The Impact of Security Training and Awareness Programs on Employee Security Policy Compliance Behavior

Introduction
High-profile data breaches in recent years have highlighted the urgent need for better data protection in business. It cost Target $148 million to clean up the mess that resulted from a data breach [1]. That data breach happened not because Target did not have the software and hardware in place to defend its data. The real story is that Target's network credentials were stolen from a third-party business partner through a malware email attack, indicating that the weakest link in the security management chain was the human component of the security system [2]. It is a common belief that security policy is essential for increasing the information security level of an organization [3]. However, there is still a lack of consensus among scholars and practitioners regarding how to improve employees' security policy compliance behavior because the research results are mixed. The purpose of this study is to shed light on the factors that influence employees' security policy compliance behavior.

Statement of the Problem
Various theories have been used to derive the factors that affect employees' security policy compliance behavior. These include the theory of reasoned action [4], the theory of planned behavior (TPB) [4], protection motivation theory (PMT) [5], and general deterrence theory (GDT) [6]. However, the results of prior research are mixed. For example, according to GDT and PMT, fear appeal should have significant impacts on employees' ISP compliance, but the results of prior empirical studies are conflicting. Some research shows that penalties based on fear appeal influence ISP compliance [e.g., 7], while other research shows that penalties constitute an insignificant factor where ISP compliance is concerned [e.g. 8]. We thoroughly reviewed the information security literature and found that, although prior studies were based on sound theories, most prior research did not include two factors, training and awareness. Furthermore, even those studies that included the two factors did not treat them as the central factors. This may have given business managers' the erroneous impression that training and awareness programs did not have a critical impact on security management systems. We conducted a survey research project with the help of the CIO office of Western Washington University in 2015 before the university launched a security training and awareness campaign. We want to complete the stream of the research by conducting a new survey to investigate the impact of the training and awareness programs on employees' security policy compliance behavior after the university started the campaign one year ago. By comparing the results of the two surveys, we can gain insights into the effectiveness of security training and awareness programs.

Opportunity for Advancing Professional Scholarship
From the previous survey data, we have produced two security research papers that investigate the theoretical issues involved in information security research in a business setting. One of the papers is under revision and the other is under review. I hope that, with the support of the summer research grant, I can finally analyze the effect of security training and awareness programs on employees' security policy compliance behavior by comparing the results from the two surveys: one conducted before the programs started and the other after the programs started. This research project will be built on the previous two studies. It is an excellent opportunity for us to advance the research agenda and may help to identify the critical and missing factors in business information security management. By completing the second survey and the associated research, we believe that we can contribute to information security research and practice as outlined in the next section.

Impact of Study
This study has many implications for practice and research. Regarding research, it will draw on a new theoretical foundation for studying employees' security policy compliance behavior. It will also advance our understanding of the dynamics of information security management by examining the issue from a different perspective. Moreover, it will provide insights into whether factors other than those derived from traditional security research theories play more important roles in securing information systems. In practice, the results of this research may impact the direction of information security management programs since they may indicate that the practices that security managers are following have critical flaws. The results of this study may help security managers to refocus their resources to improve information security level in their organizations.
Suitability and Feasibility of the Research Methods

We will base our research model on a new theoretical foundation for human actions—the Awareness-Motivation-Capability (AMC) framework. We will conduct a cross-sectional survey study to test the hypotheses of the research model. A survey can be used to gather information about the characteristics, actions, or opinions of a large group of people, to answer the question “why,” and to test theories and associative relationships [9].

We will work with the CIO office of Western Washington University (WWU) to survey WWU employees. Previously, we completed the first survey successfully and obtained promising results for the existing studies. It is reasonable to believe that this second survey will go as well as the first one and its results will help us to answer the questions that interest us and advance our knowledge in business information security management.

We will use partial least squares (PLS) modeling to assess the measurement model and the structural model. PLS is appropriate for this study because it is variance-based and places minimal restrictions on measurement scales, sample size, and residual distribution [10]. We have acquired SmartPLS software to analyze the data as it has been used successfully for group analysis in a wide range of published studies. Group analysis is the technique that we will employ to compare the results of the two surveys.

Expected Results

This research will be built on the two prior studies. It will be a logical extension of them. One of the two studies is under revision, and the other is under review in academic journals. This study will provide insights into the under-studied factors in information security management. With the support of the summer research grant, we could produce a promising study and publish it in a high-quality information systems journal since we already have half of the necessary data, have conducted a thorough literature review, and have selected a promising theoretical foundation for the research model. We will complete the second survey in the current academic year and expect to complete the study during the summer of 2017 and to get it published soon thereafter.

References