp. 1–35.

Harmsen, A.F. (1996): "Situational Method Engineering," Habilitation, University of Twente, pp. 31–41.

Jeong, J., Mihelcic, J., Oliver, G., Rudolph, C. (2019): "Towards an Improved Understanding of Human Factors in Cybersecurity," in IEEE 2019: Proceedings of the 1st International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS) and the 5th International Conference on Collaboration and Internet Computing (CIC), IEEE, Piscataway, N. J., pp. 338–345.

Koza, E. Öztürk, A. (2021): "A Literature Review to analyze the State of the Art of Virtual Power Plants in Context of Information Security" in Progress in IS, in: Volker Wohlgemuth & Stefan Naumann & Grit Behrens & Hans-Knud Arndt (ed.), Advances and New Trends in Environmental Informatics, pp. 49–69, Springer.

National Institute of Standards and Technology, (2018): Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018, Accessed on: August 19, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

National Institute of Standards and Technology, SP 800 – 50, (2003): Building an Information Technology Security Awareness and Training Program, in NIST Special Publication, pp. ES-1 – A9.

Patel, C., De Cesare, S., Iacovelli, N., Merico, A. (2004): "A Framework for Method Tailoring: A Case Study," in Proceedings of the Second Workshop on Method Engineering for Objected-Oriented and Component-Based Development, M. Serour, Ed. Centre for Object Technology Applications and Research, Sydney, pp. 23–37.

R. Mayer, R., Crump, J. W., Fernandes, R., Keen, A. K., Painter, M. (1995): "Information integration for Concurrent Engineering (IIEC) Compendium of Methods Report," College Station: Knowledge Based System, Inc., pp. 1–150.

Rolland, C. (2007): "Method Engineering: Trends and Challenges," in: Ralyté J. Brinkkemper S., Henderson-Sellers B. (eds) Situational Method Engineering: Fundamentals and Experiences. ME. IFIP – The International Federation Processing, Vol. 244, Springer, Boston, MA, p. 6.

Widdowson, A.J., Goodliff, P. B. (2015): "CHEAT, an approach to incorporating human factors in cyber security assessments," 10th IET System Safety and Cyber-Security Conference, Bristol UK, 2015, pp. 1–5.