Association for Information Systems
AIS Electronic Library (AISeL)

GlobDev 2017

Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development

12-10-2017

Exploring the Impacts of Individual Styles on Security Compliance Behavior: A Preliminary Analysis

Charlette Donalds
The University of the West Indies, charlette.donalds02@uwimona.edu.jm

Kweku-Muata Osei-Bryson
Virginia Commonwealth University, KMOsei@vcu.edu

Exploring the Impacts of Individual Styles on Security Compliance Behavior: A Preliminary Analysis

Charlette Donalds
University of the West Indies at Mona, Jamaica
Charlette.Donalds02@UWIMona.Edu.JM

Kweku-Muata Osei-Bryson
Virginia Commonwealth University, USA
KMOsei@VCU.Edu

ABSTRACT: It is well known that while there is a strong correlation between adoption of ICTs and economic growth there is also a corresponding strong correlation between the adoption of ICTs and increased ICT-related technological threats that can have severe economic and other negative consequences. Within this context cybersecurity has become a major issue in both "developed" and "developing" countries, with humans being considered the "weakest link in the chain" of system security. While the cybersecurity literature has previously explored constructs such as awareness and self-efficacy to explain cybersecurity compliance behavior, there has been no exploration of the impacts of individuals' decision styles on cybersecurity related compliance behavior and some other antecedents of such behavior. In this paper we address this issue using an exploratory approach and present a causal model for consideration in future research.

Keywords: Decision Style, Cybersecurity Compliance Behavior, Decision Tree, General Security Orientation, Awareness, Self-efficacy

1. INTRODUCTION

The Jamaican Government (GoJ), in its National Development Plan – Vision 2030 – posits that to achieve one of its national goals, sustainable development, by 2030, among other things, it has to create a technology-enabled society (Planning Institute of Jamaica 2009). The expectation of the GoJ is that increased adoption of technology will boost productivity, efficiency and propel socio-economic growth. This vision is realistic; research in other jurisdictions have demonstrated the correlation between information and communication technology (ICT) adoption and growth in gross domestic product (GDP) per capita (Amiri and Reif 2013; UNCTAD 2006).

However, increased adoption of ICTs is positively correlated with increased technological threats and economic loss. For instance, during a single six month period, January – June 2016, electronic fraud alone costs the Jamaican economy some $500 million (Williams 2016) and the WannaCry ransomware attack in May 2017 affected more than 300,000 victims in over 150 countries (McAfee Labs 2017), negatively impacting citizens and disrupting business operations around the globe. To cope with these technological or cybersecurity threats, security stakeholders have: i) implemented technology-based protection solutions; and ii) conducted cybersecurity awareness activities for users, recognizing that users' are a key threat to achieving security because they often fail to adhere to the security best practices. Humans are often considered the "weakest link in the chain" of system security (Sasse and Flechais 2005; Warkentin and Willison 2009).

To improve users' security compliance behavior, the literature emphasizes the need for managers and practitioners to focus on awareness initiatives (D'Arcy et al. 2009; Herath and Rao 2009; Puhakainen and Siponen 2010). The idea is that awareness mechanisms such as posters, bulletins and newsletters can act as reminders to users to take appropriate security-related actions. However there is a scarcity of empirical studies that examine the direct link between security awareness and users' compliance behavior. Stanton (2005) reported that through increased awareness measures, users changed passwords more frequently and chose better passwords. Too, Bulgurcu et al. (2010) provide empirical evidence that general security awareness *(GSAW)* exerts significant influence on a user's attitude toward compliance. Donalds (2015) also provides empirical support for the link between security awareness and compliance behaviour. Of note however, is that these studies examined security awareness in different but related contexts. For instance, D'Arcy et al. (2009) examined the role of user awareness in relation to information system (IS) misuse while Herath and Rao (2009) examined the influence of security awareness on employees' compliance with the organization's information security policy (ISP). Bulgurcu et al. (2010) also examined the influence of security awareness on employees' compliance with the organization's ISP, however, security awareness was conceptualized as having two key dimensions: "general security awareness" and "information

policy awareness". Donalds (2015) examined the influence of users' general awareness of cybersecurity threats on compliance behaviour. Even though there is some evidence that the direct link between security awareness and compliance behavior is significant, work in the area is still limited and fragmented. As a result, we wish to examine further the role of general security awareness in shaping users' compliance behavior in the cybersecurity context. Security compliance behavior in the cybersecurity context is hereafter referred to synonymously as cybersecurity compliance behavior.

A construct that has been incorporated, but has gained little attention in the IS domain is general security orientation (*GSOR*). According to Ng et al. (2009), general security orientation is an individual's predisposition and interest concerning practicing computer security and is analogous to general health orientation of the health belief model. General health orientation captures the individual's tendency towards performing healthy behaviors. Since it has been observed that individuals with higher levels of health awareness have exhibited greater levels of healthcare behaviors (Jayanti and Burns 1998), it is reasonable to theorize that individuals with greater predisposition towards computer security should exhibit higher levels of security compliance behavior. While the results of Ng et al's. (2009) study did not find that *GSOR* is a direct predictor of security compliance behavior, it found that perceived severity moderated the effects of *GSOR* on security compliance behaviour. That is, when the perceived severity of a security threat is severe or great, then the individual who has a higher level of predisposition towards security will be more proactive in practicing computer security. These results (no direct but indirect relationship between *GSOR* and compliance behavior) warrant further investigation. In this study we aim to improve our understanding of the influence of *GSOR* on compliance behavior by examining the relationship between *GSOR* and security compliance behavior in the cybersecurity context.

Another factor that has been cited to influence users' behavior is self-efficacy (*SLEF*). *SLEF* is a construct of protection motivation theory and emphasizes an individual's ability or judgment of his or her ability to perform an action (Bandura 1977). More specifically, the theory suggests that increasing individual's *SLEF* can improve their competence in coping with a task. For

instance, in a training course *SLEF* was found to exert a strong influence on individual's performance with computer use (Compeau and Higgins 1995). Recent empirical security studies show that *SLEF* has a significant effect on users' intention to comply with (Bulgurcu et al. 2010; Herath and Rao 2009; Pahnila et al. 2010) as well as their attitude toward security compliance (Herath and Rao 2009). Few other studies have studied the role of *SLEF* on users' compliance behavior (Chan et al. 2005; Ng et al. 2009) and have found the link between *SLEF* and compliance behavior significant. While prior research focused mainly on the effects of *SLEF* on users' intention to comply or general security behavior, this study seeks to examine the influence of *SLEF* on users' self-reported actual cybersecurity compliance behaviour. According to theories such as theory of reasoned action (TRA) (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975) and technology acceptance model (TAM)(Davis 1989), an individual's behavior is driven by their behavioral intentions, that is, actual behavior is mediated by behavioral intention. This study differs from others in that we examine the direct relationship between *SLEF* and actual compliance behavior and not users' intention to comply.

