2022

Precursors of Email Response to Cybersecurity Scenarios: Factor Exploration and Scale Development

Miguel A. Toro-Jarrin  
*Old Dominion University*

Pilar Pazos-Lago  
*Old Dominion University*

Miguel Padilla  
*Old Dominion University*

Follow this and additional works at: https://digitalcommons.odu.edu/emse_fac_pubs

Part of the Applied Behavior Analysis Commons, Information Security Commons, and the Operations Research, Systems Engineering and Industrial Engineering Commons

Original Publication Citation


This Conference Paper is brought to you for free and open access by the Engineering Management & Systems Engineering at ODU Digital Commons. It has been accepted for inclusion in Engineering Management & Systems Engineering Faculty Publications by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.
Precursors of Email Response to Cybersecurity Scenarios: Factor Exploration and Scale Development

Miguel A. Toro-Jarrin, Pilar Pazos-Lago, and Miguel Padilla

Old Dominion University, Norfolk, Virginia, USA

Abstract

In the last decade, information security research has further expanded to include human factors as key elements of the organization’s cybersecurity infrastructure. Numerous factors from several theories have been explored to explain and predict the multitude of information security-related behaviors in organizations. Lately, there has been a call for the study of specific cybersecurity behaviors in contextualized scenarios that reflect specific and realistic situations of a potential cyber-attack. This paper focuses on precursors of email response in situations that can be the origin of cybersecurity incidents in organizations (i.e., phishing attacks, ransomware, etc.). This study explores participants’ intentions to follow recommendations related to personal information handling when using email at work, attitudes towards and subjective norms relative those recommendations, and anticipated regret for ignoring secure recommendations. To capture the proposed factors, this study develops and tests a survey-based measurement. This paper describes the approach to item formulation, survey administration, pretesting, and analysis of the instrument’s preliminary psychometric properties along with preliminary evidence of predictors of compliance with information security recommendations. The developed measurement will be instrumental in future research to test the predictive capability of the factors explored in this study.

Keywords
Compliance, information security behavior, scale development, personal information, factor exploration.

1. Introduction

Employee actions threaten the confidentiality, integrity, and availability of information in organizations. These actions can be the result of human error or malicious intent [1]. This study focuses on developing a scale to capture the precursors of non-intentional acts that contravene recommendations in information security. Precursors of action research has advanced information security research in organizations. Although the situations in which insecure behaviors were studied were evaluated in general terms. Lately, there have been calls for more context-specific theorizing and measurements [2]. Aurigemma and Mattson [3] argue that compliance with each of the mandatory threat-specific security actions requires different explanatory models and suggest that the information security literature can improve if it focuses on the mechanism, treatments, and antecedents associated with required actions around specific threats. This study develops a scale to capture factors (or precursors) of ubiquitous (in)secure acts (i.e., handling personal information in the workplace online) portrayed in a scenario that presents a situation familiar to organization’s members. The study develops the scale following the information security and social sciences literature in scale development practices. The preliminary evidence suggests the explanatory and predictive capability of subjective norms regarding recommendations to influence specific information security intentional behavior described in specific situations. The evidence also indicates regret as an additional precursor of compliance. The low correlation between the evaluative factor of attitudes towards information security recommendations and the intention to comply with those recommendations suggest that this factor might not be a strong precursor of deterrence as the literature suggests. The correlation found between the evaluative factor of attitudes with descriptive norms and the potency factor of attitudes with injunctive norms suggest a possible interaction. The scale presented in this study contributes to research at providing preliminary evidence of the internal structure among factors captured using a specific action to a specific situation.

