Summer 8-2022

Predictors of Email Response: Determinants of the Intention of not Following Security Recommendations

Miguel Angel Toro-Jarrin
Old Dominion University, matoro81@hotmail.com

PREDICTORS OF EMAIL RESPONSE: DETERMINANTS OF THE INTENTION OF NOT FOLLOWING SECURITY RECOMMENDATIONS

by

Miguel Angel Toro-Jarrin
B.Sc., August 2005, Escuela Politécnica Nacional, Ecuador
M.Sc., May 2015, Instituto Tecnológico y de Estudios Superiores de Monterrey, México

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

ENGINEERING MANAGEMENT AND SYSTEMS ENGINEERING

OLD DOMINION UNIVERSITY
August 2022

Approved by:

Pilar Pazos (Director)

Miguel Padilla (Member)

Holly Handley (Member)

Ariel Pinto (Member)

ABSTRACT

PREDICTORS OF EMAIL RESPONSE: DETERMINANTS OF THE INTENTION OF NOT FOLLOWING SECURITY RECOMMENDATIONS

Miguel Angel Toro-Jarrin
Old Dominion University, 2022
Director: Dr. Pilar Pazos

Organizations and government leaders are concerned about cyber incidents. For some time, researchers have studied what motivates people to act in ways that put the confidentiality, integrity, and availability of information in organizations at risk. Still, several areas remained unexplored, including the role of employees' evaluation of the organizational systems and the role of value orientation at work as precursors of secure and insecure actions in relation to information technologies (information security [IS] action). The objective of this research project was to examine how the evaluations of formal and informal security norms are associated with the intention to follow them and to explore the role of work values, security systems, monitoring employees, and demographics in this association. It is essential to understand the determinants of IS action in the workplace so that interventions aim for organizational behavioral change focusing on a few determinants of IS action. In the execution of the project, several scenarios were formulated. In the scenarios, a character whose actions enact a particular value orientation at work fails to follow security recommendations. Several items were formulated to capture the variables of interest. After ensuring that the materials had good psychometric properties, a sample of 661 U.S. workers was collected and the data submitted to several analyses. The results revealed that the negative evaluation of the importance of security recommendations and the negative evaluation of others relative to following security recommendations were positively associated with the intention of not following those security recommendations. The evaluation of the completeness of security recommendations was negatively associated with the intention of not following them. The perception of others following security recommendations was not associated with the intention of not following them. It was also found that work values, security systems, monitoring, and demographics play a role in the association found. This research project does not support causality but provides evidence of the investigated association. The survey research did not investigate actual actions; however, several precautions were taken to ensure that the results provide preliminary evidence of the precursors of IS action at work.

I dedicate this work to my dear daughter, Eva. With all the love that one person can possibly have for another, with all the love that fills my heart every minute that I think of her.

"Yo te llevo dentro, hasta la raíz."

ACKNOWLEDGMENTS

Several people contributed to the successful completion of this dissertation. I extend my gratitude to my advisor, Dr. Pilar Pazos, for her patience and constant advice throughout the execution of this dissertation. I am also grateful to Dr. Miguel Padilla for teaching me the tools that I implemented in the analysis section. To Dr. Holly Handley and Dr. Pinto for providing their timely advice when I needed a fresh perspective. I also thank the chair of the Department of Engineering Management and Systems Engineering (EMSE), Dr. Andres Souza-Poza, for his constant support and advice during these years. I am also grateful to Dr. Ghaith Rabadi, the graduate program director for the doctoral program at EMSE, for his timely help in completing my degree. I would also express my gratitude to all my instructors who so kindly shared their knowledge and experience with me. Finally, a special thanks to all my friends in the department with whom I shared moments of frustration and success.

TABLE OF CONTENTS

Page

LIST OF TABLES viii

LIST OF FIGURES x

Chapter

I. INTRODUCTION 1

1.1 Consequences of Phishing Attacks 2
1.2 Information Security in Organizations 3
1.3 IS Actions 4
1.4 Predictors of IS Action 9
1.5 Research Questions 10
1.6 Relevance of the Present Study 11
1.7 Brief Description of the Methodology 13
1.8 Overview of This Document 14

II. LITERATURE REVIEW 15

2.1 IS Behavioral Research 15
2.2 Theories Supporting IS Behavioral Research 27
2.3 Theoretical Background 29
2.4 Theoretical Premise and Hypotheses 32

III. METHODOLOGY 43

3.1 Population 45
3.2 Scenarios and Items Development 45
3.3 Factor Exploration 50
3.4 Confirmatory and Hypotheses Evaluation 59

IV. RESULTS 72

4.1 Items' Descriptive Statistics 72
4.2 Descriptive Statistics 72
4.3 Structural Analysis Results (H1–H6) 85
4.4 Structural Invariance Analyses Results (H7–H10) 86

V. DISCUSSION 101

5.1 Negative Evaluation of Formal and Informal Norms Relative to Security Recommendations (SR) as Predictors of the Intention (IN) of Not Following Them 101
5.2 The Role of Work Values 103
5.3 The Role of Secure Systems 104
5.4 The Role of Monitoring 105
5.5 The Role of Demographics 106

5.6 Limitations 108

VI. CONCLUSIONS 111

REFERENCES 113

APPENDICES 129

A. FACTOR ANALYSES RESULTS FOR ALL SCENARIOS 130
B. MATERIALS 138
C. FACTORIAL INVARIANCE ANALYSES ACROSS SAMPLES 143
D. STRUCTURAL INVARIANCE ANALYSES ACROSS SAMPLES 172
E. ITEMS'S DESCRIPTIVE STATISTICS 202
F. VARIANCE – COVARIANCE MATRICES 208

VITA 209

LIST OF TABLES

Table Page

1.1. Two-Dimension Taxonomy of IS Actions (Stanton et al., 2005) 4

1.2. Information Security-Related Behaviors (IS Actions) 6

2.1. Definition of Constructs 33

2.2. Hypotheses Summary 41

3.1. Research Methodology 44

3.2. Statistics of the Employed Labor Force in the U.S. (U.S. Bureau of Labor Statistics, 2021) 45

3.3. Scenario Realism Check Results 47

3.4. Variables' Operational Definition 48

3.5. Factor Correlation Matrix and Cronbach's Alpha Per Scenario 53

3.6. Factor Analysis Results for Scenario 1 54

3.7. Correlation Coefficients Between Factors in This Study and Williams's Scale Dimensions 58

3.8. Sample Characteristics (N = 721 Valid Responses) 60

3.9. Items' Loadings Per Scenario for the Modified Six-Factor Solution 63

3.10. Reliability and Internal Structure Results for the Modified Six-Factor Solution 64

3.11. Fit Indexes and Item Loadings Per Scenario for the Modified Six-Factor Solution 68

3.12. Counts Per Group (N = 661, No Outliers) 70

4.1. Factors' Descriptive Statistics (N = 661) 72

4.2. Descriptive Statistics and Comparison Across Groups for ATI 74

4.3. Descriptive Statistics and Comparison Across Groups for ATC 76

4.4. Descriptive Statistics and Comparison Per Group for MSR 78

4.5. Descriptive Statistics and Comparison for DN 80

4.6. Descriptive Statistics and Comparison Per Group for Inj 82

4.7. Descriptive Statistics and Comparison for IN 84

4.8. Structural Model (H1–H6) 85

4.9. Regression Coefficients Across Scenarios from the Structural Invariant Model (H7) 88

4.10. Regression Coefficients for Both Those That Have Secure Systems and Those That Do Not (AD01) (H8) 90

4.11. Regression Coefficients for Both, Employees Whose Email Accounts Are Monitored and Those Whose Are Not (Ad02) (H9) 92

4.12. Regression Coefficients Per Age Group for the Structural Invariant Model 94

4.13. Regression Coefficients Per Gender for the Structural Invariant Model 94

4.14. Regression Coefficients Per Level of Education for the Structural Invariant Model 95

4.15. Regression Coefficients Per Work Experience for the Structural Invariant Model 95

4.16. Regression Coefficients Per Job Level for the Structural Invariant Model 96

4.17. Regression Coefficients Per Organization Size for the Structural Invariant Model 96

4.18. Summary of Findings 97

LIST OF FIGURES

Figure Page

1. Conceptual Model 42

2. Modified Six-Factor Measurement Model 65

3. Results 100

CHAPTER 1
INTRODUCTION

Several events in the last decades have proven that cyber incidents transcend individual consequences and have a social impact. For example, in 1982, a Trojan horse in the Trans-Siberian Pipeline's supervisory control and data acquisition (SCADA) system caused an explosion equivalent to 3 kilotons of TNT (Cherdantseva et al., 2016; McLaughlin et al., 2016). In 2000, a former employee of a sewage treatment plant hacked the SCADA system, causing 800 kiloliters of raw waste to enter the nearby river (McLaughlin et al., 2016). In 2003, a virus infiltrated a petrochemical company's process control servers, resulting in a production shutdown of 5 hours (McLaughlin et al., 2016). In 2005, a worm infected a Daimler-Chrysler plant stopping, production for 50 minutes (McLaughlin et al., 2016). In 2008, a cyber-attack on the Baku-Tbilisi-Ceyhan pipeline caused an explosion in which 3,000 oil barrels were spilled (McLaughlin et al., 2016). In 2010, the virus Stuxnet infiltrated a uranium enrichment site in Iran. The attack destroyed 10% of its centrifuges (Cherdantseva et al., 2016; De Falco, 2012; McLaughlin et al., 2016).

The negative consequences of such events, which risk the confidentiality, integrity, and availability of individuals and organizations' digital information, have created concern. A survey developed in March 2016 revealed that most Americans (64%) report having suffered a significant data breach or fraud (Olmstead & Smith, 2017). A considerable share of Americans (49%) feel that their personal information is less secure than it was 5 years ago, and a significant majority (70%) believe that a cyberattack will impact the nation's public infrastructure and its financing system (66%; Olmstead & Smith, 2017). Government leaders share these concerns. In 2003 President George W. Bush established the National Strategy to Secure Cyberspace (Department of Homeland Security, 2003). In this strategy, the U.S. government acknowledged that protecting cyberspace is crucial for the country and established the need to invest the necessary resources.

Although necessary, technical solutions such as firewalls, software updates, patches, and security software are not sufficient protection against potential cyber-attacks (Terranova Security, 2020). The human element is of fundamental importance to an organization's cybersecurity posture (Terranova Security, 2020). The employees in organizations perform insecure actions regarding information technologies with or without being aware of the potential negative consequences. In this sense, a conscious IS action is an act of awareness that digital information mismanagement will impact other individuals, the entire organization, and society (Parsons et al., 2017). Organizations provide guides and recommendations about secure IS procedures. Olmstead and Smith (2017) reported, however, that many Americans fail to follow those recommendations. For example, only 12% of internet users in America use

password management software, and 54% use unsecured wi-fi connections (Olmstead & Smith, 2017). Americans believe that a cyber-incident will impact public infrastructure; still, cybersecurity hygiene is not at the top of the list of worries for the American public (Olmstead & Smith, 2017).

1.1 Consequences of Phishing Attacks

One set of secure and insecure actions in relation to information technologies (information security [IS] action) that are important for their potential impact (e.g., phishing attacks) are the activities related to the personal management of email accounts. Phishing is a socially engineered action that influences people to visit fraudulent websites or persuades them to enter personal information (Purkait, 2012). Phishers use several means to reach their victims (Shein, 2011), but email is the most common (FBI, 2019).

A successful phishing attack has serious consequences. From 2015 to 2019, the Federal Bureau of Investigation received around 1.7 million cybercriminal activity complaints (FBI, 2019); among those activities, phishing was the most prevalent. The estimated loss corresponding to the same period was around $10 billion (FBI, 2019). Incalculable losses are also due to harm of reputation and trust (Terranova Security, 2020). The number of events worldwide has increased as well, as evidenced by the number of domains (e.g., att.com, intel.com) targeted by phishing attacks. There were 326.3 million domains globally in 2016; in the same year, 255,065 new phishing attacks on domains were reported worldwide, increasing 10% from the previous year (Aaron & Rasmussen, 2017). Changes in the way people work have contributed to the problem. These days, more people work or do work activities remotely, and the COVID-19 pandemic accelerated this trend. Presumably, for that reason, cyber criminality events have also substantially increased. From January to March 2020, the number of blocked suspicious messages targeting remote workers increased 30,000%. During the 2020–2021 pandemic, COVID-19-related spear-phishing attacks increased by 667% (Terranova Security, 2020). The economic loss has increased correspondingly. For example, the FBI reported that the estimated losses of cybercriminal activities increased from $1.1 billion in 2015 to $3.5 billion in 2019 (FBI, 2019).

These reports point to the considerable consequences at a societal level. Still, it only takes one malicious email, visiting a dubious webpage, or intentionally downloading a virus to potentially compromise vast amounts of confidential data (Terranova Security, 2020). Employees' careless IS actions are a significant cause of concern for organizations. The 2016 World Target List reports several sectors affected, including banking and financial services (25%), government (1%), e-commerce (30%), money transfer (18%), and social networks and email companies (19%; Aaron & Rasmussen, 2017). In a 2020 study of employees' IS actions in firms of various sizes and from a wide variety of industries, the findings revealed that nearly 19.8% of workers clicked phishing links, 13.4% submitted their credentials on a

phishing website, and an average of 50% of clickers submit data on a web form (Terranova Security, 2020).

1.2 Information Security in Organizations

To cope with malicious and nonmalicious IS-related behaviors, organizations implement systems typically reflected in an information security policy (hereafter, security policy [ISP]; Cram et al., 2017). An ISP defines the mechanisms (technical and human) to prevent, detect, and respond to security incidents (Landoll, 2016). Organizations create ISP in compliance with external regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the European Union Data Protection Directive (EU DPD; Cram et al., 2017; Landoll, 2016). The development, implications, and implementation of ISP in organizations involves three levels: security program, issue-specific, and technical (Cram et al., 2017). Security program defines the strategic direction in alignment with sector or government regulations (Whitman, 2008), typically addressed by the public policy community (e.g., Weber, 2017). Issue-specific security policy includes guidelines and procedures that employees must comply with (Cram et al., 2017), which are typically addressed by the information systems and organizational science communities. Finally, technical security policy includes technological architecture (Baskerville & Siponen, 2002), which is typically addressed by the IT community (e.g., Purkait, 2012). The security policy literature focus on 10 elements (Cram et al., 2017):

- Security standards, guidelines, and regulations;
- Desired policy format and structure;
- Internal and external risk management considerations;
- Security policy design and implementation;
- Information security culture, awareness, and support;
- Socioemotional consequences for employees;
- Personality and dispositional traits;
- Security policy legitimacy, fairness, and justice;
- Compliance with security policy, and;
- Organizational security objective.