In order to improve the cybersecurity behaviors of users, it is necessary to understand the security behavior of men and women and the differences and/or similarities in their compliance behavior. In general, gender has been shown to have a profound influence on an individual's perceptions, attitudes and performance (Nosek et al. 2002). Studies in the security literature also found that gender is significantly correlated with employees' security compliance intention and behavior. For instance, research shows that females have a higher policy compliance intention than males (Herath and Rao 2009; Ifinedo 2012) and that habitual IS security compliance and personal factors, such as gender, influences employees security behavior (Vance et al. 2012). Too, Anwar et al. (2017) found that females reported lower cybersecurity scores than males. Further, Anwar et al. (2017) reported significant difference between males and females on security self-efficacy; this suggests that men and women have differences in their perceived computer abilities. Consequently, we argue that studying the role that gender plays with respect to cybersecurity compliance behavior of users is warranted.

While the cybersecurity literature has previously explored constructs such as awareness and self-efficacy to explain cybersecurity compliance behavior, there has been no exploration of the impacts of individuals' decision styles on cybersecurity related compliance behavior and some other antecedents of such behavior. In this study we examine such impacts. Cognitive theorists have long argued that decision style is an important determinant of behavior. In fact, several investigations (e.g. Henderson and Nutt 1980; Niu 2013) report that an individual's decisions seem to be a function of the individual's cognitive makeup, which differs for psychological types. The Decision Styles Inventory (DSI) tool (Rowe and Boulgarides 1983; Rowe and Mason 1987), that is adopted in this study, has been used in varying setting to test the relationship between individual decisions styles and behaviour. For instance, Moretti (1994) used the tool to classify volunteers as typical or not typical leaders and found that typical leaders deal better with ambiguity and uncertainty; Jamian et al. (2013) explored how decision styles of deans in institutions of higher education relate to leadership effectiveness. To the best of our knowledge, decision styles have not been investigated in previous security or cybersecurity studies.

In this paper we explore the impacts of individuals' decision styles on their cybersecurity compliance behavior and on other constructs theorized to influence security compliance behavior. Subsequent sections present an overview of individuals' decision styles, the research methodology, results of the interactions of decision styles on behavior and antecedents of behavior, abduction of hypotheses for future testing and conclusion.

2. OVERVIEW ON INDIVIDUAL DECISION STYLES

The Decision Style Inventory (DSI) was developed by Rowe in 1981 and further elaborated by Rowe & Boulgarides (1983) and Rowe & Mason (1987) is a cognitive management tool to understand the type of decisions an individual is likely to make under certain situations. Rowe and Boulgarides (1992) argued that effective decision-makers are the ones whose decision style matches the requirements of the decision situations. Thus, a better understanding about one's likely behavior or decisions can help not only the individuals but their organizations in more

strategic decision-making. Within the context of the decision styles model there are four decision styles (*Directive, Analytical, Conceptual*, and *Behavioral*) each with its own characteristics with regards to level of tolerance for ambiguity, need for structure, people or task orientation and so on (see Table 1).

Table 1: Decision Styles

Style	Description
Analytical	Achievement oriented without the need for external rewards; enjoys problem solving; strong ability to cope with new situations; oriented towards acquiring and utilizing all relevant information; make decisions slowly because of orientation to examine the situation thoroughly and consider many alternatives systematically; prefer information that is given in the form of written reports.
Behavioral	Strong people orientation, driven primarily by a need for affiliation; typically receptive to suggestions, willing to compromise, and prefer loose controls; have short-range focus; comfortable making decisions using limited relevant information; prefer to do their information exchange at meetings.
Conceptual	Achievement and people oriented with the need for external rewards; have long-range focus; make decisions slowly because of orientation to examine the situation thoroughly and consider many alternatives systematically.
Directive	Results and power oriented but have al low tolerance for ambiguity and cognitive complexity; prefer to consider a small number of alternatives based on limited information; prefer structure and information that is given verbally; have short-range focus.

Martinsons and Davison (2007) observed that in different cultures, different individual decision styles are dominant, and that these differences determine the types of decision support system that are most appropriate. For example they noted that in several non-Western societies, decision-makers "focus on collective interests, emphasize relationships and intuition (at the expense of factual analysis), and discourage conflicting views that would threaten group harmony or the face of the individual", with some having "greater acceptance of tacit knowledge management". To paraphrase Martinsons and Davison (2007), for such non-Western societies, Knowledge Management Systems (KMSs) that support interpersonal communications and encourage tacit knowledge sharing and individual discretion would be more helpful than KMSs that mainly involve codified knowledge.

Elicitation of decision styles information is done using a standard DSI questionnaire (Rowe 1981; Rowe and Mason 1987), that consists of 20 multi-response questions. For each question there is a set of 4 response statements, one for each of the four decision styles, and the respondent is required to rank the set of response statements: Most Preferred (8 points), 2nd Most Preferred (4 points), 3rd Most Preferred (2 points), Least Preferred (1 points). This implies that for each question, 15 points have to be distributed across the 4 response statements. Therefore the overall maximum number of points is 300; and overall maximum possible number of points for each decision style is 160 (= 20* 8), with the corresponding minimum being 20 (= 20*1).

$$Score_{Analytical} + Score_{Behavioral} + Score_{Conceptual} + Score_{Directivel} = 300$$

Idea/Action Orientation:

An individual can also be characterized as having a preference for acting (i.e. *Action*-oriented) or thinking (*Idea*-oriented). Given a decision-making task, an *Idea-oriented* individual is predisposed to first engage in deep analysis and synthesis before acting, formulate creative and innovative solutions, and engage in written communication. The *Action-oriented* individual on the other hand is predisposed to focus on the achievement of results, feeling internal pressure to act he/she may engage in inadequate reflection before acting (Rowe and Mason 1987).

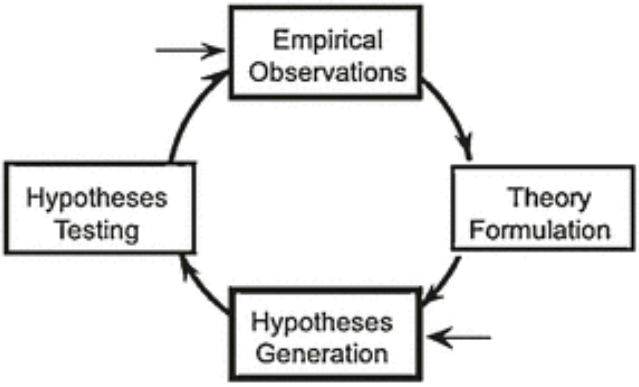
Determination of the Idea/Action *Orientation* of the individual can also be defined in terms of the 4 elementary individual decision styles. An individual would be categorized as being Idea-oriented if his/her combined score for the *Analytical* and *Conceptual* decision styles was at least 170; otherwise the he/she would be characterized as being Action-oriented (combined score for the Behavioral and Directive decision styles was at least 130).