2. Problem Description

Four assumptions in the information security literature highlight the problem. First, the information security literature has focused on psychosocial factors that explain (in)secure actions [4, 5]. The assumption is that when scales are
developed to capture those factors, they are capturing all possible situations and actions. However, the situation in which an (in)secure act takes place presents other motivators besides security and compliance [6]. Organization members decide the best course of action considering alternatives that might or might not be aligned with security considerations. For example, an employee might decide not to follow a recommendation if the alternative produces a more favorable outcome for a specific situation. The study includes a scenario-based scale with contextual elements that might influence individuals to not follow security policy provisions. Additionally, the measurements are developed to capture the attitudes towards information security recommendations, instead of the evaluation of whether it is positive to follow them. Second, the information security literature mainly uses self-report measures to capture predictors of (in)secure acts in organizations. However, it is uncommon in the literature to investigate social desirability. Asking respondents whether they think they should follow rules skews responses to an affirmative answer [7]. As such, this study investigates the impact of social desirability on the measures. Third, the information security literature assumes that attitudes can be characterized with a few arbitrary terms that capture a broad assessment of the constructs (e.g., good-bad, important-unimportant). According to Osgood [8], attitudes can be capture through a variety of perspectives, evaluation (good-bad), potency (hard-soft), stability (sober-drunk), tautness (angular-rounded), novelty (new-old), receptivity (savory - tasteless), and aggressiveness (aggressive - defensive). Researchers should determine what attitudinal factors are captured by the items (or variables) and the relation they have to the behavioral objective for a specific context [9]. The variables included in this study to capture the attitudinal factors are taken from Osgood [8]. This study explores the relevance of the evaluative and potency factors of attitudes towards security recommendations to deliver a more concise list of items (or variables). In line with the information security literature, this study also includes two factors of subjective norms. Items were developed to capture descriptive norms, the perceptions of other people at work following security recommendations; and injunctive norms, the perception of how other people at work judge an act of non-compliance. This study presents first a scenario where a character acts in non-compliance with security recommendations, and then administers the scales. Additionally, the information security literature has suggested anticipated regret [10] as one additional precursor of compliance. This study captures this factor as reflecting feeling of regret due to non-compliance instead of taking an alternative course of action (i.e., using secure systems). Fourth, in many studies in the review, it is assumed that the factor internal structure is unchanged if minor changes are made to the instrument. However, good practices for scale development suggest that modifying item wording demands a factor exploration [11, 12]. Additionally, combining factors from different theoretical frames change the nomological structure. Thus, assuming internal structure and moving forward to a confirmatory factor analysis invites issues like multicollinearity, poor factor loadings, or ambiguous loadings [13, 14]. This study pretests the item wording and explores the internal factor structure of the items, leaving the confirmation of the nomological structure for a future instance with a separate sample.

3. Related Research

The information security literature suggests that factors that express security as important to organization members are precursors to following information security recommendations [5, 15]. The literature has focused on theorizing and measuring variables to align with those recommendations [16]. Another focus is on perception of threat that security incidents represents for individuals and organizations, the perception of the vulnerability of suffering such incidents, and the perceived benefits and barriers of following recommendations [17, 18]. A third avenue of research is on contextual elements, such as other priorities besides security in the workplace as predictors of (in)secure actions [19, 20]. Finally, the information security literature focuses on micro-level factors such as attitudes, norms, behavioral control towards and regarding the (in)secure actions itself as well as self-efficacy relative to taking the steps to act in alignment with information security recommendations [4, 21]. Usually, researchers use modified versions of instruments from previous research. Then, researchers confirm the factor structure typically with a confirmatory factor analysis (CFA). The internal structure is tested assuming that the modified instruments have the same internal structure than the original scales. Additionally, it is common in the information security literature to use the same data for exploring the measurement model and hypothesis testing.

4. Methodology

This study formulated several scenarios where a character act against recommendations in terms of information security. Although the motivation to respond is different in each scenario, all of them present the same context and the same character emailing personal information. For this study, only one scenario was used for factor exploration, revision, and improvement. Based on the situation described in the scenario and current information security literature, several items were formulated to capture the intention to comply with recommendations in terms of handling personal information online, attitudes (evaluation and potency) towards those recommendations, subjective norms regarding
those recommendations, and anticipated regret regarding not following an alternative secure course of action. A total of 36 questions (items) were formulated. The evaluative factor captures the evaluation of information security recommendations in terms of handling personal information online. The potency factor captures the perception of how potent (e.g., hard, constrained, complex) are the information security recommendations. The descriptive normative factor captures the perceptions of other people at work regarding handling personal information. The injunctive normative factor partially departs from the focus on organizational systems (i.e., recommendations) and asks respondents how other people at work would feel with the action performed by the character in the scenario. This change of focus was seen as appropriate given the operational definition of injunctive normative norms (the perception of others relative to the individual performing an action [9]). To reduce a possible impact of social desirability in this measurement, the items were worded in a way that respondents give their perception about what other people think of the action performed by the character in the scenario and not about their own. The items that capture the anticipated regret were based on Buchanan et al. [22]. The items were modified to capture whether respondents have feeling of regret if they would have acted as the person in the character given an alternative option (using secure systems to share personal information). The focus of this construct is also relative to the action. Finally, four items capture the absence of intention to act like the character in the scenario. These items were formulated following Fishbein & Ajzen [9]. This research study received an IRB exemption.

