TOWARD A PROCESS THEORY OF EMPLOYEE COMPLIANCE WITH IS (INFORMATION SYSTEMS) SECURITY PROCEDURES

Information security (IS) is a key organizational concern. One of the most significant issues identified in the IS literature pertains to why employees fail to comply with IS security procedures that are instituted per organizational policies. Often-cited problems include non-compliance with IS security procedures related to the use of passwords that are not sufficiently robust, password sharing, leaving ones computer unlocked, sending highly valuable information without encryption over email, and unsafe USB-stick practices.

To understand why employees comply (or do not comply) with IS security policies, IS scholars have formulated variance or factor models. In doing so, most of them have drawn upon health behavior theories (e.g., protection motivation theory) and criminology theories (e.g., deterrence theory, neutralization techniques). These works, while undoubtedly valuable in providing an overall view of the phenomenon, tend to offer static explanations for compliance with IS security procedures using the same set of fixed factors for different IS behaviors, whether password selection and sharing, email encryption, or not locking ones computer, for example. For example, a leading theoretical explanation used in these studies involve employees calculation of the likelihood of getting caught and how severe the sanctions would be on password selection/use of encryption/not locking their computer (deterrence theory).

We believe such static factor models ignore the dynamic elements that lead to specific compliant or non-compliant behaviors, overlooking, for example, the complexity of the thinking process and how it dynamically interacts with the context. We argue that these underlying changes are important for understanding IS security behaviors. In this paper, we take the perspective that the behavior emerges through conflict and balance between certain oppositions. For example, employees may balance organizational IS security guidelines with their own values, goals, and work preferences. Specifically, when employees choose a
suitably complex password and change the password frequently so as to ensure an increased level of protection, they may be simultaneously sacrificing their convenience as well as their efficiency, as they need to expend significant cognitive effort to create and then remember complex passwords that need to be changed frequently. Similarly, a task as simple as locking ones computer often puts the individual in a position where he or she needs to balance the (however miniscule) effort associated with physically securing the computer with responsiveness to sudden interruptions like managers asking their subordinates to the meet them right away. The point worth noting is that each security compliance scenario requires an individual to reconcile one or multiple tensions, where the opposing ends tend to differ for different security procedures.

In this study, we take a first step in this dynamic (process) direction, informed by the notion of dialectics. Specifically, we find that employees IS security behavior in organizations results as conflicts between organizational IS security procedures and other goals, values, and preferences play out. Our investigation reveals that the conflicts and how they define behaviors differ based on the nature of information security behaviors (e.g., selecting password vs. locking computer) and other elements of the context.

As a theoretical contribution, our study proposes a new dialectical process theory of IS security behavior, which highlights conflicts that continuously shape employees IS security awareness and behaviors. For practice, our results offer new insights into a key problem in IS practice, namely, employees non-compliance with IS security procedures by pointing out how the conflicts between organizations IS security requirements and employees goals, values, and preferences in their work are necessary for understanding and improving IS security behavior in organizations.

Biodata:

Mikko Siponen is a Full Professor and Head of IS Department at the University of Jyväskylä, Finland. Before that he was full Professor and the Director of the IS Security Research Center at the University of Oulu, Finland. He holds a Ph.D. in Philosophy from the University of Joensuu, Finland, and a Ph.D. in IS from the University of Oulu, Finland. He has 45 published papers in journals such as MIS Quarterly, Journal of the Association for Information Systems, European Journal of Information Systems, Information & Organization, and Information Systems Journal. He has received over 5.4 million USD of research funding from corporations and numerous funding bodies. He has served as a senior editor three times for ICIS and ECIS.