Cram et al. (2017) associated them with five relations: (a) influences on the design and implementation of policies, (b) the influence of security policies on the organization and individual employees, (c) the influence of policy compliance on organizational objectives, (d) adjustment on policy design, and (e) the influence of organization and individual employee factors on policy compliance, which was the focus of the current study.

1.3 IS Actions

ISP provides recommendation and regulations regarding many IS actions at work. Examples of these behaviors include creating strong passwords, verifying the content of an email before clicking on links, and avoiding sharing personal information on social media (Posey et al., 2013). Users perform these behaviors with or without awareness of their consequences, and the technical skills they require to execute such behaviors vary. There are different motivations to, for instance, share confidential information with friends and publish bank account numbers. To classify secure-related behaviors, Stanton et al. (2005) suggested six types of IS action categories that fit into a two-dimensional taxonomy. One dimension captures the level of technical expertise needed to perform the IS action, and the second captures the IS action's malicious/nonmalicious intentionality. Table 1.1 shows the six categories and descriptions thereof.

Table 1.1

Two-Dimension Taxonomy of IS Actions (Stanton et al., 2005)

Expertise	Intentionality	Category	Description
High	Malicious	Intentional destruction	Behavior requires technical expertise and a strong intention to harm the organization's IT and resources. Example: user breaks into an employer's protected files to steal a trade secret.
Low	Malicious	Detrimental misuse	Behavior requires minimal technical expertise but includes an intention to harm through annoyance, harassment, rule-breaking, etc. Example: using company email for spam messages marketing a sideline business.
High	Neutral	Dangerous tinkering	Behavior requires technical expertise but no clear intention to harm the organization's IT and resources. Example: user configures a wireless gateway that inadvertently allows wireless access to the company's network.
Low	Neutral	Naive mistakes	Behavior requires minimal technical expertise and no apparent intention to harm the organization's information technology and resources. Example: choosing a bad password such as ''password.''
High	Beneficial	Aware assurance	Behavior requires technical expertise and a firm intention to do good by preserving and protecting the organization's information technology and resources. Example: recognizing the presence of a backdoor program through careful observation of own PC.
Low	Beneficial	Basic hygiene	Behavior requires no technical expertise but includes a clear intention to preserve and protect the organization's IT and resources. For example, a trained and aware employee resists social engineering attempts by refusing to reveal her password to a caller claiming to be from computer services.

Two categories of behaviors are typical in organizations: naïve mistakes and basic hygiene behaviors. These types of behaviors require low skills and have no malicious intentionality. A naïve mistake transforms into a basic hygiene behavior when an employee follows security recommendations. Authors further define and categorize basic hygiene types of behaviors. After a series of exploratory studies, Parsons et al. (2014, 2017, 2015) defined 23 behaviors, which they grouped into seven areas of behaviors that fit into low skill and nonmalicious intentionality: password management, email use, internet use, social network use, incident reporting, mobile computing, and information handling. Posey et al. (2013), in their study of protective motivated behaviors, identified 14 clusters: (a) legitimate email handling, (b) protection against unauthorized exposure, (c) policy-driven awareness and action, (d) appropriate data entry and management, (e) document conversion, (f) secure software, email, and internet use, (g) verbal and electronic sensitive-information protection, (h) wireless installation, (i) widely applicable security etiquette, (j) distinctive security etiquette, (k) coworker reliance, (l) account protection, (m) immediate reporting of suspicious activity, and (n) equipment location and storage.

Other researchers have refined and expanded the category of basic hygiene behaviors. For example, Hadlington (2017) investigated the relationship between risky cybersecurity behaviors, attitudes towards cybersecurity, internet addiction, and impulsivity. This author addressed the same areas that Parsons et al. (2017) identified, except incident reporting, including software protection. Calic et al. (2016) identified the eleven most essential behaviors from the perspective of information security experts, and nine were part of the Parsons et al. (2017) list. Anwar et al. (2017) conducted a cross-sectional survey among employees of diverse organizations, focusing on four groups of behaviors: device securement, password generation, proactive awareness, and updating. These are included in the list of behaviors presented before (Parsons et al., 2017), except device security, which was also identified by Egelman and Peer (2015). Table 1.2 provides a summary of areas and basic hygiene behaviors addressed in the literature.

Table 1.2

Information Security-Related Behaviors (IS Actions)

Area	Behavior	Publications
Password management	Using the same password	(Anwar et al., 2017; Calic et al., 2016; Egelman & Peer, 2015; Hadlington, 2017; Parsons et al., 2017)
	Sharing passwords	(Calic et al., 2016; Hadlington, 2017; Parsons et al., 2017; Stanton et al., 2005)
	Using a strong password	(Egelman & Peer, 2015; Hadlington, 2017; Parsons et al., 2017; Stanton et al., 2005)
	Storage passwords that are easily accessible	(Posey et al., 2013; Stanton et al., 2005)
	Use of a password management software	(Aurigemma & Mattson, 2019a)
Email use	Click on links in emails from (unsolicited) known senders	(Downs et al., 2007; Egelman & Peer, 2015; Hadlington, 2017; Jagatic et al., 2007; Moody et al., 2017; Parsons et al., 2015, 2017; Posey et al., 2013)
	Click on links in emails from unknown senders	(Downs et al., 2007; Hadlington, 2017; Jagatic et al., 2007; Moody et al., 2017; Parsons et al., 2015, 2017; Posey et al., 2013)
	Opening attachments in emails from unknown senders	(Anwar et al., 2017; Calic et al., 2016; Downs et al., 2007; Jagatic et al., 2007; Moody et al., 2017; Parsons et al., 2017; Posey et al., 2013)
Internet use	Downloading files from unknown sources	(Hadlington, 2017; Parsons et al., 2017)
	Accessing dubious websites	(Calic et al., 2016; Parsons et al., 2017)
	Entering information online	(Egelman & Peer, 2015; Hadlington, 2017; Parsons et al., 2017)

Table 1.2 (continue)

Area	Behavior	Publications
Internet use	Using free-to-access public Wi-Fi	(Hadlington, 2017)
	Relying on a trusted friend or colleague to advise on aspects of online security.	(Hadlington, 2017)
	Disabling the anti-virus on the work computer to download information from websites.	(Hadlington, 2017)
	Reviewing privacy/security settings on social media sites (e.g., Facebook, Twitter, LinkedIn).	(Anwar et al., 2017)
	Knowing what website is being visited based on its look and feel, rather than by looking at the URL bar	(Egelman & Peer, 2015)
	Knowing what website is being visited based on its look and feel, rather than by looking at the URL bar	(Egelman & Peer, 2015)
	Mouse over links to see where they go before clicking them.	(Anwar et al., 2017; Egelman & Peer, 2015)
	Customizing browser and computer settings to prevent the intrusion of spyware into my computer	(Dinev & Hu, 2007)
Social media use	Setting social media privacy	(Parsons et al., 2017)
	Considering consequences	(Calic et al., 2016; Parsons et al., 2017)
	Posting about work	(Parsons et al., 2017)
	Sharing my current location on social media.	(Hadlington, 2017)
	Accepting friend requests on social media because the photo is familiar	(Hadlington, 2017)
	Oversharing information on social media	(Calic et al., 2016)
Mobile devices	Physically securing mobile devices	(Calic et al., 2016; Parsons et al., 2017)
	Sending sensitive information via Wi-Fi	(Calic et al., 2016; Parsons et al., 2017)
	Shoulder surfing	(Parsons et al., 2017; Posey et al., 2013)
	Using a PIN or passcode to unlock a mobile phone.	(Egelman & Peer, 2015)

Table 1.2 (continue)

Area	Behavior	Publications
Information handling	Disposing of sensitive printouts	(Parsons et al., 2017; Posey et al., 2013)
	Inserting removable media	(Calic et al., 2016; Hadlington, 2017; Parsons et al., 2017)
	Leaving sensitive material	(Parsons et al., 2017)
	Using online storage systems to exchange and keep personal or sensitive information.	(Hadlington, 2017)
	Storing company information on personal electronic devices	(Anwar et al., 2017; Hadlington, 2017)
	Supporting sensitive information on workstation computers	(Menard et al., 2018)
	Sending sensitive information such as passwords, account numbers, and so on via email	(Anwar et al., 2017)
	Discussing sensitive information with authorized individuals only	(Posey et al., 2013)
Incident reporting	Reporting suspicious behavior	(Anwar et al., 2017; Parsons et al., 2017)
	Ignoring poor security behavior by colleagues	(Calic et al., 2016; Egelman & Peer, 2015; Parsons et al., 2017; Posey et al., 2013)
	Reporting all incidents	(Parsons et al., 2017; Posey et al., 2013; Stanton et al., 2005)
	Watching for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, and so on).	(Anwar et al., 2017; Posey et al., 2013)
Software protection	Checking that the smartphone/tablet/laptop/PC software is updated.	(Egelman & Peer, 2015; Hadlington, 2017; Schaffer & Debb, 2019)
	Check for updates to any anti-virus software you have installed.	(Anwar et al., 2017; Dinev & Hu, 2007; Egelman & Peer, 2015; Hadlington, 2017)
Device security	Setting the computer screen to automatically lock if not used for a prolonged period.	(Egelman & Peer, 2015; Posey et al., 2013)
	Using a password/passcode to unlock a laptop or tablet.	(Egelman & Peer, 2015)
	Manually locking the computer screen when stepping away from it.	(Egelman & Peer, 2015; Posey et al., 2013)

1.4 Predictors of IS Action

In the existing body of literature, scholars have investigated the predictors of IS actions from different theoretical perspectives, such as the reasoned action approach, protection motivation theory, and deterrence theory. These perspectives include one or more of the following concepts: (a) action evaluation includes the attitudes towards action, the vulnerability of suffering the consequences of an IS action, and the costs-benefits of IS action; (b) self-evaluation regarding IS action is the self-efficacy or the perceived behavioral control regarding the action and the evaluation of the moral component of IS action; (c) context evaluation includes the evaluation of social norms and organizational structures; (d) level of intention-action specificity refers to how specific the intention-action is defined such as complying with ISP (general) vs. sharing password (specific); and (e) level of context elaboration is the level of contextualization from which studies capture the precursors of IS actions.

The body of literature has expanded to include all the considerations numbered before. From these highly contextualized studies, it is known that the perceived severity and vulnerability of the consequences of IS actions are precursors of the attitudes toward conforming with specific security policy provisions (Bélanger et al., 2017; D'Arcy & Lowry, 2019). Attitudes toward conforming with ISP are precursors of the intention to comply with ISP (Bélanger et al., 2017; D'Arcy & Lowry, 2019). In turn, intention predicts actual compliance when such provisions are strictly enforced (Bélanger et al., 2017; D'Arcy & Lowry, 2019) or when they are presented as recommendations (e.g., regular backup information; Boss et al., 2015). Perceived severity is a direct precursor of intention when attitudes are not considered (Boss et al., 2015; Schuetz et al., 2020). Previous scholars have reported that when recommendations guide IS-related actions, the perceived susceptibility, perceived benefits, and self-efficacy of implementing such action positively correlate with the self-report of IS-related actions (Ng et al., 2009). Self-efficacy relative to exercise security recommendations correlates positively with the self-report of IS-related actions (D'Arcy & Lowry, 2019; Ng et al., 2009) and the intention to perform such actions (Boss et al., 2015; Johnston & Warkentin, 2010; Schuetz et al., 2020). Response efficacy positively impacts the intention to implement security measures (Boss et al., 2015; Johnston & Warkentin, 2010; Schuetz et al., 2020). The perceived severity of the consequences of not following specific security recommendations positively affects the effect of perceived susceptibility and self-report over IS actions (Ng et al., 2009). Interestedly, perceived severity negatively moderates the effect of self-efficacy and the negative impact of perceived barriers on the self-report of IS actions (Ng et al., 2009). Perceived costs of implementing specific IS-related actions defined in specific situations in the workplace negatively impact the intention to implement them (Boss et al., 2015; Schuetz et al., 2020), response efficacy, and self-efficacy (Johnston & Warkentin, 2010). Social influence of others' specific IS-related actions positively correlates with the intention of security compliance behavior (Johnston & Warkentin,

2010), security compliance behavior (D'Arcy & Lowry, 2019), and moral considerations (Banerjee et al., 1998; D'Arcy & Lowry, 2019). Organizational commitment and attitudes towards specific organizational systems (e.g., monitoring IS-related actions) positively correlate to the intention of supporting the implementation of those systems (Spitzmüller & Stanton, 2006). In contrast, evaluating organizational efforts to motivate employees to follow recommendations, operationalized as action cues, weakly correlates with the self-report of IS-related actions (Ng et al., 2009). Aurigemma and Mattson (2019a) found that long-term orientation moderates the impact of attitudes towards adopting security controls on implementing security controls. Security climate moderates the impact of attitudes towards organizational systems and the intention to accept those systems (Spitzmüller & Stanton, 2006). Banerjee et al. (1998), however, found security climate to be a direct precursor of IS action intention.

1.5 Research Questions

Overall, previous scholars have presented findings suggesting that attitudes toward complying with security policy provisions are precursors of the employee's intention to act in compliance with SP. The negative attitudes towards security recommendations and their impact on intentions to perform specific insecure acts in situations employees live day by day have not been explored. Therefore, the current researcher asked:

> **RQ1:** How do the negative attitudes toward specific security recommendations relate to the intention to act against those recommendations?