4.1. Participants
Participants were recruited through Amazon Mechanical Turk. Respondents completed the survey in exchange for payment. Effectively, 50 respondents participated in the scenario realism check, 80 respondents in the first pilot study and 80 in the second. For the main data collection, a total of 400 respondents attempted to submit the survey. After discarding responses that fail attention, memory, or participation check (unemployed, or people that do not used an organizational email account), 139 males and 56 females ages 18 to 74 years old were retained. In terms of education, 4% had a high school degree or less; 6% some college; 5% 2-year degree; 64% 4-year degree; 21% professional degree; and 2% doctorate. In terms of work experience, 4% has less than one year; 38% between 1 and 5 years; 36% between 5 and 10 years; and 22% more than 10 years. In terms of job level, 14% were entry-level; 65% mid-level; and 21% executive level. Finally, in terms of organization size, 4% work in an organization that has between 2 and 10 members; 17% between 11 and 50; 32% between 51 and 100; 32% between 101 and 500; and 14% more than 500. The scale with the most items is the evaluative attitudinal scale with 13 items. For a ratio of 10 responses per variable, 130 respondents will be necessary [23].

4.2. Materials
The scenario presents a text that reads, “Sharing personal information by email is typically not recommended in organizational policy as it could lead to a security incident. Some organizations have systems in place that allow employees to enter and share personal information. However, due to a lack of resources or privacy concerns, it is difficult for organizations to monitor whether employees email personal information or use secure systems.” Then the scenario describes a character that in response to a colleague, proceeds to email personal information. Items were formulated to capture the factors of evaluative attitudes (13 items), potency of attitudes (6 items), and descriptive norms (4 items) scored from (1) Strongly agree to (5) Strongly disagree. Four items were formulated to capture injunctive norms scored from (1) Strongly unfavorable to (5) Strongly favorable. Five items were reworded from Buchanan [22] to capture anticipated regret scored from (1) Strongly agree to (5) Strongly disagree. Finally, four items were formulated to capture the intention construct scored from (1) Strongly agree to (5) Strongly disagree. The social desirability scale [24] has five items scored from (1) Definitely true to (5) Definitely false. All items were 5-point Likert.

4.3. Procedure
In the realism check, 50 participants were asked to rate the realism of the scenarios on a 4-points scale from (1) Realistic to (4) Unrealistic. The realism means for the scenarios ranged from 1.68 to 2.1. To those respondents that saw a scenario as unrealistic, the survey asked how the scenario could be improved. All the suggestions were incorporated in further versions. After the realism check, only the four most realistic scenario were kept. Only one scenario was used to test the items that capture the factors in this study.

The pilot questionnaires were administered via Qualtrics. First, the initial item pool went through several rounds of revisions. The item pool and factor operational definitions were presented to respondents and were asked to match the items with the factors using their own judgment. After including some of their suggestions, the item pool was
administered to a reduced sample of 80 respondents to test for wording issues, survey structure, or any other issues. A factor analysis of this data gave preliminary evidence of internal structure, although two items required further rewording as they had a poor factor loading (<0.3). After item improvements, a second sample was taken with 80 different participants. The analysis was repeated and after rewording some problematic items, the study collected a final sample of 200 respondents. The developed scale was administered with an additional social desirability scale [24]. Correlations between social desirability and each of the items (variables) were examined. There was no evidence of social desirability.

4.4. Analysis

4.4.1. Data checking
The study used the software RStudio and the library psych for all analyses. There was no missing data in the main data collection. The data were screened for outliers. According to the Mahalanobis distance cutoff of 67.98, 17 respondents were above this value and were recoded as missing data leaving 179 valid respondents giving a ratio of 13 cases per variable. The assumptions of multivariate normality, linearity, and homogeneity were tested, and there was no evidence of strong non-normality.

4.4.2. Factor Analysis
An exploratory factor analysis was used to explore the factor structure of the 36 items. Factors were extracted using principal axis components and rotated using an Oblimin rotation that allows rotated factor to correlate. First, six factors were extracted based on the theoretical framework that supports this study. The items that capture the potency factor of attitudes and anticipated regret load into one factor. Therefore, the extraction was repeated with seven factors. The seven-factor solution, which explained 63% of the variance, was preferred at this instance because, the ‘leveling off’ of eigenvalues on the screen plot after seven factors, and an insufficient number of primary loadings after the seven-factor solution. The eigenvalues indicate that the first 7 factors explained 15%, 10%, 9%, 8%, 10%, 8%, and 5% of the variance. A total of 10 items were eliminated as they had factor loadings less than 0.3. The final exploratory factor analysis explored the remaining 26 items and extracted six factors that explained 65% of the variance. Each item uniquely loaded into one factor above 0.5. All items load low moderate or low with the social desirability composite score. Internal consistency for each of the scales was examined using Cronbach’s alpha.