3. RESEARCH METHODOLOGY

For this research we adapted the steps from the methodology presented by Osei-Bryson and Ngwenyama (2011) and included an additional step, “Exploratory Factor Analysis”. In general,

this methodology employs the hypothetico-deductive (H-D) process for theory development, on which positivist IS research is based (see Figure 1). The process can be described as cyclical with theory formulation generally resulting from empirical observations and from formulated theory, hypotheses generation, which are subsequently tested and used to inform empirical observations. According to Osei-Bryson and Ngwenyama (2011), the general limitation of the H-D model is that hypotheses generation are limited by human imagination. Osei-Bryson and Ngwenyama (2011) demonstrate that this limitation can be overcome by incorporating data mining techniques such as decision tree generation. Applying the H-D process to this study, we formulate theory based on empirical observations and then generate hypotheses using decision tree technique, which can then be subjected to testing.

Figure 1: Hypothetico-deductive (H-D) model



The following outlines the steps from the methodology presented by Osei-Bryson and Ngwenyama (2011):

1. Use existing theory to select potential direct and indirect predictor variables for security compliance behavior.
2. Collect relevant data.
3. Conduct exploratory factor analysis.
4. Use decision tree induction technology to do recursive partitioning of the given dataset resulting in rulesets.

5. Abduct hypotheses from the results of the decision tree induction. Sibling rules hypotheses will be generated using the approach presented in Osei-Bryson & Ngwenyama (2011).

3.1 Overview on Decision Tree Induction

A decision tree (DT) is a tree structure representation of the given decision problem such that each non-leaf node is associated with one of the decision variables, each branch from a non-leaf node is associated with a subset of the values of the corresponding decision variable, and each leaf node is associated with a value of the target (or dependent) variable. There are two main types of DTs: 1) classification trees and 2) regression trees. For a classification tree, the target variable takes its values from a discrete domain, and for each leaf node the DT associates a probability for each class (i.e. value of the target variable). A regression tree (RT) is a DT in which the target variable takes its values from a continuous domain (numeric). For each leaf, the RT associates the mean value and the standard deviation of the target variable.

There are two major phases of the RT induction process: the *growth phase* and the *pruning phase* (e.g. Kim and Koehler, 1995). The *growth phase* involves a recursive partitioning of the training data resulting in a RT such that either each leaf node is pure (i.e. all observations have the same value for the target), further partitioning of the given leaf would result in at least one of its child nodes being below some specified threshold, or the split is not statistically significant at a specified level. The *pruning phase* aims to generalize the RT that was generated in the *growth phase* by generating a sub-tree that avoids over-fitting to the training data. The actions of the *pruning phase* is often referred to as *post-pruning* in contrast to the *pre-pruning* that occurs during the *growth phase* and which aims to prevent splits that do not meet certain specified threshold (e.g. minimum number of observations for a leaf).

In order to reduce over-fitting the generated RT to the data that was used to generate it, for large modeling datasets, the original dataset would be divided into mutually exclusive *Training* and *Validation* subsets, where the Training subset is used during the *Growth Phase* to generate the initial RT, and the *Validation* subset would be used during the Post-Pruning phase. For small

modeling datasets, such an approach is not possible so techniques such as k-fold cross validation (e.g. 10-fold) are used where the original model dataset is divided into k mutually exclusive subsets (k-folds), and k runs are done each in involving a unique combination of (k-1) folds.

During the Growth Phase, the given dataset is recursively split into smaller and smaller datasets based on the selected splitting method. A splitting method is the component of the DT induction algorithm that determines both the attribute that is selected for a given node of the DT and also the partitioning of the values of the selected attribute into mutually exclusive subsets such that each subset uniquely applies to one of the branches that emanate from the given node. It is well known that there is no single splitting method that will give the best performance for all datasets. While some datasets are insensitive to the choice of splitting methods, other datasets are very sensitive to the choice of splitting methods. Given that it is never known beforehand which splitting method will lead to the best DT for a given dataset, it is advisable that the data miner explore the effects of different splitting methods (e.g. Variance Reduction, F-Test).

3.2 Sibling Rules Hypotheses

Nodes that share the same parent are considered to be Sibling Nodes (see Figure 2). For each set of Sibling Nodes there is a corresponding set of Sibling Rules and an associated discriminating variable (e.g. *DominantOrientation*). *Sibling Rules Hypotheses* are formed based on the discriminating variable associated with a given set of Sibling Rules, and its test worthiness is evaluated by applying traditional statistical hypothesis testing to the statistics of the target variables that are associated with pairs of Sibling Nodes (Osei-Bryson and Ngwenyama 2011; Osei-Bryson and Ngwenyama 2014).

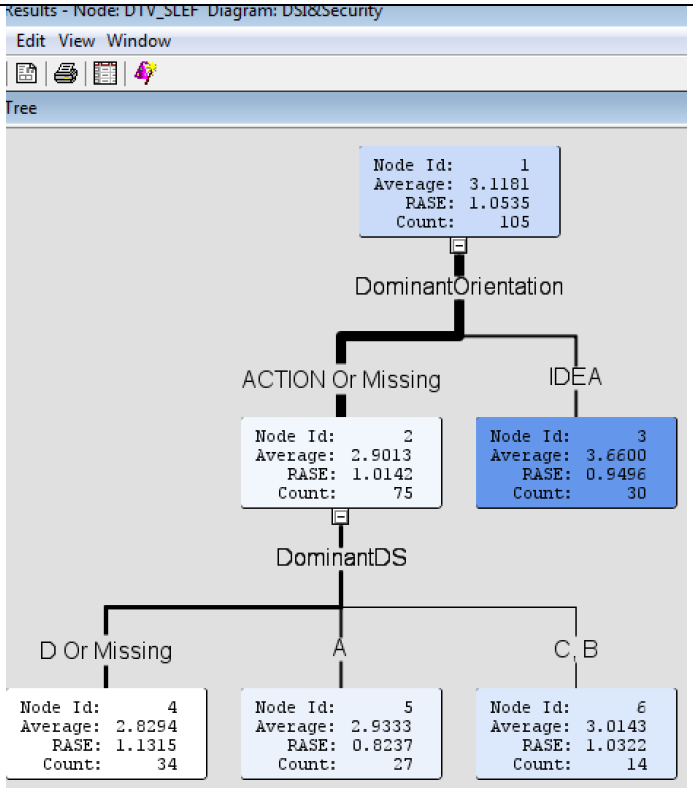
For example given the pair of Sibling Rules that are associated with Nodes 2 and 3 the following hypotheses and its alternative hypothesis would be formed and its test worthiness evaluated.

H_O: The difference in the mean value of the target variable that is associated with *Orientation* = '*Action*' from that associated with *Orientation* = '*Idea*' is not statistically significant.