The literature also suggests that social norms relative to following security policy provisions impact the intention to follow those provisions. The impact of the negative perception of how others evaluate security recommendations and actions against those recommendations with the intention to perform specific insecure acts in specific day-by-day situations in organizations has not been explored. Therefore, the following research question was developed:

> **RQ2:** How does the negative evaluation of others relative to security recommendations and a positive evaluation of actions against those recommendations relate to the intention of not following security recommendations?

The moral component relative to IS action is a precursor of intention to align with security policy provisions. An indirect measure of the moral component is the self-evaluation of regret. The anticipated affective evaluation of IS action (anticipated regret) is an additional precursor of intention to comply with ISP (Sommestad et al., 2015b); however, the role of the lack of anticipated regret relative to contravening security recommendations on the intention to perform specific insecure acts in specific day-by-day situations in organizations has not been explored. Therefore, the current researcher asked:

RQ3: How does the absence of anticipated regret of not following security recommendations affect the intention to follow those recommendations?

The impact of individual work value orientation on IS action has been found implicitly in the literature. Variables such as organizational attachment, commitment, organizational climate, or neutralization techniques suggest that work values play a role in predicting IS action, but the effect of work values has not been explicitly addressed in the literature. The following research question was developed to bridge this gap:

RQ4: Do different individual work value orientations modify the relationship between the negative evaluation of formal and informal norms and the intention to not act in alignment with security recommendations?

Due to a lack of resources or commitment to security, not all organizations have secure systems that support employees following security recommendations at work. How the awareness of the existence of these supporting systems affects the association between the evaluation of formal and informal norms and the intention of not following them has not been explored. Therefore, this study asked:

RQ5: Do the awareness of the existence of secure systems modify the relations between the evaluation of formal and informal norms and the intention of not following security recommendations?

Monitoring employees' behaviors concerning the management of information at work might be considered an act of distrust or a violation of privacy. Even though the impact of monitoring is a precursor of IS action, how monitoring affects the association between the negative evaluation of formal and informal norms and the intention of not following security recommendations has not been explored. Therefore, the sixth research question was as follows:

RQ6: Do the awareness of monitoring systems modify the relations between the negative evaluation of formal and informal norms and the intention to not act in alignment with security recommendations?

Finally, demographics play a role in the prediction of IS action. To complement the results, the final research question was:

RQ7: Do demographics associate with the intention of not following security recommendations? And do demographics modify the relationship between the negative evaluation of formal and informal norms and the intention of not following security recommendations?

1.6 Relevance of the Present Study

Although government and sector-level recommendations and guidelines do not have the status of directives, and organizations are not required to comply, they offer a general frame to support policy

design and implementation. The relationship between those guidelines and policy design is typically not theory-driven and relies more on practical considerations (e.g., regulation compliance) or best practices (Alshaikh et al., 2021; Aurigemma & Mattson, 2019b; Cram et al., 2017). For example, among the recommendations is implementing security, education, and training (SETA) programs (SO/IEC, 2012, 2013). The guidelines emphasize the importance of providing periodic training and evaluating its impact on employees' security behavior (Kumaraguru et al., 2010; Kweon et al., 2021; Sheng et al., 2007). SETA programs mainly meet compliance requirements, rather than behavioral change (Alshaikh et al., 2021). Additionally, current rule-based programs focus on improving employees' knowledge rather than influencing determinants of behavioral response (Alshaikh et al., 2021; Aurigemma & Mattson, 2019b). There is a limited translation from research outcomes to program implementation, and there is little attention to the employee context (Aurigemma & Mattson, 2019b). Understanding the psychosociological determinants of IS action is necessary to inform more effective security interventions (e.g., SETA programs).

Any information security-related behavior can cause a data breach or an information security incident (Stanton et al., 2005). Capturing all precursors of IS actions in one study considering many potential determinants of IS actions seemed impractical or not informative (Aurigemma & Mattson, 2019b). An alternative was to study security behaviors with a high level of generality (e.g., policy compliance as a dependent variable (e.g., Bulgurcu et al., 2010)) or to study several behaviors in a more detailed context aiming to develop a theory of security compliance (e.g., Lowry & Moody, 2015). Furthermore, Djajadikerta et al. (2015) found that the predictors of information security-related behaviors differ depending on the behavior. Multiple studies have corroborated this difference with several scenarios describing noncompliance behaviors (Aurigemma & Mattson, 2019b; Barlow et al., 2013, 2018; Siponen & Vance, 2010). For example, the predictors of ignoring a warning message might not be the same as those about sharing sensitive information. An alternative approach explores factors that effectively influence one specific behavior and extend their application to other related behaviors (Bandura, 1977; Fishbein et al., 2007). Although this approach has received some criticism in the IS literature (Crossler et al., 2013), an intervention is more effective when it focuses on specific behaviors described in concrete ways (Ajzen, 1991; Beck & Ajzen, 1991; Fishbein, 1975; Fishbein & Ajzen, 1977; Siponen & Vance, 2014). In the taxonomy of IS actions (e.g., Stanton et al., 2005), typical organization's members' actions (nonmalicious intention and low level of expertise) fall into naïve mistakes and basic hygiene. Parsons et al. (2017) found that proper email use actions have one of the lowest incidences and the highest variability compared to other related basic hygiene behaviors. This fact reveals that many email users fail to follow security recommendations. Understanding the predictors of forged email response is especially relevant to the cybersecurity posture in organizations for its relationship with

phishing attacks, ransomware, and other cyber-incidents (Moody et al., 2017; Parsons et al., 2015; Wright et al., 2014).

In the extant literature on precautionary email actions, researchers have investigated external context (e.g., workload), internal context (e.g., persuasive elements of a phishing email or characteristics of the email), knowledge as a predictor of precautionary email handling, and response cognitive processes (e.g., anti-phishing self-efficacy). In contrast with ISP compliance research, there is relatively little research on the attitudes and social norms relative to security policy provisions and the affective component of noncompliance behaviors as precursors of email management. It is essential to understand the evaluation of formal and informal norms as precursors of IS action at work so practitioners can intervene with evidence that the employee's evaluation of the efforts made by management has an impact on individual actions in day-by-day situations.

1.7 Brief Description of the Methodology

The methodology in this study implements survey research as the research method and follows a quantitative research design (Creswell, 2009). Overall, this study captures the negative evaluation of formal and informal security norms as determinants of the intention of not following them. Participants were presented with several scenarios that portrayed a day-by-day situation at work where a character failed to follow specific security recommendations. The scenarios presented the action enacting different value orientations at work. After the scenarios, participants answered several questions (items). The items captured the variables that form the nomology in this study. The methodology was designed to ensure that the materials (scenarios and items) had good psychometric properties and were appropriate to answer the research questions. The methodology was devised into three stages: (a) scenarios and items development and pretest, (b) factor exploration, and (c) confirmatory and hypotheses evaluation.

Several scenarios and items were formulated in the first stage, which involved the development and pretesting of scenarios and items. The realism of the scenarios was evaluated with participants collected in a first sample. The items were pretested for item wording, social desirability, survey flow, and to preliminarily examine the measurement model's internal structure. For this purpose, a second sample was collected. In the second stage, the factor structure of the measurement model was examined. All scenarios and improved items were administered to a new sample. Finally, the measurement model was confirmed in the third stage, and the hypotheses were examined. A new sample was collected from participants recruited from Qualtrics online panels. In Chapter 3, the researcher provides a detailed description and justification of the selected methodology.

1.8 Overview of This Document

In Chapter 2, the researcher reviews literature related to IS action in organizations. Chapter 3 is a description of the methodology and a presentation of preliminary results. Chapter 4 reflects the final results. Chapter 5 contains a discussion of the results, implications, limitations, and future research suggestions. Finally, Chapter 6 includes the researcher's conclusions.

CHAPTER 2
LITERATURE REVIEW

This chapter contains a review of IS behavioral research, emphasizing the key findings and opportunities for expanding the state of research. The researcher briefly describes the theories used in the IS research. The researcher then introduces the theoretical framework that supports this project and describes the theoretical premise and hypotheses for this study.

2.1 IS Behavioral Research

2.1.1 Information Security Policy (ISP) Compliance

The existing IS literature has focused on determinants of information security policy (ISP) compliance at the individual level. In this line of research, the intention to comply with ISP receives considerable attention. Determinants of the intention of ISP compliance include habit (Gregory, 2018; Pahnila et al., 2007), role values (Gregory, 2018), perceptions of potential sanctions (Gregory, 2018; Pahnila et al., 2007), attitudes towards security policy compliance, normative beliefs relative to security policy compliance (Bulgurcu et al., 2010; Ifinedo, 2012), self-efficacy (Bulgurcu et al., 2010) and perceived behavioral control relative to security compliance (Ifinedo, 2012), and perceived vulnerability of the consequences of noncompliance (Ifinedo, 2012). Other distant determinants are threat appraisal, facilitating conditions (Pahnila et al., 2007), the overall assessment of consequences, and knowledge about recommendations (Bulgurcu et al., 2010).

One common element in the studies above and many others (see Cram et al., 2017) is the generality relative to the definition of IS actions (ISP compliance). Authors have suggested increasing the specificity and providing more context to investigate determinants of ISP compliance (Siponen & Vance, 2014). Problems with a general definition of IS-related actions are, for example, that respondents answer questions like, “Do you intend to comply with the information security policy?” (Bulgurcu et al., 2010). When researchers ask whether a respondent complies with an ISP in a survey, they do not know which insecure acts respondents have in mind (Gregory, 2018). Additionally, asking respondents about their intentions to comply with a security policy can unintentionally capture the employee’s general predisposition towards complying with any other policy in their organization (Sommestad & Hallberg, 2013). Providing context to the evaluation of specific IS actions and the evaluated security policy can help scholars identify the predictors of ISP compliance more clearly.

2.1.2 Categories of Security Behaviors

Answering the call for more explicit identification of IS action (Siponen & Vance, 2014), the IS literature has also focused on the antecedents of categories or groups of security behaviors part of a

security policy. Including a more detailed description of the expected security actions, the IS literature has found that (a) security awareness, (b) the need for privacy and fear of crime, (c) attitudes and subjective norms towards preventive measures, and (d) ethical norms and work values are predictors of IS-related actions.

In terms of awareness of information security as a predictor of preventive measures, Hazari et al. (2008), in their study of organizations' member's behaviors using their computers at home for work-related activities, found that awareness of information security influences the predictors of security behaviors. Anderson and Agarwal (2010) found that psychological ownership (the state in which an individual feels a target is his; Pierce et al., 2001) adds to the prediction of conscious cybercitizens' behaviors. These authors also found that descriptive and subjective norms predict secure behaviors. Dinev and Hu (2007) found that technology awareness (i.e., users' consciousness of technical issues and interest in knowing how to deal with them) predicts security behaviors. Cain et al. (2018) found that knowledge about security concepts threat to information security are determinants of several cyber hygiene behaviors (security software, authentication, phishing scams, social networking, web browsing, Wi-Fi hotspot usage, and USB drive use). Cain et al. also found that older users tend to behave more securely than younger users and that self-identified experts reported less secure behaviors and had less knowledge about cyber hygiene than other participants. Additionally, Cain et al. reported that training did not increase users' cyber hygiene behaviors or knowledge.

The need for privacy and fear of the consequences of action also predict precautionary IS actions. Yao and Linz (2008) found that the need for privacy and fear of crime predict attitudes towards online privacy protection strategies. Fear appeals positively impact user intentions to comply with security recommendations, but the impact is not uniform (Johnston & Warkentin, 2010). It was partly determined by perceptions of self-efficacy, response efficacy, threat severity, and social influence. Similarly, Schuetz et al. (2020) conducted a study of the impact of fear appeals communicated through short messages to private users and organization members, finding that concrete fear appeals are more effective than abstract fear appeals in stimulating fear appeal outcomes. Furthermore, organizational users reported higher fear and protection motivation levels than personal users (Schuetz et al., 2020).

The attitudes and subjective norms toward precautionary IS actions are also precursors of IS action. Using two broad categories, Burns and Roberts (2013) studied online safety behavior against cybercrime. The first is overall cautiousness, which covers, for example, reading license agreements and privacy policies on websites before registering. The second is online technology knowledge and covers behaviors such as using pop-up window blockers, implementing firewalls and other internet security programs, and regularly checking the computer for spyware. The authors found that attitudes and subjective norms are predictors of intentions and that perceived behavioral control and intentions directly

predicted online safety behaviors. Jansen (2017) investigated precautionary online behaviors that financial organizations would like their customers to take. This author found that social norms do not significantly predict bank clients' precautionary online behaviors. This is likely because the behavior under study concerned individual interest that does not necessarily align with the organization's interests (Jansen, 2017).

Finally, ethical norms and values are also predictors of IS action. Authors (e.g., Banerjee et al., 1998; Leonard et al., 2004) have found a significant influence of ethical elements over attitudes and intentions. Guo et al. (2011) cited that relative advantages for job performance and workgroup norms positively influence the attitudes toward non-malicious behaviors such as writing down passwords, use of unauthorized portable devices carrying sensitive information, installation and use of unauthorized software and use of insecure public wireless. Guo et al. also found that the perception of risk and perceived identity match negatively affect the attitudes towards nonmalicious behaviors, and attitudes are a significant predictor of intention towards non-malicious behavior. A common theme in this line of research is measuring the respondent's probability of acting like the character in a hypothetical scenario where IT ethics are examined.

The literature above focused on factors relative to the IS actions and the employee. Still, the evaluation of specific security rules and regulations and their relation to IS action has been unexplored. Knowledge of concepts is a predictor of IS action. Still, awareness of specific systems in place that would prevent a potential cyber-incident and its role as a precursor of IS action remains unexplored. In studies with a lower level of generality, the attitudes and subjective norms toward precautionary IS action have been found to be predictors of IS actions, but the attitudes towards specific security policy provisions and the subjective norms relative to those provisions and their association with following SP have not been explored. Ethical norms are precursors of IS actions, but the affective component related to IS actions that contravene SP in a contextualized study remains unexplored. Additionally, the role of work values over IS action has been studied only tangentially. The value orientation of IS action and how it affects the relations between the precursors of IS action and the intention to comply with security policy has been unexplored.

