Research Report

Employees' Struggle with Information Security

TO INCREASE THE INFORMATION SECURITY AWARENESS AMONG THEIR WORKFORCE AND TO ACHIEVE SECURE INFORMATION SYSTEMS, DECISION-MAKERS EMPLOY MEASURES OF INFORMATION SECURITY, SUCH AS SECURITY POLICIES OR ASSOCIATED TRAINING AND EDUCATIONAL PROGRAMS. HOWEVER, THESE MEASURES MIGHT STRESS EMPLOYEES. THIS IS TRUE IF, FOR INSTANCE, INFORMATION SECURITY MEASURES ARE PERCEIVED AS DIFFICULT TO UNDERSTAND, AS AN INVASION OF PRIVACY, OR IF THEY GIVE RISE TO CONFLICTS OF INTEREST. CONSEQUENTLY, A MULTI-FACETED PERSPECTIVE ON EMPLOYEES' STRUGGLE WITH INFORMATION SECURITY IS DISCUSSED.

Clara Ament

Steffi Haag

Introduction

Over the last years, the frequency of information security incidents, such as intellectual property or customer data theft, has increased tremendously and also the financial losses affected organizations are confronted with have soared. Moreover, affected organizations often overlooked negative longterm effects, such as reputational damages, the decline in customer trust, and the resulting fatal effects such information security incidents can have on businesses.

To avert these risks, organizations allocate a significant amount of resources to the protection of their information systems. They secure their networks by using, for instance, firewalls, encryption techniques, and antivirus programs. Though, a purely technical defense neglects "the weakest link" in the information security chain. An ever so technically secure system can still become a victim of human errors. A holistic security strategy is desirable as incidents frequently originate from the unaware or aware but non-malicious behavior of organization's own employees. To overcome this issue, various approaches have been suggested to cover, among others, information security policies, awareness programs, and security training. Such measures are supposed to decrease shortcomings in employees' security behavior and to equip personnel with a sound orientation for secure decision-making.

First evidence, however, points out that secure information systems will not be achieved if employees perceive elements of behavioral information security or even the company's entire information security strategy as difficult to understand, overwhelming, or time-consuming (D'Arcy et al., 2014). In other words, employees can feel strain and pressure due to organizational information security requirements and experience so-called security-related stress.

Methodology

Because this field of research is scarce and lacks reliable quantitative measures that comprehensively capture stress from information security requirements, a first logical step was to conduct expert discussions as well as a number of target group interviews to examine employees' struggle with information security requirements. A subsequent pretest evaluated the instrument and examined its validity (Ament and Haag, 2016). Based on these results, a large questionnaire-based survey with 213 participants was implemented in mid-2016.

Empirical Findings

An information security strategy has complex consequences and a multi-layered effect on employees. The findings suggest six stressors of information security:

- *Complexity:* Often information security policies are rather difficult to understand as they use technical jargon. Consequently, employees have to spend time and effort on learning, understanding, and implementing information security requirements. Furthermore, the complexity of security requirements possibly exceeds an employee's intellectual abilities. As such, interview partners pointed out that they fear to unintentionally cause an information security breach.

- *Overload:* Overload is a common work-place stressor, which also applies to the information security context. Due to information security requirements, employees have to fulfill additional tasks and are confronted with more work than they can handle. As a result, they are forced to work faster in order to fulfill their actual tasks in time, which leads to a decrease in working quality. In addition, information security measures, such as the pop-up of a security scan, interrupt the routine workflow and lead to multitasking.

- *Uncertainty:* As a consequence of rapid technology developments, technical and behavioral information security is in the course of constant transition. This includes changes in information security policies, procedures, and technologies alike. Employees have to continuously update their security knowledge, which prevents them from building a solid security routine.

- *Invasion of privacy:* Moreover, employees' information security behavior can be easily monitored and tracked. This might include monitoring staff members' Internet usage or E-mail traffic. Employees are stressed out because they fear that their employer could violate their privacy.