H_A: The difference in the mean value of the target variable that is associated with *Orientation* = '*Action*' from that associated with *Orientation* = '*Idea*' is statistically significant.

Figure 2. Examples of Sibling Nodes & Sibling Rules

- Node 2 & Node 3 are child nodes of Node 1 so are Sibling Nodes with *DominantOrientation* being the discriminating variable.
  The corresponding Sibling Rules are:
  - **IF** *DominantOrientation* = '*Action*' **THEN** the target variable has an Average value of 2.9013 & StdDev of 1.0142
  - **IF** *DominantOrientation* = '*Idea*' **THEN** the target variable has an Average value of 3.6600 with StdDev of 0.9496
- Nodes 4, 5 & 6 are child nodes of Node 2 so are Sibling Nodes with *DominantDS* being the discriminating variable



In this case its test worthiness would be evaluated using a difference of means statistical test since the target variable has the interval data type; if the target variable had a discrete data type then its test worthiness would be evaluated using a difference of proportions statistical test. If the *p-value* is below the specified level of significance then the hypothesis H_O is rejected and its alternative hypothesis H_A is not rejected. For this example the corresponding *p-value* is 0.0006, and so H_O is rejected and its alternative hypothesis H_A is not rejected. Since there is only

a single pair of Sibling Rules then there is need to evaluate only a single null hypotheses and since it H_O is rejected then the *Sibling Rules Hypothesis* is formed based on H_A:

Orientation has a statistically significant impact on the given target variable.

In general, if the parent node has more than 2 child nodes then multiple (H_O, H_A) pairs would need to be evaluated, as demonstrated in section 4.

4. APPLICATION OF THE RESEARCH METHODOLOGY

Step 1: Selection of Potential Predictor Variables

Table 2. List of Constructs – Dependent Variable & Potential Predictors

Construct	Factor Label	Items	Reference
Password Compliance Behavior	PWDC	**CMPB1** – I use different passwords for my different online accounts (e.g., online banking/shopping, Facebook, email).	Anwar et al. (2017)
		CMPB2 – I have changed the passwords to access my different online accounts (e.g., online banking/shopping, Facebook, email) during the past 12 months.	Special Eurobarometer 390 (2012)
Security Compliance Behavior	SECC	**CMPB5** – I never usually send sensitive information (such as account numbers, passwords, and ID numbers via email or using social media.	Anwar et al. (2017)
		CMPB6 – Concerns about security issues made me visit only websites I know/trust or click on URLs if I know where the URLs will really take me.	Anwar et al. (2017); Special Eurobarometer 390 (2012)
		CMPB7 – Concerns about security issues made me not open emails from people I don't know and/or only use my own computer.	Special Eurobarometer 390 (2012)
General Security Awareness	GSAW	**GSAW1** – Overall, I am aware of potential information/cyber security threats and their negative consequences.	Bulgurcu et al. (2010)
		GSAW2 – I understand the concerns regarding information/cyber security threats and the risks they pose in general.	Bulgurcu et al. (2010)
		GSAW2 – I have sufficient knowledge about the cost of potential information/cyber security threats.	Bulgurcu et al. (2010)
General Security	GSOR	**GSOR1** – I read information/cyber security bulletins or newsletters.	Ng et al. (2009)

Construct	Factor Label	Items	Reference
Orientation		**GSOR2** – I am concerned about information/cyber security incidents and try to take actions to prevent them.	Ng et al. (2009)
		GSOR3 – I am usually mindful about computer security.	Ng et al. (2009)
Self-Efficacy	SLEF	**SLEF2** – I feel confident updating security patches to the operating system.	Rhee et al. (2009); Anwar et al. (2017);
		SLEF3 – I feel confident setting the Web browser to different security levels.	Rhee et al. (2009); Anwar et al. (2017);
		SLEF4 – I feel confident using different programs to protect my information and information system.	Rhee et al. (2009)
		SLEF5 – I feel confident handling virus infected files and/or getting rid of malware/spyware.	Rhee et al. (2009); Anwar et al. (2017);
		SLEF6 – I feel confident learning the method to protect my information and information system.	Rhee et al. (2009)

Step 2: Data Collection

We collected data via a web-based survey, which was pre-tested by faculty members, graduate students as well as some IS security experts, all from Jamaica. Based on feedback, several items were reviewed and modified. The survey instrument was then used to collect data from faculty members, undergraduate and graduate students in an institution of higher learning and from employed individuals across industries in Jamaica. In order to elicit participation, the survey link was sent to all members in one faculty and students of several undergraduate and graduate courses. Additionally, participants were asked to forward the survey link to potential participants known to them. This type of technique wherein people make referrals to identify other participants is referred to as "snowball sampling". Because the snowball sampling technique was incorporated to elicit participation, it is difficult to establish the sample frame for the study. Nonetheless, the link was directly advertised to approximately 370 individuals, of which 105 responses were received. Without considering referrals, this yields a response rate of 28%. Of the 105 participants in the survey, 56 percent were females and 44 percent males. Too, respondents of the survey were from varying industries, such as: education, banking and financial services, telecommunications/IT and the security services.

Step 3: Exploratory Factor Analysis

From the exploratory factor analysis of the four potential predictor and determinant variables (security compliance behavior, security awareness, general security orientation and security self-efficacy), five factors emerged to explain the maximum portion of the variance in the original variables (see Tables 3 and 4). That is, five factors explained approximately 65 percent of variance in the original variables (see Table 3). Table 4 identifies the five factors. Of note, the items of the original security compliance behavior variable loaded unto two factors: components 3 and 4. Based on the items, the two factors are now identified as "Security Compliance Behavior" (*SECC*) and "Password Compliance Behavior" (*PWDC*) (see Table 2).

Factors can be identified by the factors loadings. That is, to interpret factors, the factor loadings are examined to determine the strength of the relationships or explain the variance explained by the items on that particular factor. One widely utilized approach is to keep items with high factor loadings and discard low ones. As a rule of thumb, items with factor loadings of 0.6 or higher can be retained for exploratory studies (Matsunaga 2010; Nunally 1967). Due mostly to low factor loadings as well as cross loadings, three items (CMPB3, CMPB4, CMPB8) were removed (see Table 4).