2.1.3 The Use of Context-Specific Security Behaviors in IS Compliance

Behavioral prediction is more accurate if the focus is on specific behaviors rather than a category of behaviors or goals (Fishbein, 1975; Fishbein & Ajzen, 2010). Sheeran (2001) and Sheeran and Webb (2016) provided a theoretical and empirical discussion about intention–behavior prediction and how this relation can be affected by the level of generality or specificity of the behavioral object in question. Regarding IS actions, Djajadikerta et al. (2015) suggested that different security behaviors have different precursors. By implementing social cognitive theory, Larose and Rifon (2007) examined the effects of

explicit privacy warnings about database information practices stated in a website's privacy policy. Warnings increased perceptions of the risks associated with information practices and decreased disclosures. The effects were moderated by consumer privacy self-efficacy and involvement with privacy. The results support the development of privacy warnings as a part of consumer privacy self-regulatory efforts. Bélanger et al. (2017) studied the predictors of early conformance toward technology-enforced security policy. These authors measure early conformers' intentions regarding password management policy changes. Attitudes towards the specified security provisions predicted the intention of policy compliance and actual behavior (Bélanger et al., 2017). Finally, Vafaei-Zadeh et al. (2019) investigated the effects of perceived behavioral control and level of awareness over attitudes towards buying antimalware software and attitude, subjective norms, and perceived behavioral control on the intention to use anti-malware software. These authors found that their model explains attitude and intentions appropriately. Their results suggest that perceived behavioral control—in this case, affordable software—influences the intention to buy protective technology. It also suggests that the information people receive about the importance of having such technologies influence their attitudes towards those technologies (Vafaei-Zadeh et al., 2019).

The intention and actual compliance with specified security policy provisions from the attitudes towards that provision expanded the understanding of IS action; however, the relation of attitudes towards ISP and the intention to follow such policy when this is not rigorously enforced (e.g., two-factor authentication) have not been explored. A potential research opportunity is to explore how the attitudes towards policy provisions associate with the intention to perform IS actions when the policy provisions are not mandatory and are presented to employees as recommendations with low or null control.

2.1.4 Scenario-Based Behaviors to Examine IS Compliance

IS researchers have advanced the understanding of security compliance by contextualizing specific conditions of noncompliance using scenarios. This technique has been used in organizational ethics research (Trevino, 1992). Researchers present scenarios with a complete description of a non-compliance action and ask participants whether they would act similarly. The authors introduced variables of interest in the scenarios. This approach aims to generalize findings from the study of several IS actions described in scenarios to all possible IS actions. With this approach, two main areas have been explored in IS research: type of administrative control and fear appeals.

The type of administrative control is a predictor of security policy compliance. For example, Lowry and Moody (2015) proposed the control-reactance compliance model to explain opposing motivators to comply with organizational information security policy. These authors combined control theory and reactance theory. Control theory classifies the types of control used in organizations to constrain employee behavior and explain the social conditions in which the control is used (Ouchi &

Maguire, 1975). Reactance theory posits that whenever people feel the behavior is restricted, they likely would experience reactance (Brehm, 1966). Lowry and Moody (2015) examined eight security issues: end-user software installation, antivirus and antispyware software use with corporate networks, use of non-work-related software, inconsistent use of antivirus software, personal use of corporate email systems, lack of centralized data storage, use of USB drivers for sensitive data and personal internet use. The authors found that high levels of administrative control influence intention to security compliance. Still, they also found that reactance provoked a boomerang effect detrimental to the information security posture in organizations.

In terms of fear appeals as a tool to influence security policy compliance, Siponen and Vance (2010) studied the effect of neutralization techniques in combination with sanctions to predict intentions to violate IS security policy described in three different scenarios. The neutralization techniques come from neutralization theory (Matza, 1964). The theory posits that individuals who commit unlawful acts neutralize specific values within themselves. Siponen and Vance (2010) used six neutralization techniques: defense of necessity, appeal to higher loyalties, condemnation of condemners, the metaphor of the ledger, denial of injury, and denial of responsibility. The sanctions that they included in their model are formal organizational sanctions, informal sanctions, and shame. The authors found that neutralization techniques affect security compliance beyond the expected effect of sanctions. In another example, Willison et al. (2018) examined the role of procedural and distributive justice on employee computer abuse intentions. These authors formulated 36 scenarios combining several conditions and presented four scenarios to each participant. They also examined the role of sanctions (perceived sanction severity and certainty) and neutralization techniques (denial of injury, denial of the victim, and the metaphor of the edger) acting as moderators. They found that employees formed the intention to commit computer abuse if they perceived procedural injustice, and neutralization techniques and certainty of sanctions moderated this influence.

Focusing on a few IS-related actions and scenarios has received some criticism (Aurigemma & Mattson, 2019b) due to the focus on theory development from a limited number of scenarios and conditions. The IS research community, however, has advanced the understanding of the predictors of secure behaviors with more contextualized studies. Still, there are some areas for future development. For example, studying IS actions in contextualized scenarios focused mainly on organizational control and fear appeals. The legitimacy of security policy provisions, captured by the attitudes towards those provisions and the perceptions of others towards those provisions and their association with SP compliance, remains unexplored. Organizational control can be effective to the extent that there is a high control, but this is not the case for most security recommendations. Employees' attitudes towards rules

and regulations can reorient policymaking to emphasize the legitimation and socialization of security recommendations more than control and fear appeals.

Additionally, a fear appeal can be effective to the extent that it is higher than other motivators of action which reveal a conflict in work values. The role of work values relative to specific situations and actions and how these modify the relation between predictors of action and IS action have not been explored. Examining workplace situations where a potential conflict among individual value orientations modifies the association between precursors of IS action and the intention to follow security policy presents an opportunity to expand the IS literature.

2.1.5 Email Use

The review of the literature on the determinants of employees following secure procedures to manage their email accounts reveals six areas of inquiry: (a) persuasion features of forged email, (b) email characteristics that influence response, (c) knowledge as a predictor of precautionary email handling, (d) psychological constructs as determinants of response, (e) integrative approaches, and (f) training to mitigate phishing attacks.

2.1.5.1 Persuasion Features of Forged Emails. The email response literature reveals that socially engineered elements in a forged email influence users to click on links or deliver sensitive information. For example, Downs et al. (2006) found that people were more likely to rely on the text within an email to determine its trustworthiness instead of more objective cues (e.g., URL verification), typically provided in rule-based training commonly found in security policy. Relative to specific elements of persuasion, Williams et al. (2018) found that authority (e.g., respected people or well-known organizations) and urgency (e.g., encouraging quick response) increased the likelihood of response. Other results on the persuasive effect of authority and urgency were reported by Patel et al. (2019). The authors additionally found that the company logo and urgency cues are features that most significantly influence response to a phishing email or spam. Ferreira and Teles (2019) combined Cialdini's (1993) principles of persuasion, Gragg's (2004) psychological triggers behind social engineering, and Stajano and Wilson's (2011) principles for systems security and created a frame to evaluate principles of persuasion on email. The authors analyzed the content of 194 forged emails. Consistent with previous findings, perception of authority and urgency (e.g., the idea that the response or lack of it would bring immediate benefits or harm) were significant determinants of response. Other additional determinants of email response found are the perception of peer response, and ethical self-restriction such as commitment, integrity, and reciprocation (Ferreira & Teles, 2019).

2.1.5.2 Email Characteristics and Workplace. Researchers have also focused on email characteristics such as known or unknown senders as determinants of email response. For instance, Jagatic et al. (2007) found that social context predicts clicking on email links. In their study, two groups

of users received an email with a link to a devious web page. Sixteen percent of users followed the link when the sender was unknown, but 72 percent did so when the sender was a friend or a known company. Further exploring internal and external contextual determinants of response, Williams et al. (2018) conducted six focus groups to explore factors that impact employee susceptibility to spear phishing. Aligned with previous research, these authors found that familiarity determines the response. They also found that expectation (i.e., users know that they are part of a phishing email exercise), workload, and previous exposure to external emails, are determinants of response. User practices, such as centralizing email accounts (including personal) in one email account, can undermine protective technical barriers (Williams et al., 2018). Williams et al. found that job role is a predictor of response and speculated that people with more responsibilities are more likely to receive a spear-phishing attempt. Place of work also plays a role in its impact on attentiveness (e.g., working from home or office) and is a determinant of response. Williams et al. posited that this is because people who work from home deal with other aspects of their lives and might not have implemented the typical protective barriers at work. Another determinant of response is the perception of IT support. Williams et al. suggested that factors that influence response were, for example, user trustworthiness in warnings and banners, the effectiveness of reporting to the IT department, peer verification, information overload (e.g., excessive precautionary warnings), and the perception that training is too frequent or irrelevant.

2.1.5.3 Knowledge as a Determinant of Precautionary Measures. It is intuitive to assume that a user who knows how to detect a forged email would react securely. Researchers have investigated whether this is the case and test whether knowledge determines the response. For example, Downs et al. (2007) examined the effect of knowledge and experience on phishing susceptibility. In their study, participants who knew they were part of a computer usage study but not that the study was about phishing, were shown images of emails addressed by a third party. Some emails were genuine, and some were phishing emails. Participants were asked to choose the action they would take (i.e., reply by email, click on the link, or delete the email). The researchers found that participants who were more knowledgeable and experienced with the internet environment were less susceptible to phishing attacks. In another study, Sheng et al. (2010) investigated the effect of several types of training materials on phishing susceptibility by controlling for demographics. One thousand people participated in the study. The researchers found that women and participants between 18 and 25 years old were more susceptible to phishing. Like Downs et al. (2007), Sheng et al. (2010) found that training material reduced users' tendency to enter information into legitimate and phishing web pages. In a contrasting result, Moody et al. (2017), in their study of victims' personalities and situational constructs as predictors of clicking on email links, found that people with more experience in internet use were more prompt to email a response. The

researchers speculated that it might be because of the influence of past benign experiences performing the same behavior (e.g., clicking on links with no adverse effects) (Moody et al., 2017).

2.1.5.4 Psychosocial Determinants of Response. Training will provide the necessary skills, but even when users know how to detect a deceitful email and the environment favors precautionary behaviors, they still need to form the intention to follow a recommendation, especially considering that social engineering influences users and persuades them to act insecurely. In an early work, Workman et al. (2008), synthesizing theory from marketing research to study factors that account for successful social engineering attacks, found that normative commitment influences people to succumb to socially engineered attempts. This was manifested by the feeling of obligation to reciprocate social engineering gestures (e.g., gift certificates) by giving up sensitive information (e.g., email addresses or identification numbers). The researchers also found that continuance commitment (e.g., continuing the interaction with a distrusting site to win a game or to test the ability to restrain from doing so) and affective commitment (e.g., providing information to feel like part of a group) were predictors of susceptibility to social engineer attempts. A later work (Workman et al., 2008) revealed that trust and obedience were precursors of secure email response. Aligned with Workman et al. (2008), Wright et al. (2014) found that reciprocity with the sender (i.e., the belief that providing the information is the correct social behavior), perception of the sender's authority, and the perception that a good opportunity is present, liking the sender, and habit, were precursors of email response.

With a focus on more proximal determinants of response, Arachchilage and Love (2014) found that the self-evaluation of the ability to gain anti-phishing knowledge (i.e., knowledge search self-efficacy) significantly determined phishing email avoidance motivation and motivation affects response. The researchers also found that procedural and conceptual knowledge did not influence self-efficacy. In another study with a multilevel perspective, Sun et al. (2016) found that internet self-efficacy significantly influenced anti-phishing behaviors and confirmed the mediator effect of anti-phishing self-efficacy. This fact reveals that when users have the knowledge to detect email and if they feel confident in acting using those skills, they reduce the risk of being phished. In contrast, Alain Tambe (2018) found that users fall prey to phishing attacks due to overconfidence (e.g., in one's capabilities or security technology). They also found that trusting dispositions (e.g., individuals with high trusting disposition are more susceptible to phishing), peripheral information processing (e.g., attending to information selectively, often ignoring essential cues that can reveal an email as a phishing attempt), and habit (e.g., clicking regularly on attachments of email) were significant determinants of response.

In line with previous works, Vishwanath et al. (2018) suggested that habitual media use patterns may contribute to the high success of phishing attacks. In this study, the researchers proposed a new construct, cyber-risk beliefs, and explored its influence on deception-detection. Their model encompasses

factors that lead to individual suspicion about phishing emails and their resultant actions. The researchers also investigated the underlying cognitive-behavioral processes in victims of different types of phishing attacks. They found that individuals were likely to fall victim to phishing emails when aspects of the email arouse suspicion. Counterintuitively, Vishwanath et al. found that susceptibility increased when individuals systematically process information (i.e., email characteristics and persuasive elements of the text) rather than heuristically. The information-processing mode that led to suspicion was contingent on cyber-risk beliefs. In addition to influencing cognitive processing, cyber-risk beliefs directly influenced suspicion and habitual patterns of email use. The results suggest that habits—whether risky or secure—influence email handling.

Another construct that has been explored as a precursor of email response is fear. For instance, in an attempt to study its overall impact, Jansen and van Schaik (2019) examined the influence of fear appeal messages on user cognitions (perceived vulnerability, perceived severity, fear, response efficacy, self-efficacy, response costs, attitudes, and attention), and preventive behavior regarding online information-sharing to protect against the threat of phishing attacks. The findings of this study demonstrated the positive effects of fear appeals on heightening end-users‘ cognitions, attitudes, and behavioral intentions.

In an attempt to bring the overall effect of several constructs over precautionary response, similar to Arachchilage and Love (2014), Verkijika (2019) investigated the influence of motivation to avoid a phishing attack and anti-phishing self-efficacy. The study is grounded in Threat avoidance theory (TTAT; Liang & Xue, 2010). TTAT proposes three factors influencing avoidance motivation: safeguard effectiveness, safeguard cost, and self-efficacy towards implementing the safeguard. According to TTAT, and similar to other theoretical propositions (Ajzen, 1991; Fishbein, 1975; Fishbein & Yzer, 2003), avoidance motivation (intention) influenced avoidance (behavior). Verkijika (2019) stated that anti-phishing behavior is influenced by the motivation to avoid a phishing attack, which is influenced by anti-phishing self-efficacy. This author also stated that regret increased the prediction of anti-phishing action. Verkijika found that anti-phishing motivation predicted anti-phishing behavior and that security self-efficacy and anticipated regret predicted anti-phishing motivation.