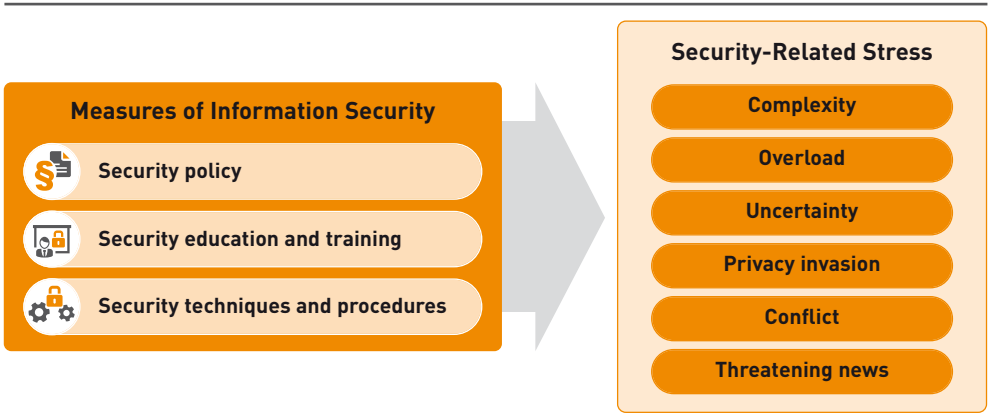

Figure 1: Security-Related Stress

- *Conflict:* Furthermore, stress can result from the interaction with superiors, peers, or customers. In addition to their business role, employees have to occupy a secondary role with regard to information security. As such employees can feel stressed if confronted with supervisors' instructions or requests by peers that deviate from established information security requirements. In such cases, employees feel stressed because they have to either violate existing regulations or to face confrontation with colleagues. For example, if security policies prohibit sharing computer passwords, an employee who will be on leave could refuse to give his login credentials to the colleague who is supposed to be his vacation replacement. This might lead to an argumentation on the common practice which can, in turn, stress the affected employee.

- *Threatening news:* Study participants stated that they feel unsettled when hearing about substantial security breaches or the misuse of sensitive data. Triggered by the possible risk of a threat, individuals are prone to perceive stress. The magnitude thereby varies depending on the information source, i.e., if the information is presented by close friends, colleagues, or mass media. Here, stress levels depend particularly on the individual relevance of the news and on whether the employees are directly affected or not. For example, employees using hard- or software that was identified to have a security gap are more likely to experience security-related stress.

Furthermore, we examined the effect of security-related stress on employees' compliance towards information security policies. The results suggest that stress from complexity, overload, uncertainty, and privacy invasion negatively affects compliance intentions. Employees confronted with these stressors are more likely to disregard their company's information security policy. Stress from conflicts and threatening news, on the contrary, strengthen employees' compliance intention, at least in the short-term.

Conclusion

This study presents a multi-faceted perspective on employees' struggle with information security requirements. The results equip researchers and practitioners alike with the necessary toolset to recognize security-related stress among employees. Due to the comprehensive set of stressors, security managers can more precisely identify the actual source of security-related stress. Moreover, they can better anticipate the effects while developing security policies, and, thus, adopt countermeasures or even avert security-related stress before it emerges. Regarding our findings with respect to the social environment (stress from conflicts or threatening news), security-related stress might also be used as a security measure itself to sensitize employees.

To counteract security-related stress, the findings suggest an information security strategy which focuses on the individual employee. Adequately formulated security policies (optimally unambiguous and easy to understand) can reduce security-related stress from complexity. Moreover, information security training and education should cover the content of information security policies and involved security measures. Employees need an expert to consult if questions concerning the topic of information security arise. Besides, employees have to be informed about the relevance of information security and its needs to be anchored in job descriptions. This way, stress in terms of overload declines. Stress from the 'invasion of privacy' can be encountered by increasing awareness among employees and educating them to understand the importance of information security. If employees act in line with information security requirements, there is no need for monitoring their security behavior and, consequently, there is no stress from privacy invasion.

In an organization with a positive and constructive working atmosphere, employees which are well educated with respect to information security will be confident enough to confront their principal or peer if information security is at risk. Moreover, those who are responsible can transform security-related stress into a useful security source if they keep in mind that security-related stress has favorable aspects. A proper reaction to current information security discussions or news, for instance, via news feeds, is necessary.

References

Ament, C.; Haag, S.:
How Information Security Requirements Stress Employees.
In: Proceedings of the 37th International Conference on Information Systems, Dublin, Ireland, 2016.

D'Arcy, J.; Herath, T.; Shoss, M. K.:
Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective.
In: Journal of Management Information Systems, 31 (2014) 2, pp. 285-318.