Table 3: Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	**Total**	**% of Variance**	**Cumulative %**	**Total**	**% of Variance**	**Cumulative %**
1	7.07	35.34	35.34	7.07	35.34	35.34
2	1.93	9.64	44.98	1.93	9.64	44.98
3	1.5	7.52	52.5	1.5	7.52	52.5
4	1.32	6.58	59.07	1.32	6.58	59.07
5	1.18	5.91	64.98	1.18	5.91	64.98
6	1.09	5.46	70.44	1.09	5.46	70.44
7	0.86	4.31	74.75			
8	0.74	3.69	78.44			
9	0.65	3.27	81.72			
10	0.58	2.89	84.6			
11	0.51	2.53	87.13			
12	0.48	2.39	89.52			
13	0.41	2.04	91.56			

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
14	0.38	1.88	93.44			
15	0.28	1.38	94.82			
16	0.26	1.3	96.13			
17	0.25	1.24	97.37			
18	0.22	1.08	98.46			
19	0.18	0.91	99.36			
20	0.13	0.64	100			

Table 4: Rotated Component Matrix

	Component					
Item	*1*	*2*	*3*	*4*	*5*	*6*
CMPB1	0.17	0.11	0.79	0.11	0.18	0.01
CMPB2	0.01	0.09	0.85	0.05	0.01	0.01
CMPB5	0.07	0.12	0.25	0.66	-0.31	0.07
CMPB6	0.15	-0.04	0.2	0.71	0.32	-0.01
CMPB7	0.02	0.25	-0.13	0.78	0.15	0.02
GSAW1	0.15	0.86	0.02	0.16	0.13	0.02
GSAW2	0.16	0.87	0.16	0.16	0.07	-0.01
GSAW3	0.29	0.6	0.18	-0.02	0.36	-0.01
GSOR1	0.33	0.06	0.07	0.01	0.77	-0.02
GSOR2	0.23	0.2	0.09	0.07	0.74	0.06
GSOR3	0.21	0.37	0.19	0.25	0.65	0.21
SLEF1	0.44	0.3	-0.12	0.31	0.33	0.04
SLEF2	0.89	0.06	0.09	0.06	0.1	-0.02
SLEF3	0.88	0.1	0.05	0.04	0.24	0.02
SLEF4	0.81	0.18	0.14	0	0.24	0.05
SLEF5	0.78	0.17	0.04	0.06	0.1	0.16
SLEF6	0.62	0.2	0.11	0.25	0.24	0.24
CMPB3	0.45	0.17	0.44	0.05	0.19	0.45
CMPB4	0.32	0.19	0.17	0.19	0.32	0.62
CMPB8	-0.01	0.11	0.07	0.05	0.06	-0.85

Step 4: Decision Tree Induction

To generate a DT from a given dataset, a single variable must be identified as the target (or dependent) variable and the potential predictors must be identified as the input variables.

Commercial data mining software (e.g. C5.0, SAS Enterprise Miner, IBM Intelligent Miner) provide facilities that make the generation of DTs a relatively easy task. In our case the SAS Enterprise Miner data mining software was applied to this dataset, resulting in the RTs that are displayed in Figures 3 - 7. Since our dataset is small we used 10-fold cross validation. We set the maximum number of splits per node to 4; the minimum number of observations associated with a rule to 10; and since our dataset is small, we such as k-fold cross validation with k= 3.

4.1 Impact Decision Styles and Orientation on GSOR:

This DT provides evidence that the individual's dominant Decision Style (i.e. DominantDS) may have a statistically significant impact on his/her general security orientation (*GSOR*) at the 5% level of significance since at least one of the corresponding pairs of (H_o, H_A) hypotheses has a H_A that is "accepted" (see Table 5).

Figure 3. DT with GSOR as the Target Variable

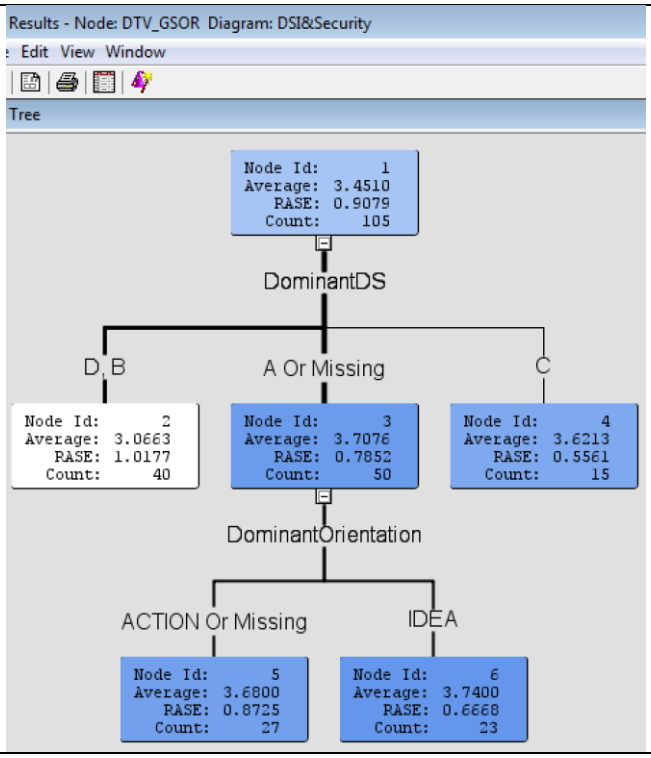
Potential Predictors	Resulting DT
○ DominantDS ○ DominantOrientation ○ Gender	

Table 5. Evaluation of (H_O, H_A) pairs associated with DT where GSOR is the Target Variable

Pair	Null Hypothesis H_O	p-value	Accept H_A
1	H_O: The difference in the mean value of GSOR that is associated with DominantDS = 'A' from that associated with DominantDS = 'B' or 'D' is not statistically significant.	0.0011	Yes
2	H_O: The difference in the mean value of GSOR that is associated with DominantDS = 'C' from that associated with DominantDS = 'B' or 'D' is not statistically significant.	0.0511	No

4.2 Impact of Decision Styles and Orientation on *GSAW*:

This DT provides evidence that the individual's dominant *Decision Style* (i.e. *DominantDS*) may have a statistically significant impact on his/her general security awareness (*GSAW*) at the 5% level of significance since at least one of the corresponding pairs of (H_o, H_A) hypotheses has a H_A that is "accepted" (see Table 6).

Figure 4. DT with GSAW as Target Variable

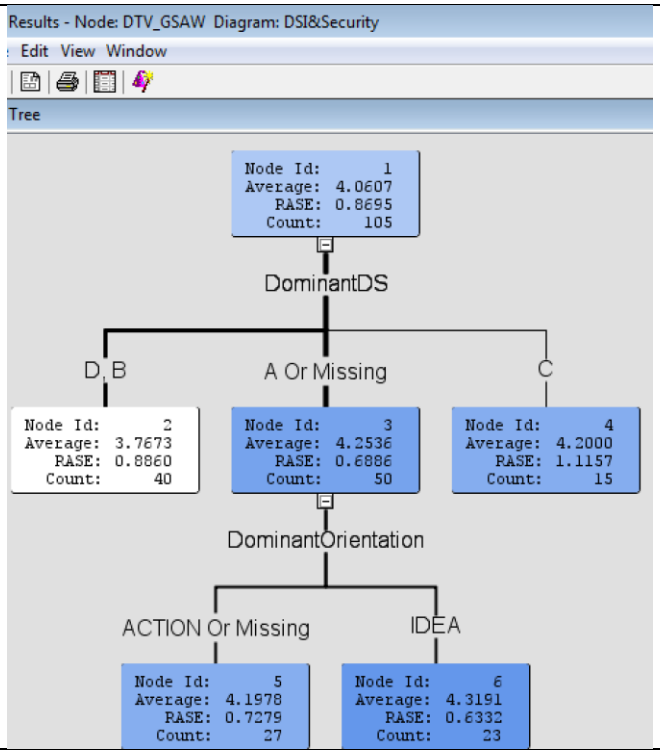
Potential Predictors	Resulting DT
○ DominantDS ○ DominantOrientation ○ Gender	