2.1.5.5 Integrative Approaches. Some researchers have integrated some of the mentioned determinants of actions related to handling their email accounts. For instance, Vishwanath et al. (2011) proposed an integrative model that combines characteristics of emails (e.g., source, grammar and spelling, urgency cues, and subject line) and how individuals process the information as determinants of phishing susceptibility. The level of involvement positively influenced the level of attention to the email characteristics and their cognitive elaboration. The influence of involvement on elaboration was significant. Its influence on attention, however, was significant only for urgency cues and non-significant

for attention to the source, grammar and spelling, and subject line. Vishwanath et al. suggested that the susceptibility to phishing emails increased large email loads. Interestingly, habitual media use patterns (e.g., individuals inattentively responding to emails) accounted for at least one-half of the variance in phishing susceptibility.

Other integrative researchers have examined the impact of email characteristics (e.g., known or unknown sender) on the user's ability to detect illegitimate emails combined with the expectancy effect (Parsons et al., 2015). To manipulate expectancy, the researchers informed half of the participants that the study was about email management (control group) and the other half about anti-phishing behaviors (alerted group). Participants evaluated 50 emails, which consisted of half genuine, half phishing emails. The phishing email was created to influence participants to click on the link by employing three motivators: risk of loss (e.g., the user will suffer financial consequences from not clicking the link), benefit or gain (e.g., the user will be rewarded if following the link), and account information (e.g., the user is directly asked for login information). Participants in the alerted group could better discriminate between phishing and genuine email than the participants in the control group. In addition, alerted respondents invested more time. Informing participants that they were completing a phishing study may have increased diligence and vigilance (Parsons et al., 2015). Respondents were more successful at discriminating email from banking, telecommunication, online retail, government, and academic organizations.

In contrast with Vishwanath et al. (2011), Parsons et al. (2015) found that participants were influenced by their perception of trust towards the email sender. Respondents said they trusted the sender because of its credibility and how the email looks (e.g., appearance, logos, grammatical errors, and personalization). Aligned with Vishwanath et al. (2011), Parsons et al. (2015) found that only a few respondents said that they trust the email for objective measures of authenticity (e.g., the URL or HTTPS checks). Canfield et al. (2016) found contrasting results concerning expectancy. They used signal detection theory (SDT) to focus on vulnerability to phishing attacks. SDT is a means to capture the ability to differentiate between information-bearing patterns and noise (Stanislaw & Todorov, 1999). Canfield et al. (2016) presented a procedure for estimating individual users' sensitivity and response bias for phishing examining performance on detection (i.e., deciding whether an email is legitimate) and behavior (i.e., deciding what to do with the email). They found that participants' behavior almost always reflected appropriate or cautious actions, given their detection beliefs. They also found that participants' response bias is sensitive to the costs of correct and incorrect choices and, in contrast with Parsons et al. (2015), Canfield et al. (2016) found that expectancy was not a determinant of response as all participants assumed roughly the same base rate (i.e., that some emails were forged regardless how many were indeed fake). In contrast with Vishwanath et al. (2011), Canfield et al. (2016) found that the most consistent predictors

were participants' confidence in their detection abilities and their perception of consequences. The authors speculated that a realistic context (less than 1% of received email is forged email in organizations) and the distractions of everyday life could affect detection ability in contrast with an experimental environment. Additionally, the researchers captured self-efficacy and threat perceptions as precursors of detection, but in the experiment, participants were alerted that there were phishing emails, which could have influenced the irrelevance of expectancy in favor of the findings of Parsons et al. (2015).

Other researchers have further investigated characteristics of email combined with psychological predispositions. For instance, Moody et al. (2017) investigated victims' personality and situational constructs as potential precursors of clicking on email links and found five factors that influence secure email use: (a) the source of the email, (b) curiosity, (c) risk propensity, (d) general internet usage, and (e) internet anxiety. Counterintuitively, the researchers found that the more recipients used the Internet, the more likely they were to click on links on unsolicited emails and more likely to fall prey to a phishing attempt if the email comes from a known sender. Additionally, Moody et al. did not find gender and age as statistically significant predictors, contradicting other results (e.g., Sheng et al., 2010; Wright et al., 2014). The last finding supports the speculation from Vishwanath et al. (2011) regarding the effects of habit as a determinant of response.

Other inclusive models combining knowledge, psychological constructs, and contextual elements have been developed. Musuva et al. (2019) explored the antecedents of attitude formation towards threat detection based on the elaboration likelihood model (ELM). The ELM explains ways of processing stimuli, why they are used, and their consequences in attitudinal change (Petty & Cacioppo, 1986). Musuva et al. (2019) explored phishing detection in a university. They studied the extent to which a targeted person will correctly perceive a phishing attack (i.e., detection), its relationship with elaboration, and its influence on phishing susceptibility (clicking on phishing links). In their study, elaboration was considered the extent to which a person cognitively evaluates a phishing message by processing the issue-relevant arguments instead of dismissively glancing at the message because of its peripheral or persuasive cues. The researchers did not alert the population about the specific nature of the study. They also explored the effects of attack quality, motivation to process (involvement, responsibility), ability to process (distractions, emotions, pressure), and knowledge (cue detection). The antecedents of threat detection and elaborations were grounded in Cialdini's (1993) and Petty and Cacioppo's (1986) work on persuasion. The researchers found that three control variables were relevant: job role, email load, and email responsiveness. They also found that faculty and staff were more susceptible to phishing than students. Respondents who received a high email volume were less susceptible to phishing, in contrast with results from Vishwanath et al. (2011). Musuva et al. (2019) found that those who were more responsive to their emails were also more susceptible to responding to phishing emails. Threat detection

accounted for the most substantial effect in reducing phishing susceptibility compared to cognitive processing (i.e., elaboration) - the greater a person's ability to detect a phishing threat, the lower their susceptibility to phishing threats. Cognitive processing of phishing messages neither directly nor significantly affects a person's susceptibility to phishing attacks. Their results also showed that the more a person cognitively evaluates a phishing message, the higher their ability to detect a phishing threat, and subsequently, the less susceptible they are to phishing attacks. The antecedent construct that had the most substantial effect on cognitive processing was the quality of the argument. This means that phishing messages with persuasive arguments are the most effective in encouraging people to process them cognitively. The increased use of persuasive cues in phishing messages reduced threat detection. In addition, the more involved a person was in the subject matter communicated in a phishing attack, the less likely they are to detect the phishing attack. Mediation analysis showed that increased use of persuasive cues and involvement led to higher phishing susceptibility due to a decrease in a person's ability to detect the threat. The antecedent construct that had the highest effect on a person's ability to detect threats was their knowledge of phishing threats and on phishing detection cues. The more knowledgeable participants were, the more likely they were to detect a phishing threat. Mediation analysis showed that threat detection indirectly accounted for people with more knowledge being less susceptible to phishing attacks. A potential limitation of this study is that researchers used one email, and it might be that the text of that email facilitated the results of the study.

Finally, Lawson et al. (2020) combined persuasive principles with psychological predispositions. These authors identified persuasion principles used by social engineering to influence computer users to share personal information in the literature. The principles were (a) commitment/consistency (e.g., complete an action previously initiated), (b) liking the sender (e.g., the trust established by a previous contact), (c) authority, and (d) scarcity (e.g., a short time frame to complete an action). Additionally, Lawson et al. (2020) mentioned that the efficacy of real-world social engineering is modulated by an interaction between the persuasion principle and the victim's personality profile, and they hypothesized that many of the interaction effects in real-world social engineering will also be present in email phishing attacks. Specifically, the authors stated that agreeableness would be predictive of susceptibility to authority, and extroversion will be predictive of susceptibility to liking and scarcity. In addition, they hypothesized that high extroversion would be predictive of overarching susceptibility to phishing emails. High extroversion was confirmed as a predictor of susceptibility to phishing emails. The authors confirmed the interaction effect between the victim's personality and the persuasion element present in the forged email. The liking persuasion principle was considered a determinant of response in phishing and legitimate emails. Conversely, the combination of authority and scarcity persuasion principles was most likely to arouse suspicion in both phishing and legitimate emails. These findings demonstrated

differential response patterns when participants encountered emails utilizing the studied persuasion principles.

2.1.5.6 Techniques to Mitigate Phishing Attacks. As a practical implication of the research presented until this point, researchers have aimed to inform policy implementation in security, education, training, and awareness programs. Authors have investigated the potential positive effects of techniques that help users counteract the persuasion cues in a forged email. For example, Jensen et al. (2017) developed a mindfulness training technique to supplement rule-based instruction to increase awareness and improve judgment in the presence of suspicious messages. These researchers tested the efficacy of their training technique with a posterior simulated phishing attack. They found that respondents that were submitted to this type of training were better able to avoid a phishing attack.

Psychosocial determinants of IS-related behaviors are central in the ISP compliance literature. Researchers in this avenue have evaluated the role of the intention to comply with an ISP or particular provisions of it. In contrast, research on email response has emphasized factors that influence response, such as email characteristics or persuasive elements of the email. Email use research contextualizes more elements than the former ISP compliance research. Employees in the workplace who are victims of phishing emails are not only influenced by the elements of persuasion present in the communication but also by external contextual elements such as conformity with social norms at work (e.g., policy compliance), training, media news, and peer behavior. ISP compliance research has narrowed the focus from security policy compliance (e.g., Bulgurcu et al., 2010) to a more contextualized study of specific behaviors (Aurigemma & Mattson, 2019b). In contrast, email research traditionally includes elements of persuasion present in an email, with psychosocial determinants influenced by the same persuasion elements. There is an opportunity to join these two lines of research investigating determinants of response considering external sources of influence such as training, security policy, concern about privacy and security, and past experiences.

2.2 Theories Supporting IS Behavioral Research

Several theories have been used to predict and explain information security and cybersecurity behaviors (see Cram et al., 2019; Cram et al., 2017; Sommestad & Hallberg, 2013; Sommestad et al., 2014, 2015a, 2015b, 2019). Commonly used behavioral theories include the protection motivation theory (PMT), general deterrence theory (GDT), cognitive theory (CT), rational choice theory (RCT), health belief model (HBM), technology acceptance model (TAM), elaboration likelihood model (ELM), and theory of reasoned Action (TRA) and its subsequent expansions, the theory of planned behavior (TPB) and integrative model (IM).

Protection motivation theory (PMT) predicts an individual's response when facing a threat (Rogers, 1975). According to the theory, three components mediate attitude change: the magnitude of the event's noxiousness, the probability of that event happening, and the efficacy of the protective response. There are numerous applications of PMT in IS research. For example, Anderson and Agarwal (2010) used PMT to study behaviors in individuals motivated to take precautions to secure their computers at home. Boss et al. (2015) investigated what motivates secure behavior to protect information security and individuals' privacy in organizations. Herath and Rao (2009b) explored a new model to study the adoption of information security practices and policies, combining constructs from the PMT and the general deterrence theory (GDT). Johnston and Warkentin (2010) investigated the influence of "fear appeals" on end-users compliance, with recommendations to enact computer security behaviors. Li et al. (2019) tested a conceptual framework that explains employees' information security behaviors in the workplace. Siponen et al. (2014) developed a multi-theory-based model to explain employees' adherence to information security policies (ISP). Workman et al. (2008) used the PMT to support a new threat control model. Their work aimed to understand why people aware of IS security threats and countermeasures neglect to implement them. They tested their model using self-reporting of behavior and samples of observed security behaviors. The researchers combined constructs from the PMT, the theory of reasoned action (TRA), and the cognitive evaluation theory, finding that the intention to complain to the ISP significantly impacts compliance.

General deterrence theory (GDT) originated from criminology and postulates that increasing the certainty, severity, and celerity of punishment deter unwanted behaviors (Blumstein, 1978). Chen et al. (2013) combined the GDT and the compliance theory (CT) to investigate employees' perceptions about implementing an information security policy in organizations. Herath and Rao (2009a) proposed a theory based on GDT, adding normative beliefs. Their study aimed to investigate the incentive effect of penalties, pressures, and perceived effectiveness of employee actions to understand employee compliance with information security policy.

Cognitive theory (CT) was developed by Etzioni (1961) to explain behaviors in organizations. Etzioni (1961) classified organizational behavior into two dimensions: power (with three subdimensions: coercion, utilitarianism, and normative), and involvement (with three subdimensions: alienating, calculative, and moral attitudes). Chen et al. (2013) combined constructs from the CT and GDT and proposed a research model to investigate the relations between coercive control, remunerative control, and certainty of control in the context of information security.

Rational choice theory states that individuals decide rationally from available alternatives, depending on the available information, probability of events, and potential costs and benefits (Becker & Landes, 1974). Han et al. (2017) joined constructs of several theories and other individual constructs to

investigate the mediating effect of a "psychological contract" between the relationship of perceived cost (part of the RCT) and information security policy compliance.

The health belief model (HBM) is based on Atkinson's expectancy-value model (1964). According to this model, attitudes towards a behavior are a function of the perceived likelihood of outcomes associated with the behaviors and the expected value outcomes (Rosenstock, 1974). The HBM identifies two elements in the individual's decision to adopt a healthcare behavior in response to potential illness: perception of illness threat and behavior evaluation to resolve this threat. Ng et al. (2009) studied users' computer security behavior using HBM and found that perceived susceptibility, perceived benefits, and self-efficacy are determinants of users' computer security behavior.

The technology acceptance model (TAM) evaluates the pertinence of two reasons for accepting or rejecting information technology (Davis, 1989). First, people tend to use information technology if they believe it will help them perform their jobs better. This author referred to this cause as "perceived usefulness." Second, users believe that the benefits of using a technology outweigh the effort of using the technology. This author called this reason "perceived ease of use." Shropshire et al. (2015) investigated information security behaviors grounded in TAM and incorporated "perceived organizational support" into their model to predict behavioral intention. The authors also included conscientiousness and agreeableness as moderator variables.