5. Results
Based on principal axis components as a method of extraction and Oblimin rotation, a 6-factor structure for 26 out of the 36 items was found. The solution fitted the theoretical factors proposed in this study. The factors are: 1) Attitudinal evaluative factor of organizational recommendations in terms of handling information online (6 items, alpha of 0.86); 2) Injunctive norms towards non-compliance with organizational recommendations in terms of handling information online, (4 items, alpha 0.92); 3) Attitudinal potency factor of organizational recommendations in terms of handling information online (4 items, alpha of 0.92); 4) Intention of complying with organizational recommendation towards handling personal information online (4 items, alpha of 0.88); 5) anticipated regret towards noncompliance (5 items, alpha of 0.87); and 6) Descriptive norms towards complying with recommendations in terms of handling personal information online (3 items, alpha of 0.82). The final factor loadings are presented in Table 1.

6. Conclusions
These preliminary results provide evidence of a clear 6-factor structure with strong internal consistency. Also, social desirability does not appear to be an issue. However, the wording could be improved for further refinement. The dropped items that capture descriptive norms could be reworded to better capture the construct. The study revealed the legitimacy of organization recommendations regarding factors that capture attitudes and subjective norms. However, items for potency of attitudes could be reworded to capture deterrence, an important precursor of non-compliance in information security research. Finally, the moral aspect of noncompliance was captured through anticipated regret. This is deemed to be appropriate since anticipated regret overlaps with moral norms [25]. However, other items that explicitly capture the moral dimension of non-compliance could be included in future factor explorations.

The preliminary evidence presented in this paper suggests that the way other people behave at work and how they would evaluate an act of non-compliance is more relevant to deter non-compliance than the general evaluation of information security recommendations. The results also suggest that regret could be an important factor to prevent acts of non-compliance. Another interesting preliminary result suggests that the evaluation of severity is an important
deterrent to non-compliance, aligned with the findings in the information security literature. The scale developed in the study provides preliminary evidence of the factor structure of security (non)compliance in organizations. After confirming the factor structure and expanding it to other similar scenarios, the scale can be used in future research designs. Other actions that contravene recommendations at work could be included, and the same scales can be used to test other model configurations, especially regarding the moderator effect of attitudes and subjective norms.

Table 1: Factor correlation matrix.
N=179. Oblimin rotation, principal (axis) factor as a method of extraction.

<table>
<thead>
<tr>
<th>PA3</th>
<th>PA2</th>
<th>PA5</th>
<th>PA4</th>
<th>PA1</th>
<th>PA6</th>
<th>Factor labels</th>
<th>Nr. of items</th>
<th>M (SD)</th>
<th>Cronbach’s alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Attitudinal potency factor</td>
<td>4</td>
<td>2.10  (0.93)</td>
<td>0.92</td>
</tr>
<tr>
<td></td>
<td>-0.41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Injunctive norms</td>
<td>4</td>
<td>3.01  (1.22)</td>
<td>0.92</td>
</tr>
<tr>
<td>0.13</td>
<td></td>
<td>0.13</td>
<td></td>
<td>1</td>
<td></td>
<td>Anticipated regret</td>
<td>5</td>
<td>1.70  (0.93)</td>
<td>0.87</td>
</tr>
<tr>
<td>0.02</td>
<td>0.31</td>
<td>0.49</td>
<td>1</td>
<td></td>
<td></td>
<td>Intention to comply</td>
<td>4</td>
<td>1.80  (0.77)</td>
<td>0.88</td>
</tr>
<tr>
<td>0.41</td>
<td>-0.06</td>
<td>0.44</td>
<td>0.23</td>
<td>1</td>
<td></td>
<td>Attitudinal evaluative factor</td>
<td>6</td>
<td>1.81  (0.63)</td>
<td>0.86</td>
</tr>
<tr>
<td>0.37</td>
<td>-0.1</td>
<td>0.4</td>
<td>0.18</td>
<td>0.52</td>
<td>1</td>
<td>Descriptive norms</td>
<td>3</td>
<td>1.80  (0.63)</td>
<td>0.82</td>
</tr>
</tbody>
</table>

Acknowledgments
This work was supported in part by the Coastal Virginia Center for Cyber Innovation and the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about COVA CCI and CCI, visit www.covacci.org and www.cyberinitiative.org.
This work was also supported in part by the Fulbright program (USA) and the Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Ecuador).

References