Table 6. Evaluation of (H_O, H_A) pairs associated with DT where GSAW is the Target Variable

Pair	Null Hypothesis H_O	p-value	Accept H_A
1	H_O: The difference in the mean value of *GSAW* that is associated with DominantDS = 'A' from that associated with DominantDS = 'B' or 'D' is not statistically significant.	0.0043	Yes
2	H_O: The difference in the mean value of *GSAW* that is associated with DominantDS = 'C' from that associated with DominantDS = 'B' or 'D' is not statistically significant.	0.1393	No

4.3 Impact of Decision Styles and Orientation on SLEF:

This DT provides evidence that: The individual's dominant Idea/Action Orientation (i.e. DominantOrientation) may have a statistically significant impact on his/her self-efficacy (*SLEF*) at the 5% level of significance since its corresponding (H_o, H_A) pair of hypotheses has a H_A that is "accepted" (see Table 7).

Figure 5. DT with SLEF as Target Variable

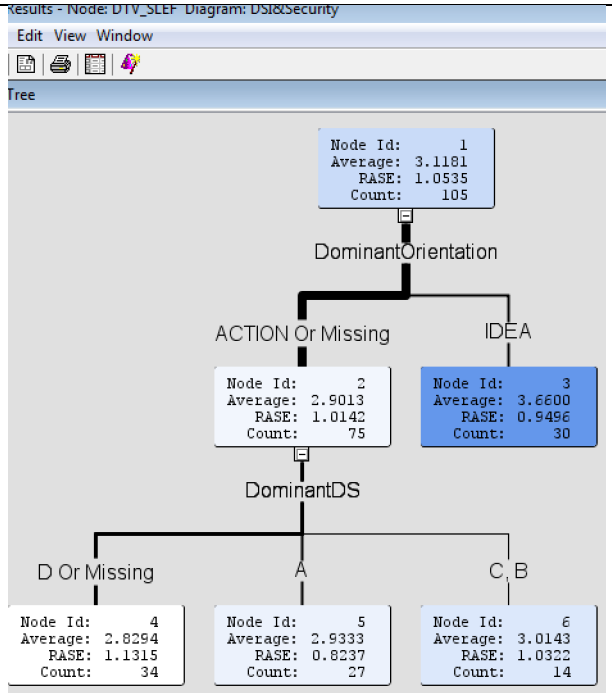
Potential Predictors	Resulting DT
○ DominantDS ○ DominantOrientation ○ Gender	

Table 7. Evaluation of (H_O, H_A) pairs associated with DT where SLEF is the Target Variable

Pair	Null Hypothesis H_O	p-value	Accept H_A
3.1	H_O: The difference in the mean value of *SLEF* that is associated with *DominantOrientation* = 'Action' from that associated with *DominantOrientation* = '*Idea*' is not statistically significant.	0.0006	Yes

4.4 Impact of Decision Styles and Orientation on *SECC*:

The resulting DT displayed below provides evidence that the individual's dominant Decision Style (i.e. DominantDS) may have a statistically significant impact on his/her security compliance behavior (*SECC*) at the 5% level of significance since its corresponding (H_o, H_A) pair of hypotheses has a H_A that is "accepted" (see Table 8).

Figure 6. DT with SECC as Target Variable

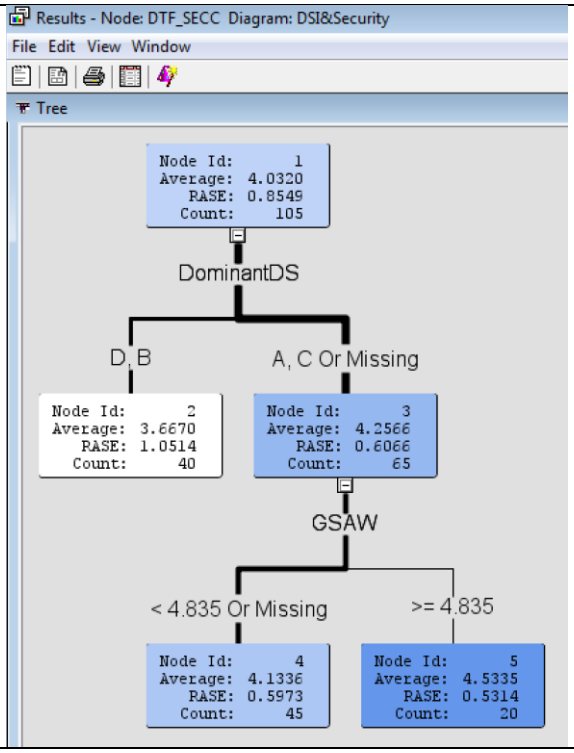
Input Potential Predictor Variables	Resulting DT
○ SLEF ○ GSOR ○ GSAW ○ DominantDS ○ DominantOrientation ○ Gender	

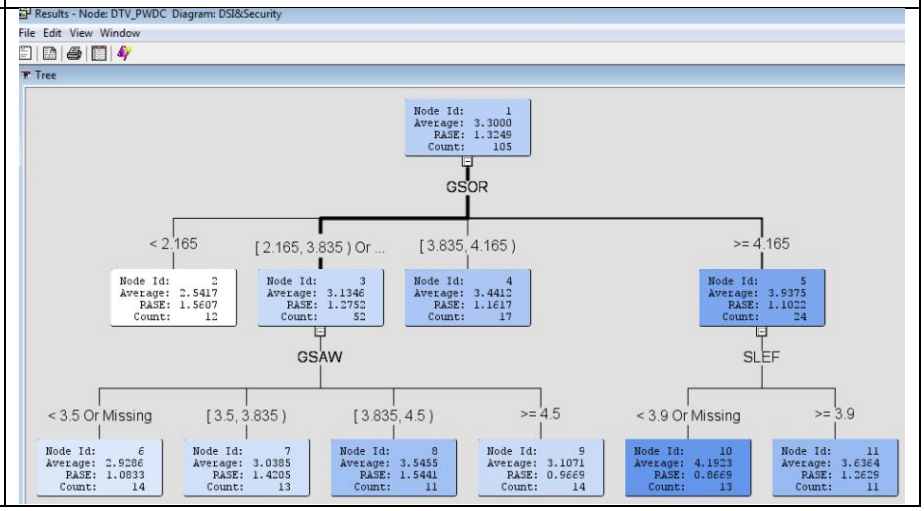
Table 8. Evaluation of (H_O, H_A) pair associated with DT where SECC is the Target Variable

Pair	Null Hypothesis H_O	p-value	Accept H_A
4.1	H_O: The difference in the mean value of *SECC* that is associated with DominantDS = ('A' or 'C') from that associated with DominantDS = ('B' or 'D') is not statistically significant.	0.0004	Yes

4.5 Impact of Decision Styles and Orientation on *PWDC*:

The resulting DT does not include *DominantDS* or *DominantOrientation* in its rules and does not provide evidence that either variable has a statistically significant impact on his/her password compliance behavior (*PWDC*).