The elaboration likelihood model (ELM) explains ways of processing stimuli, why they are used, and their consequences in attitudinal change (Petty & Cacioppo, 1986). Musuva et al. (2019) implemented the ELM to explore threat detection, the extent to which a person who is targeted will be able to correctly perceive the phishing attack, and elaboration, the extent to which a person cognitively evaluates a phishing message by processing the issue-relevant arguments as opposed to dismissively glancing at the message because of its peripheral (or persuasive) cues, influence phishing susceptibility (i.e., clicking on phishing links).

2.3 Theoretical Background

2.3.1 The Reasoned Action Approach

Fishbein and Ajzen (1977) introduced the reasoned action approach with the theory of reasoned action (TRA). The TRA states that the intention to perform a behavior is a good predictor of performing that behavior and that attitudes toward performing the behavior and social norms relative to it predicts the intention to perform the behavior. Later, Ajzen (1991) introduced the theory of planned behavior (TPB) to capture nonvolitional behaviors (behaviors that are not under people's control). TPB adds to TRA that the prediction of behavior is more accurate if there is knowledge about the control people have to perform the behavior. Since individuals do not know whether they have control to perform a behavior, Ajzen (1991)

proposed perceived behavioral control as a proxy variable of actual control. Perceived behavioral control predicts both the intention to perform a behavior and the performance of the behavior itself. Finally, Fishbein et al. (Fishbein, 2000; Fishbein et al., 2002; Fishbein & Cappella, 2006; Fishbein & Yzer, 2003; Fisher & Fisher, 1992; Institute of Medicine, 2002) proposed the integrative model (IM) to expand TPB. IM, as its predecessors TRA and TPB, posits that the intention to perform a behavior is formed from the person's attitude toward performing the behavior, the perception that others would support the person's adoption of the behavior, the perception of others performing the behavior, and people's perception of their abilities to perform the behavior under various circumstances (self-efficacy/PBC). IM adds that people's beliefs about expectancy, norms, and evaluation of self-abilities and environmental conditions towards performing a behavior are additional predictors of intention (Fishbein, 2000; Fishbein et al., 2002). The reasoned action approach posits that behavior results from a chain of relations that starts in background factors (e.g., demographics, stigma, values, and so on) and ends in the actual behavior. Background factors inform beliefs, which explain the predictors of intention, which, combined with environmental factors, ultimately predict behavior.

There is abundant empirical evidence to support the reasoned action approach (Albarracin et al., 2001; Armitage & Conner, 2001; Bednall et al., 2013; Cohen, 1988; Cooke et al., 2016; Cooke & French, 2008; De Vivo et al., 2016; Fleming et al., 2017; Hagger et al., 2002; Han & Stoel, 2017; McDermott et al., 2015; McEachan et al., 2011; Plotnikoff et al., 2013; Rich et al., 2015; Riebl et al., 2015; Scalco et al., 2017; Sheeran & Taylor, 1999; Starfelt Sutton & White, 2016). The reasoned action approach has been used in numerous domains. Examples include condom use (Albarracin et al., 2001; Sheeran & Taylor, 1999), alcohol consumption (Cooke et al., 2016), cigarette consumption (Topa & Moriano, 2010), treatment adherence (Cooke & French, 2008; Rich et al., 2015), sun-protective behaviors (Starfelt Sutton & White, 2016) (McEachan et al., 2011), exercising and dietary habits (De Vivo et al., 2016; Hagger et al., 2002; McDermott et al., 2015; Plotnikoff et al., 2013; Riebl et al., 2015; Scalco et al., 2017), other health-related behaviors, and socially responsible behaviors (Han & Stoel, 2017), or blood donation (Bednall et al., 2013). There is empirical evidence supporting the predictive validity of TRA/TPB/IM. Multiple meta-analyses (Cooke et al., 2016; Cooke & French, 2008; Hagger et al., 2002; Tyson et al., 2014) have reported medium and large predictive validity for intention and behavior. Prediction is similar in other domains, such as screening programs (Cooke & French, 2008), physical exercise (Hagger et al., 2002), dietary patterns (2015), health-related behaviors (McEachan et al., 2011), chronic illness treatment adherence (Rich et al., 2015), nutrition-related behaviors (Riebl et al., 2015), organic food consumption (Scalco et al., 2017), condom use (Sheeran & Taylor, 1999), sun-protective habits (Starfelt Sutton & White, 2016), cigarette consumption (Topa & Moriano, 2010), and physical activity in adolescents (Plotnikoff et al., 2013).

One element that has received some criticism (Ogden, 2003) is that the reasoned action approach significantly predicts action from predictors relative to the same behavioral object. If the interest is in predicting a specific action, at a particular time, in a certain context, and towards a certain target, then the predictors should be operationalized in the same conditions. The authors of the reasoned action approach call this operationalization the principle of compatibility. The criticisms are in line with the following considerations: (a) how difficult it is to generalize findings from the study of single actions, (b) the possibility that model predictive capability is inflated by methodological bias (Ogden, 2003), and (c) how challenging it would be to inform policy, which should address a myriad of behaviors, from a study focusing on one or only a few behaviors (Albrecht & Carpenter, 1976).

Relative to the discussion of the implementation of the principle of compatibility, Albrecht and Carpenter (1976) discussed two major research traditions in sociology and social psychology. The first is attributed to Melvin L. DeFleur and the second to Martin Fishbein. The principle of compatibility is one of the crucial differences between the two approaches. For the reasoned action approach, intention prediction is from attitudes towards specific circumstances. In contrast, from a sociological view, the attitude-behavior relationship is examined by measuring attitudes towards a general object. The principle of compatibility is neither a necessary nor sufficient condition for predicting action (Fishbein & Ajzen, 2010). The operationalization of the predictors of action can be relative to other behavioral objects related to performing a behavior. Thus, the possibility of predicting the intention of action from a broad definition of attitudes and social norms towards, for example, policy, aligns with the central tenets of both traditions in social sciences. Thus, the association between action and the evaluation of social structures, besides providing theoretical explanations of action with acceptable effect sizes, is informative to practitioners and policymakers.

2.3.2 Individual Value Orientation at Work

Values are abstract motivations that explain attitudes and norms and are drivers for actions (Schwartz, 2003). Individuals assign different importance to some values over others and form a system of values that ground their beliefs and motivate their actions across different situations (Schwartz, 1992). The theory of human values categorizes values into four groups: self-enhancement, self-transcendence, openness to change, and conservation (Schwartz, 1992). Self-enhancement is how individuals look for social status, prestige, and control over people and resources (Schwartz, 2003). Values in this group are power, achievement, and hedonism. Self-transcendence refers to a primary interest in helping and the well-being of others (Schwartz, 2003). Values in this group are universalism and benevolence. Self-enhancement and self-transcendence appear opposite in the theory of human values and form a dimension orthogonal to openness to change and conservation. Openness to change refers to individuals' primary interest in setting their goals, freedom, challenge, and independence in their lives (Schwartz, 2003). The

values in this group are stimulation and self-direction. In opposition, conservation guides actions to maintain the status quo and respect history and traditions (Schwartz, 2003). The values in this group are security, conformity, and tradition.

Consiglio et al. (2017) contextualized the theory of human values in the workplace. In this context, achievement is defined as personal success at work as defined by recognition of one's abilities and products in the organization. Power is defined as social status and prestige in the work setting expressed through leadership roles and influence. Benevolence is defined as devoting oneself to the needs of people with whom one is in frequent work contact and creating harmonious and supportive work relationships. Universalism is defined as fairness, respect, protection against discrimination for all members of the work organization. Security is defined as safety, stability, health, avoiding risks in the work and organizational setting. Tradition is defined as respect, acceptance, and diffusion of organizational traditions, culture, and custom. Conformity is defined as complying and adapting to management expectations and norms, sacrificing personal inclinations to preserve organizational order. Self-direction is defined as independent thought and decision-making, creating, and exploring at work; freedom to choose how to perform one's job. Stimulation is defined as variety, novelty, and challenges in work situations and contexts. Hedonism is defined as pleasure in doing work, compatibility between work and one's recreational and leisure interests. It is logical to assume that individual work values orientation will impact information security in organizations because values are known to drive individuals' actions at work and present an opportunity to expand the state of IS research.

2.4 Theoretical Premise and Hypotheses

2.4.1 Intentions of Not Following Security Recommendations

Intention has been defined as a function to accomplish the desired outcome (Searle, 1983). Intentions indicate how hard people are willing to attempt to perform a behavior or how much effort they are willing to make in that attempt (Ajzen, 1991). Several meta-analyses demonstrate the predictive capability of intention over behavior (e.g., Ajzen & Fishbein, 1973; Sheppard et al., 1988). Intentions have also been found as determinants of IS actions in compliance with security policy (see Cram et al., 2019 for a review). Further evidence has been found for predicting specific behaviors contained in security policy from intentions (Bélanger et al., 2017; Burns & Roberts, 2013; Vafaei-Zadeh et al., 2019), including email response (Verkijika, 2019). The present study investigates the intentions of not following security recommendations as the dependent variable. Table 2.1 shows the definition of constructs in this study.

Table 2.1

Definition of Constructs

Construct	Definition	Source
Negative attitudes relative to the importance of security recommendations	The degree to which the importance of security recommendations is negatively valued.	Reasoned action approach (Fishbein & Ajzen, 2010)
Negative attitudes relative to the completeness of security recommendations	The degree to which the completeness of security recommendations is negatively valued.	
Mildness of security recommendations	The degree to which the severity of security recommendations is negatively valued.	
Negative descriptive norms relative to security recommendations	The employee perception that security recommendations are not followed at work	Reasoned action approach (Fishbein & Ajzen, 2010)
Negative injunctive norms relative to following security recommendations	The employee perception of the favorableness of not following security recommendations.	
No anticipated regret relative to not following security recommendations	The employee lack anticipated feelings of regret relative to not following security recommendations.	Sandberg and Conner (2008)
Intention of not following security recommendations	An employee's intention of not following security recommendations	Reasoned action approach (Fishbein & Ajzen, 2010)

2.4.2 Attitudes Towards Security Recommendations

Attitude is the tendency to respond favorably or unfavorably to a psychological object, concept, or behavior (Albarracin, 2019; Fishbein & Ajzen, 2010; Fiske et al., 2010). Meta-analyses report that attitudes relative to behavioral objects are determinants of intention and action (e.g., Glasman & Albarracín, 2006; Kraus, 1995). Attitude is also a determinant of the intention to perform specific IS actions (Bélanger et al., 2017; Vafaei-Zadeh et al., 2019), category of behaviors (Burns & Roberts, 2013; Siponen et al., 2014), and general ISP compliance (e.g., Bulgurcu et al., 2010; Ifinedo, 2012; Pahnila et al., 2007; Siponen et al., 2014). Several meta-analyses confirm these findings (e.g., Cram et al., 2019).

The IS literature on email response has focused on constructs such as the feeling of commitment to the email originator, obedience (Workman, 2008a), the self-evaluation of the ability to gain anti-phishing knowledge (Arachchilage & Love, 2014), internet self-efficacy (Sun et al., 2016), overconfidence (Alain Tambe, 2018), habit (Vishwanath et al., 2018), fear regarding the potential harm of no response (Jansen & van Schaik, 2019), and anti-phishing self-efficacy (Verkijika, 2019). The attitudinal construct, although a central psychological construct broadly studied in social psychology

(Albarracin, 2019; Eagly, 1993; Fiske et al., 2010), has received little attention in email response research.

Additionally, people's evaluation of a behavioral object can have multiple aspects. Authors (Ajzen, 1991, 2001; Ajzen & Fishbein, 1973; Fishbein & Ajzen, 1977, 2010) have recommended exploring the relevance of the different aspects of attitudes for the behavior of interest before the main study. Current research on attitudes towards IS-related behaviors captures the attitudinal construct typically with items that ask for general evaluation (e.g., good-bad); however, the evaluative aspect of attitudes toward an attitudinal object is typically reflected in two sub-factors, instrumental and experiential (Fishbein & Ajzen, 2010). The instrumental aspect of attitude is a cognitive evaluation of the need of the attitudinal object and is captured with dimensions such as *necessary – unnecessary* (Fishbein & Ajzen, 2010). The experiential aspect involves the affective evaluation of the attitudinal object based on the experience concerning that object and involves dimensions such as *complete – uncomplete* or *pleasant – unpleasant* (Fishbein & Ajzen, 2010). These two dimensions of attitudes are evaluative (Osgood, 1957). Scholars have studied the instrumental aspect of attitudes towards IS, including action and policy compliance. It follows that a multidimensional negative evaluation of specific security recommendations will impact the intention of not following them. The more unimportant (instrumental aspect) and unnecessary (experiential aspect) employees think security recommendations are, the stronger the intention of not following security recommendations. Based on this rationale, the researcher developed the following hypotheses:

Hypothesis 1: The negative attitudes toward the importance of security recommendations are positively associated with the intention of not following them (Instrumental aspect of attitudes).

Hypothesis 2: The negative attitudes toward the completeness of security recommendations are positively associated with the intention of not following them (Experiential aspect of attitudes).

Potency and activity are other aspects besides instrumental and experiential aspects of the attitudes towards a behavioral object (Osgood, 1957). The potency aspect involves terms such as *hard-soft*, whereas the activity aspect involves terms such as *active – passive*. Ajzen and Driver (1991) found that the items formulated to capture the potency and activity loaded into the experiential aspect of attitudes. The type of action and context changed the relevant aspects of attitudes, and exploration with a pool of items is recommended (Fishbein & Ajzen, 2010). The relevance of the potency aspect of attitudes toward security recommendations seems particularly interesting for security policy compliance research. The literature relative to IS action ostensibly relies on deterrence theory. It follows that employees perceiving security recommendations as mild or not strict will impact the intention of not following those recommendations. The milder security recommendations are perceived, the stronger the intention of not following security recommendations. Based on this rationale, the researcher hypothesized:

Hypothesis 3: The mildness of severity of security recommendations is positively associated with the intention of not following them (Potency aspect of attitudes).