Figure 7. DT with PWDC as Target Variable

Potential Predictors	Resulting DT
○ SLEF ○ GSOR ○ GSAW ○ DominantDS ○ DominantOrientation ○ Gender	

Step 5: Abduction of Hypotheses

Given the alternative hypotheses (i.e. H_As) that were accepted in Step 4, the following hypotheses can be abducted:

Table 9: Abducted Hypotheses

Hypothesis	Justification	
	Test Worthiness	Informed Argument
DominantDS $\Rightarrow$ *GSOR*	p-value = 0.0011	Since some decision styles (DS) give more emphasis to the use of data in decision-making then security issues

		such as data integrity, availability and confidentiality may be of greater concern to individuals with those DSs.
DominantDS ⇒ *GSAW*	p-value = 0.0043	Similar to the above.
DominantOrientation ⇒ *SLEF*	p-value = 0.0006	*SLEF* emphasizes an individual's ability or judgment of his or her ability to perform an action (Bandura 1977). Given characteristics of *Idea*-orientation vs *Action* –orientation it seems reasonable that *DominantDS* impacts *SLEF*.
DominantDS ⇒ *SECC*	p-value = 0.0004	DS is a predictor of decision behavior and action (Rowe and Boulgarides, 1992)

Kositanurit et al. (2011) proposed a hybrid process for empirically based theory development that is described in Table 10 below. Given the abducted hypotheses displayed in Table 9 and hypotheses proposed in other previous research, Table 11 displays a set of relevant causal links (i.e. hypotheses) along with their justifications, of a new extended model that could be empirically tested in future search. Further, figure 8 provides the new research model that has emerged from our analyses and which can be subjected to empirical testing.

Table 10. Model of Process for Empirically based Theory Development

Ideal Model of Scientific Inquiry		**Hybrid Process for Empirically based Theory Development**
Phase	**Description**	
Empirical Observation	Observer (gather data about) some phenomena of interest.	1a: Use existing theory to identify variables that are likely to be relevant to the phenomena of interest.
		1b: Based on *Substep 1a* above, gather data related to the phenomena of interest.
Hypothesis Generation	Using these observations (data) invent one or more hypotheses that might explain the phenomena.	2a: Use data mining approach to do automatic generation & preliminary testing of hypotheses
		2b: Based on the results of *Substep 2a*, generate a preliminary model that appears to explain the phenomena of interest.
		2c: The researcher examines & of necessary revised the preliminary model that was generated in *Substep 2b*. This revision may be based on the researcher's knowledge of existing theory.

Design of Experiments	Using the hypotheses, design an experiment to test the logical consequences of the hypotheses.	3: Design an experiment to test the logical consequences of the hypotheses.
		Conventional data analysis approaches may be included in the experimental design.
Empirical Testing	Having designed the experiment, collect observations about the phenomena and examine them to see if the predictions prove to be true or false.	4a: Collect observations about the phenomena.
		4b: Conduct measurement validity.
		4c: Determine if hypotheses of the current model are supported based on data analysis of the given dataset
		This phase should be repeated since no amount of testing can ever guarantee the truth value of a theory about phenomena but only gradually increasing confirmation of the theory.