2.4.3 Subjective Norms Relative to Security Recommendations

Social norms dictate acceptable behavior in a group or society (Bandura, 1977; Cialdini, 1993; Fishbein & Ajzen, 2010). Subjective norms refer to the perception of social norms around the performance of a behavior (Fishbein & Ajzen, 1977, 2010). The stronger subjective norms about a behavioral object, the more likely the intention to perform the behavior (Ajzen, 1991; Fishbein, 1975; Fishbein & Ajzen, 2010). Subjective norms include two constructs: descriptive and injunctive norms (Fishbein & Ajzen, 2010). Descriptive norms are a person's perceptions about how others important to the individual would behave, whereas injunctive norms are people's perceptions of what important others think of them performing a behavior. Both factors can coexist regarding one specific behavior and be congruent or contradictory (Fishbein & Ajzen, 2010).

In the study of IS-related behavior, subjective norms and their associated normative beliefs, at the highest level of generality, predict the intention to comply with ISP (Ifinedo, 2012). Subjective norms have also been found as a determinant of intention and actual performance of categories of IS behaviors such as following standard security rules (e.g., locking office doors, turning off PCs at the end of the workday, using appropriate passwords) (Siponen et al., 2014), overall cautiousness (e.g., reading license agreements and privacy policies on websites before registering on them) (Anderson & Agarwal, 2010; Burns & Roberts, 2013; Jansen, 2017), and online technology knowledge (e.g., using pop-up window blockers, implementing firewalls and other internet security programs, and regularly checking the computer for spyware) (Burns & Roberts, 2013).

Previous researchers have shown that social norms can drive people to fall for socially engineered forged emails (Workman, 2008a, 2008b), but the social norms in this area of research focus on the norms towards the email sender (i.e., a feeling of obligation to answer to the company or the originator of the forged email). Scholars have explored the persuasive effect of authority cues as determinants of response - for example, the use of company logos or the name of a well-known personality. In contrast, and similar to the attitudinal construct, the literature on IS policy compliance emphasizes a higher level of abstraction. It considers social norms as the social obligation to comply with peers, for example, to comply with an ISP. When employees manage their email account and encounter a forged email, the social norms are those influenced by the text of the email but also the social norm of complying with their supervisor, management, security officer, the IT help desk, peers, knowledgeable colleagues, a friend, security policies, and outside sources of influence such as news, social media, friends outside work, or an IT specialist. IS researchers have revealed that other sources of influence decrease or reinforce the influence of authority cues present in a forged email and rule-based training. For example, an email from

the security officer that alerts of potential threats might represent a more important figure of authority than a company logo. Scholars have shown that cues of authority positively influence uses to avoid responding to forged emails because they make respondents suspicious. Other people—not necessarily figures of authority—influence decisions, and people might be more likely to refer to them when seeking security advice. An unfavorable evaluation of subjective norms relative to security recommendations will impact the intention of not following those recommendations. The stronger the negative descriptive norms relative to security recommendations, the less likely employees will be to follow those recommendations. Equally, the more favorable employees think that peers will judge an action that does not follow security recommendations, the less likely that employees will follow these recommendations. Based on this rationale, the researcher hypothesized that:

> **Hypothesis 4:** The negative descriptive norms relative to security recommendations are positively associated with the intention of not following them.
>
> **Hypothesis 5:** The negative injunctive norms relative to following security recommendations are positively associated with the intention of not following them.

2.4.4 Anticipated Regret (AR) Relative to Not Following Security Recommendations

There is evidence suggesting that human behavior is better understood if the affective component is considered (Abelson et al., 1982; Eagly, 1993). The affective component can be evaluated in terms of temporality (i.e., present or future). Authors have argued that the present affective evaluation differs from the attitudinal factor (Abelson et al., 1982). A semantic evaluation of attitudes includes the current affective evaluation (Ajzen, 2011). In contrast, anticipated affect predicts future emotions (Ferrer et al., 2015) associated with the outcome of future action. This prediction can have a positive or negative evaluation. The IS-related behavioral literature has focused on the negative evaluation (i.e., anticipated regret) (Sommestad et al., 2014, 2015a, 2019). Anticipated regret has been defined as an emotional outcome that people strive to avoid (Janis, 1977). Sandberg and Conner (2008) defined this as a cognitive-based emotion experienced when people realize or imagine that the situation could have been better had they acted differently. Meta-analysis confirms anticipated regret as a determinant of IS/CS intention-behaviors (e.g., Sandberg & Conner, 2008). Sommestad et al. (2015b) found that anticipated regret explains an additional 3% of variance over and above the attitudinal factor as a determinant of security policy compliance.

One challenging aspect of IS-related research is that the consequences of an insecure action are not immediately evident. For example, when responding to a forged email, the respondent might not immediately suffer consequences. These consequences will be perceived later with a report about irregular banking account movement, unusual behaviors of portions of a process (e.g., changes in valves or pump parameters), or ransomware attacking the company (e.g., Colonial Pipeline). The IS research

does not investigate the association of current actions with future consequences for users or the public good (Weber, 2017). The email response literature explores the role of anticipated effect but only towards deceitful cues of action (e.g., click an email to avoid harm). There is an opportunity to explore the role of anticipated regret on email response considering workplace contexts.

Some authors have argued that anticipated regret is implicit in the attitudinal construct (Fishbein & Ajzen, 2010). Others have posited that the affective component is a significant determinant of decisions in addition to attitudes and norms for volitional behaviors (Eagly, 1993). Additionally, anticipated regret has been found as an additional predictor of intention to perform IS-related actions (Sommestad & Hallberg, 2013; Sommestad et al., 2014, 2015a, 2015b, 2019) and specifically email response (Verkijika, 2019). It follows that the lack of anticipated regret relative to not following security recommendations will impact the intention of not following them. The stronger the no anticipated feelings of regret relative to not following security recommendations, the stronger the intention of not following those recommendations. Based on this rationale, the researcher developed the following hypothesis:

Hypothesis 6: The no anticipated regret relative to not following security recommendations is positively associated with the intention of not following them.

2.4.5 The Role of Individual Value Orientation at Work

Values are distant precursors of action (Fishbein & Ajzen, 2010). Security policy aims to guide actions concerning information confidentiality, integrity, and availability. It follows that values at work guide actions in compliance with security policy. The taxonomy of basic human values defines four basic orientations of action: self-enhancement, self-transcendence, openness to change, and conservation (Schwartz, 1992). Different values form each dimension. The self-enhancement dimension is formed by power, achievement, and hedonistic value orientation. Self-transcendence is formed by universalism and benevolence. Openness to change is formed by stimulation and self-direction. Finally, the conservationism dimension is formed by security, conformity, and tradition.

The value orientation can supplement the interpretation of the predictors of IS action. In this exploratory study, the researcher proposed that work values moderate the relation between the negative evaluation of formal and informal norms and the intention of not following security recommendations. The role of benevolence, self-direction, power, and achievement was examined. Benevolence was considered because this value orientation is close to security and conformity in the taxonomy of basic human values. A situation that enacts benevolence was considered as a baseline. The other three value orientations do not provide a complete representation of the rest of the basic human values; still, they are a starting point to study their role in organizations relative to security compliance.

Interventions implement programs that focus on motivating secure actions that conform with formal norms. If an intervention is considered successful, the employee value orientation at work will

lean towards conservationism, but if the organizational culture reflects and influences a distinct value orientation, the actions will follow that orientation. The context where the action takes place helps reveal the value orientation. According to the theory of basic human values, actions follow a value orientation that seems the most important for individuals in specific situations and relative to specific actions (Schwartz, 1992). Action is driven by the most important value orientation, but other value orientations play a role. For example, following a formal norm that was made to protect the security of information at work reflects a security value orientation to the extent that the employee thinks that violating such a norm will endanger the security of his company and employees, but it also reflects a value orientation toward conforming to rules and regulations. In contrast, if companies intervene to bring awareness about the security of information and employees' actions violate formal norms, then these actions that oppose conformity and security align with achievement, power, or self-direction if the culture favors this value orientation. It follows that in situations that enact power, achievement, and self-direction, these values drive IS action and predict not following security recommendations making the negative evaluation of them irrelevant in the prediction of not following security recommendations. In situations that enact benevolence, the negative evaluation of formal and informal norms impacts the intention of not following security recommendations. Based on this rationale, the following hypotheses were developed:

Hypothesis 7.1: The association between negative attitudes toward the importance of security recommendations with the intention of not following them is weaker in situations that enact power, self-direction, and achievement than in situations that enact benevolence.

Hypothesis 7.2: The negative association between attitudes toward the completeness of security recommendations with the intention of not following them is weaker in situations that enact power, self-direction, and achievement than in situations that enact benevolence.

Hypothesis 7.3: The association between mildness of security recommendations with the intention of not following them is weaker in situations that enact power, self-direction, and achievement than in situations that enact benevolence.

Hypothesis 7.4: The association between negative descriptive norms relative to security recommendations with the intention of not following them is weaker in situations that enact power, self-direction, and achievement than in situations that enact benevolence.

Hypothesis 7.5: The association between negative injunctive norms relative to following security recommendations with the intention of not following them is weaker in situations that enact power, self-direction, and achievement than in situations that enact benevolence.

Hypothesis 7.6: The association between no anticipated regret relative to not following security recommendations with the intention of not following them is weaker in situations that enact power, self-direction, and achievement than in situations that enact benevolence.

2.4.6 The Role of Secure Systems

Some organizations have the capability, or the willingness, to put in place systems to help employees perform their tasks in compliance with security recommendations and regulations. Specifically relative to sharing personal information, if this is necessary, organizations have systems such as secure internal webpages. The use of secure systems acts as a safeguard that minimizes the risks of sharing personal information by other means (e.g., email). The safeguard effectiveness is a precursor of the motivation to avoid risks (Liang & Xue, 2010). With supporting systems aiming to minimize risks, the decision of not following security recommendations (e.g., avoid sending personal information by email or using secure webpages for it) is influenced by a negative evaluation of the safeguard effectiveness. safeguard costs, the perception that implementing such a safeguard will have a cost higher than the perceived benefits of implementing, negatively affect the intention to avoid risks (Liang & Xue, 2010). It follows that the inexistence of secure systems motivates a negative evaluation of security recommendations considering them unproductive or incomplete and impacts the intention of not following them. Based on this rationale, the following hypotheses were posed:

Hypothesis 8.1: The association between the negative attitudes toward the importance of security recommendations and the intention of not following them is weaker for employees who do not have secure systems at work than for those who do.

Hypothesis 8.2: The association between the negative attitudes toward the completeness of security recommendations with the intention of not following them is weaker for employees who do not have secure systems at work than for those who do.

Hypothesis 8.3: The association between the mildness of security recommendations and the intention of not following them is weaker for employees who do not have secure systems at work than those who do.

Hypothesis 8.4: The association between the negative descriptive norms relative to security recommendations with the intention of not following them is weaker for employees who do not have secure systems at work than those who do.

Hypothesis 8.5: The association between the negative injunctive norms relative to following security recommendations with the intention of not following them is weaker for employees who do not have secure systems at work than those who do.

Hypothesis 8.6: The association between no anticipated regret relative to not following security recommendations and the intention of not following them is weaker for employees who do not have secure systems at work than for those that do.

2.4.7 The Role of Email Monitoring

Administrative control has been found to be a predictor of IS actions (Spitzmüller & Stanton, 2006). Employees accept monitoring, to the extent that it does not affect privacy and there is an adequate justification of its implementation (Zweig & Webster, 2002). Scholars have argued that employee's evaluation of formal and informal norms relative to what the organization recommends in terms of information security will be affected by the awareness that they are monitored. Thus, the evaluation of norms and the perception of being monitored interact and jointly affect the intention of following security recommendations. It follows that monitoring will negatively impact the association between the negative evaluation of formal norms and the intention of not following security recommendations. Based on this rationale, the researcher hypothesized:

Hypothesis 9.1: The association between negative attitudes towards the importance of security recommendations and the intention of not following them is weaker for employees whose organizations monitor their email accounts than for those that do not.

Hypothesis 9.2: The association between negative attitudes towards the completeness of security recommendations and the intention of not following them is weaker for employees whose organizations monitor their email accounts than for those that do not.

Hypothesis 9.3: The association between the mildness of security recommendations and the intention of not following them is weaker for employees whose organizations monitor their email accounts than those that do not.

Hypothesis 9.4: The association between negative descriptive norms relative to security recommendations with the intention of not following them is weaker for employees whose organizations monitor their email accounts than for those that do not.

Hypothesis 9.5: The association between negative injunctive norms relative to following security recommendations with the intention of not following them is weaker for employees whose organizations monitor their email accounts than for those that do not.

Hypothesis 9.6: The association between no anticipated regret relative to not following security recommendations and the intention of not following them is weaker for employees whose organizations monitor their email accounts than for those that do not.

2.4.9 Demographics

Several demographics play a role in the prediction of IS action (e.g., Lowry & Moody, 2013; Parsons et al., 2014). To complement the results, the role of age, gender, education level, work experience, organizational size, and job level were examined. Table 2.2 summarizes the hypotheses in this study, and Figure 1 shows the conceptual model that guided its execution.

Table 2.2

Hypotheses Summary

ID	Hypotheses
H1	Negative attitudes toward the importance of security recommendations are positively associated with the intention of not following them (Instrumental aspect of attitudes).
H2	Negative attitudes toward the completeness of security recommendations are positively associated with the intention of not following them (Experiential aspect of attitudes).
H3	Mildness of security recommendations is positively associated with the intention of not following them (Experiential aspect of attitudes).
H4	Negative descriptive norms relative to security recommendations are positively associated with the intention of not following them.
H5	Negative injunctive norms relative to following security recommendations are positively associated with the intention of not following them.
H6	No anticipated regret relative to not following security recommendations is positively associated with the intention of not following them.
H7.1-H7.6	The association between the negative evaluation of formal and informal norms with the intention of not following security recommendations is weaker in situations that reflect value orientation towards power, achievement, and self-direction in contrast with situations that reflect benevolence.
H8.1-H8.6	The association between the evaluation of formal and informal norms with the intention of not following security recommendations is weaker for employees that do not have security systems in place than for those that do.
H9.1-H9.6	The association between the evaluation of formal and informal norms with the intention of not following security recommendations is weaker for employees whose organizations monitor their email accounts than those that do not.
H10.1-H10.6	Differences in age, gender, education level, work experience, organizational size, and job level impact the intention of not following security recommendations and influence the relations between the negative evaluation of formal and informal norms and the intention of not following security recommendations.