Figure 8. Future Research Model

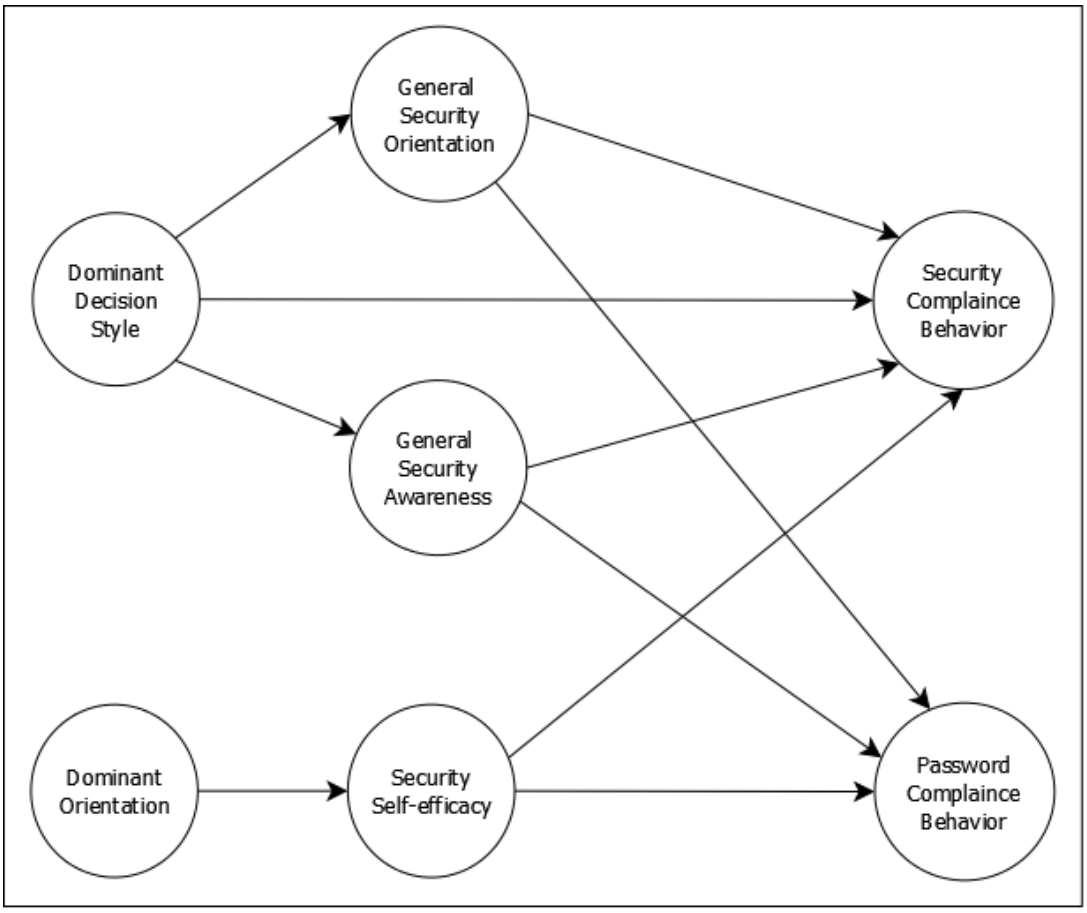


Table 11. Hypotheses of Extended Model

Causal Link	Justification
DominantDS ⇒ GSOR	Abducted in this study
DominantDS ⇒ GSAW	Abducted in this study
DominantOrientation ⇒ SLEF	Abducted in this study
DominantDS ⇒ SECC	Abducted in this study
SLEF ⇒ SECC	Chan et al. (2005); Ng et al. (2009)
GSOR ⇒ SECC	Ng et al. (2009); (Jayanti and Burns 1998)
GSAW ⇒ SECC	Stanton (2005); Bulgurcu et al. (2010); Donalds (2015)
SLEF ⇒ PWDC	Chan et al. (2005); Ng et al. (2009)
GSOR ⇒ PWDC	Ng et al. (2009); (Jayanti and Burns 1998)
GSAW ⇒ PWDC	Bulgurcu et al. (2010); Donalds (2015)

5. CONCLUSION

It is the hope of the GoJ that the continued adoption if ICTs, among other things, will lead to sustainable economic growth. While this vision can be realized, there is a direct correlation between ICT adoption and cybersecurity threats. Additionally, since individuals are considered the "weakest link in the chain" of IS security, it is an imperative of the GoJ and other organizations to identify factors that can positively influence users' security compliance behavior.

The purpose of this paper is to identify factors that influence users' security compliance behavior. We accomplish this by: i) considering the effects that decision styles may have on security compliance behavior; and ii) employing the H-D process for theory development. Specifically, we used a data mining based exploratory data analysis approach to abduct some new hypotheses. For future research, one possible direction is to empirically validate these constructs and abducted relationships. By identifying and understanding the determinants of users' security compliance behavior, interventions can be designed to change behavior by directing same at one or more of the determinants.

REFERENCES

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behaviour*. Englewood Cliffs, New Jersey: Prentice-Hall Inc.

Amiri, S., and Reif, B. 2013. "Internet Penetration and Its Correlation to Gross Domestic Product: An Analysis of the Nordic Countries," *International Journal of Business, Humanities and Technology* (3:2).

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. 2017. "Gender Difference and Employees' Cybersecurity Behaviors," *Computers in Human Behavior* (69:C), pp. 437-443.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behaviour Change," *Psychological Review* (84:2), pp. 191-215.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security* (1:3), pp. 18-41.

Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 318-340.

Donalds, C. 2015. "Cybersecurity Policy Compliance: An Empirical Study of Jamaican Government Agencies," in: *SIG GlobDev Pre-ECIS Workshop*. Munster, Germany.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Henderson, J. C., and Nutt, P. C. 1980. "The Influence of Decision Style on Decision Making Behavior," *Management Science* (26:4), pp. 371-386.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18), pp. 106–125.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Jamian, L. S., Sidhu, G. K., and Parmjit, S. A. 2013. "Managerial Decision Styles of Deans in Institutions of Higher Learning," *Procedia - Social and Behavioral Sciences* (90), pp. 278 – 287.

Jayanti, R. K., and Burns, A. C. 1998. "The Antecedents of Preventive Health Care Behavior: An Empirical Study," *Academy of Marketing Science Journal* (26:1).

Kositanurit, B., Osei-Bryson, K.-M., and Ngwenyama, O. 2011. "Re-Examining Information Systems User Performance," *Expert Syst. Appl.* (38:6), pp. 7041-7050.

Martinsons, M. G., and Davison, R. M. 2007. "Strategic Decision Making and Support Systems: Comparing American, Japanese and Chinese Management," *Decision Support Systems* (43:1), pp. 284-300.

Matsunaga, M. 2010. "How to Factor-Analyze Your Data Right: Do's, Don'ts, and How-To's," *International Journal of Psychological Research* (3:1), pp. 97-110.

McAfee Labs. 2017. "Mcafee Labs Threat Report, September 2017," 3525_0917_rp-threats-sept, pp. 1-66.

Moretti, R. J. 1994. "Executive Level Decision Styles and Learning Strategies of Volunteer Leaders." Montana State University, p. 131.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

Niu, H.-J. 2013. "Cyber Peers' Influence for Adolescent Consumer in Decision-Making Styles and Online Purchasing Behavior," *Journal of Applied Psychology* (43:6), pp. 1228–1237.

Nosek, B. A., Banaji, M. R., and Greenwald, A. G. 2002. "Harvesting Implicit Group Attitudes and Beliefs from a Demonstration Web Site," *Group Dynamics: Theory, Research, and Practice* (6:1), pp. 101-115.

Nunally, J. C. 1967. *Psychometric Theory*. New York: McGraw-Hill.

Osei-Bryson, K.-M., and Ngwenyama, O. K. 2011. "Using Decision Tree Modeling to Support Piercian Abduction in Is Research: A Systematic Approach for Generating and Evaluating Hypotheses for Systematic Theory Development," *Information Systems Journal* (21:5), pp. 407-440.

Osei-Bryson, K.-M., and Ngwenyama, O. K. 2014. *Advances in Research Methods for Information Systems Research: Data Mining, Data Envelopment Analysis, Value Focused Thinking*. Boston, MA: Springer.

Pahnila, S., Mahmood, M. A., and Siponen, M. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64-71.

Planning Institute of Jamaica. 2009. "Vision 2030 Jamaica: National Development Plan." Jamaica: Planning Institute of Jamaica, p. 412.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.

Rhee, H.-S., Kim, C., and Ryu, Y. U. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Compters & Security* (28:8), pp. 816-826.

Rowe, A. J. 1981. "Decision Style Inventory."

Rowe, A. J., and Boulgarides, J. D. 1983. "Decision Styles—a Perspective," *Leadership & Organization Development Journal* (4:4), pp. 3-9.

Rowe, A. J., and Boulgarides, J. D. 1992. *Managerial Decision Making: A Guide to Successful Business Decisions* New York, USA: McMillan.

Rowe, A. J., and Mason, R. O. 1987. *Managing with Style: A Guide to Understanding Assessing, and Improving Decision Making*. San Francisco, CA: Jossey-Bass.

Sasse, M. A., and Flechais, I. (eds.). 2005. *Usable Security: Why Do We Need It? How Do We Get It?* Sebastopol, US: O'Reilly.

Special Eurobarometer 390. 2012. "Cyber Security," S1058_77_2_EBS390, European Commission, p. 129.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24:2), pp. 124-133.

UNCTAD. 2006. "Wir06. Fdi from Developing and Transition Economies: Implications for Development." Switzerland: United Nations, p. 372.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:s 3–4), pp. 190–198.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Williams, A. 2016. "$500m Robbed from Bank Accounts in 6 Months …Tellers, University Students Are Main Culprits," in: *The STAR*. Jamaica.