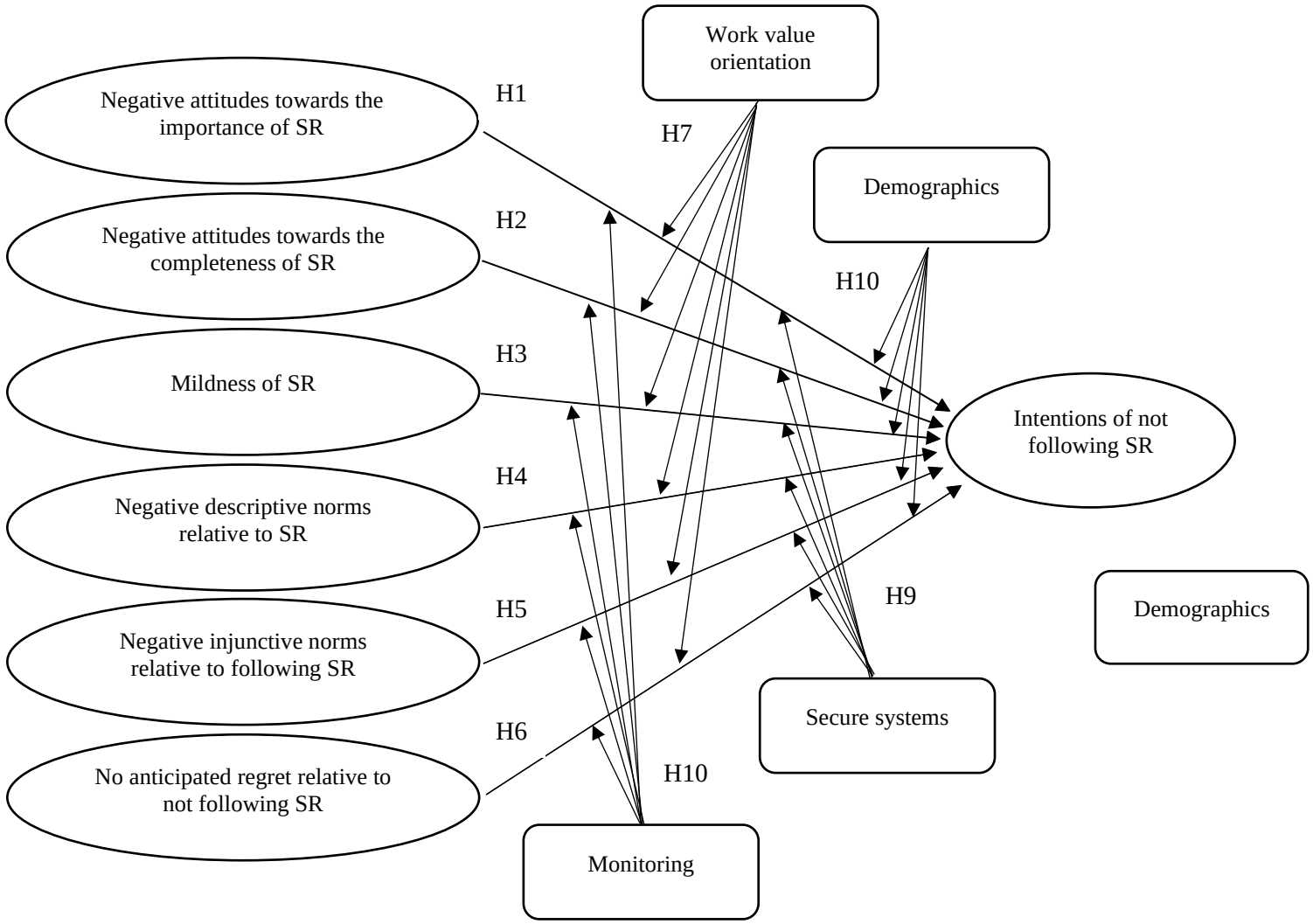


Figure 1: Conceptual Model

CHAPTER 3
METHODOLOGY

In this study, the researcher investigated the negative evaluation of formal and informal norms as precursors of not following security recommendations at work. Several scenarios and questions (items) were developed to test the hypotheses and answer the research questions. The scenarios presented a character that failed to follow security recommendations, and the items captured the variables involved in the hypotheses. The Old Dominion University Institutional Review Board approved the research protocol. Participants provided their written informed consent. The study was carried out in three stages. In Stage 1, the scenarios and items were developed and pretested; in Stage 2, the internal structure of the measurement model was explored; in Stage 3, the measurement model was confirmed, and the hypotheses were examined. The researcher recruited a total of four samples from participants recruited from two online panels, Amazon Mechanical Turk and Qualtrics. The data were submitted to several analyses to ensure the appropriateness of the materials, to assess the measurement model's validity, and to provide evidence to examine the hypotheses and answer the research questions. Table 3.1 presents a summary of the methodology with details for each stage. The following sections define the target population and describe the selected methodology in detail. Preliminary results are also presented, leaving the final results for Chapter 4.

Table 3.1

Research Methodology

Research stage	Purpose	Data point	Activities	Analysis	Outcome
Stage 1: Scenarios and items development and pretesting	Develop and test realistic scenarios that enact the intended value orientation.	First data collection n=51	Scenario development and analysis	Means comparison	Realistic scenarios.
	Develop items that capture the variables in this study.	Second data collection n=560 (distributed in three pilot studies)	Item formulation and check	Wording clarity, survey flow, and social desirability	List of 36 items
Stage 2: Factor exploration	Exploring the internal structure of the measurement model.	Third data collection n=2524 (705 valid)	Survey administration and analyses.	1) Exploratory factor analysis (EFA) 2) Convergent and discriminant analysis with external scale	Evidence of internal structure and validity relative to an external scale.
Stage 3: Confirmatory study and hypotheses evaluation	Confirm and validate the measurement model and evaluate the hypotheses in this study.	Fourth data collection n=5611 (661 valid)	Survey administration and analyses.	1) Reliability and validity analyses (internal structure)	Internal structure confirmed.
				2) Confirmatory factor analyses	Measurement model confirmed for each sample.
				3)Factorial invariance analyses	Measurement model invariant across samples.
				4) Structural equation analysis	Hypotheses H1 – H6 examined
				5) Structural invariance	Hypotheses H7 – H10 examined

3.1 Population

The target population included adults working in the United States that use an organizational email account. The study was at a national level and considered several demographic groups. All data were collected from participants with the same characteristics as the population of interest. The final data were obtained using quotas based on age, gender, and level of education according to the last report of the U.S. Bureau of Labor Statistics (2021; Table 3.2).

Table 3.2

Statistics of the Employed Labor Force in the U.S. (U.S. Bureau of Labor Statistics, 2021)

Age	Percentage
18 – 24	9%
25 – 34	23%
35 – 44	22%
45 – 54	21%
55 – 64	18%
65 and over	7%
Gender	**Percentage**
Male	53%
Female	47%
Level of education	**Percentage**
Less than a high school diploma	6%
High school graduates, no college	25%
Some college, no degree	14%
Associate degree	11%
Bachelor's degree only	27%
Advanced degree	17%

3.2 Scenarios and Items Development

3.2.1 Scenario Development and Evaluation

Several scenarios were developed based on the IS literature. The scenarios had two main pieces; (a) to specify security policy provisions and (b) to depict a character that acted against those provisions. Then, the scenarios portrayed a character with one of several value orientations at work, emailing personal information in response to a colleague at work. The scenarios were formulated using the definitions of basic human values (Schwartz, 1992, 2003) and items that capture values at work

(Consiglio et al., 2017). More specifically, the scenarios provided the following information: (a) sharing personal information by email is not recommended, as it could lead to a security incident; (b) some organizations have systems in place that allow employees to enter and share personal information; and (c) due to lack of resources or privacy concerns, it is difficult for organizations to monitor whether employees email personal information or use secure systems.

An initial pool of scenarios was formulated combining three dimensions: action, work value, and sender. Action specifies the action taken by the character in the scenario. The options were: emailing personal information or clicking on links/attachments. Work value specifies a specific work value enacted in the scenario. The options were (a) authority (power), (b) ambition (achievement), (c) enjoyment (hedonism), (d) variety (stimulation), (e) autonomy (self-direction), (f) social justice (universalism), (g) environmental sustainability (universalism), (h) helping and supporting (benevolence), (i) rule respecting (conformity), (j) traditional values (tradition), and (k) safety (security; parentheses indicate the denominations of values by Schwartz, 2003). The sender specifies the person with whom the character in the scenario interacts, of which the options were colleagues, supervisors, and managers. After eliminating unrealistic situations, 11 scenarios were chosen for further refinement. These scenarios focused on emailing personal information and four work values: power, achievement, self-direction, and benevolence.

The 11 scenarios were submitted to a realism check. The scenarios were presented to 51 participants recruited from Amazon Mechanical Turk (MTurk). The participants were asked to evaluate the realism of the scenario on a four-points scale from *realistic* (1) to *unrealistic* (4). Table 3.3 shows the mean and standard deviation of realism measurement for each scenario. Overall, all the scenarios were rated as *realistic* or *moderately realistic*. Participants that considered that the scenarios were *unrealistic* were asked how they would improve the scenarios. The suggestions were incorporated for the next examination. Here, items that capture the hypothesized precursors of intention to follow security recommendations were formulated relative to each scenario. The sample and the number of items to evaluate all scenarios were considered untenable. Therefore, only the scenarios focusing on “colleagues” as the person with whom the character in the scenario interacts were retained. One more scenario was added, considering power as a work value orientation. All scenarios had the same structure and were used as part of the materials for the next stages of this study.

Table 3.3

Scenario Realism Check Results

Scenario Nr.	Work value	Person or group to whom the character in the scenario interacts.	*M* (*SD*)
1	Authority (Power)	Supervisor	1.92 (0.80)
2	Authority (Power)	Management	1.80 (0.78)
3	Ambition (Achievement)	Colleagues	1.90 (0.86)
4	Ambition (Achievement)	Supervisor	1.88 (0.77)
5	Ambition (Achievement)	Management	1.84 (0.89)
6	Autonomy (Self-direction)	Colleague	2.18 (0.94)
7	Autonomy (Self-direction)	Supervisor	2.10 (0.86)
8	Autonomy (Self-direction)	Management	1.98 (0.94)
9	Helping and supporting (Benevolence)	Colleague	1.64 (0.78)
10	Helping and supporting (Benevolence)	Supervisor	1.64 (0.69)
11	Helping and supporting (Benevolence)	Management	1.68 (0.74)

Note. M: mean, *SD*: Standard deviation.
The scenarios were rated on a 1–4 scale from *realistic* (1) to *unrealistic* (4)

3.2.2 Items' Formulation

Based on the definition of the variables in the hypothesized model, 36 questions (items) were formulated. Table 3.4 shows the variables' operational definitions. The items that capture negative attitudes towards the importance of security recommendations asked participants whether security recommendations in terms of handling personal information online in their organizations are important, necessary, and other similar terms. The items were scored using a 5-point Likert-type scale from *strongly agree* (1) to *strongly disagree* (5). A high score indicates that participants think that security recommendations in their organizations are unimportant. The items that captured the negative attitudes towards the completeness of security recommendations asked participants whether security recommendations in terms of handling personal information online in their organizations are complete, sufficient, and other similar terms. The items were scored on a 5-point Likert-type scale from *strongly agree* (1) to *strongly disagree* (5). A high score indicates that participants think that security recommendations in their organizations are incomplete.

Table 3.4

Variables' Operational Definition

Construct	Definition	Example (score)	Interpretation
Negative attitudes relative to the importance of security recommendations	The degree to which the importance of security recommendations is negatively valued.	The recommendations my organization has in terms of handling personal information online are important. (Strongly agree (1) to strongly disagree (5))	A high score indicates that participants think that security recommendations in their organizations are unimportant or unnecessary.
Negative attitudes relative to the completeness of security recommendations	The degree to which the completeness of security recommendations is negatively valued.	The recommendations my organization has in terms of handling personal information online are complete. (Strongly agree (1) to strongly disagree (5))	A high score indicates that participants think that security recommendations in their organizations are incomplete.
Mildness of security recommendations	The degree to which the severity of security recommendations is negatively valued.	The recommendations my organization has in terms of handling personal information online are severe. (Strongly agree (1) to strongly disagree (5))	A high score indicates that participants think that security recommendations in their organizations are soft and mild.
Negative descriptive norms relative to security recommendations	The employee perception that security recommendations are not followed at work	People at my work observe recommendations in terms of handling personal information. (Strongly agree (1) to strongly disagree (5))	A high score means that participants think that others at work do not follow security recommendations.
Negative injunctive norms relative to following security recommendations	The employee perception of the favorableness of not following security recommendations.	How would people at your workplace be about John's* decision? (Strongly unfavorable (1) to strongly favorable (5))	A high score means that participants think that others at work would favorably evaluate not following security recommendations.
No anticipated regret relative to not following security recommendations	The employee lack anticipated feelings of regret relative to not following security recommendations.	If you would have decided like John, answer whether the following statement is true to you. "Things would have gone better if I had chosen another option to respond to the request from my colleague." (Strongly agree (1) to strongly disagree (5))	A high score means that the participants will not have feelings of regret if they would not follow security recommendations.
Intention of not following security recommendations	An employee's intention of not following security recommendations	I intend not to do as John did in similar situations. (Strongly agree (1) to strongly disagree (5))	A high score indicates the participant's intention to email personal information in the future as the character did, failing to follow security recommendations.

Note. *John is the character in the scenario. John emailed personal information.

The items that capture the mildness of security recommendations asked participants whether security recommendations in terms of handling personal information online in their organizations are hard, severe, and other terms. The items were scored on a 5-point Likert-type scale from *strongly agree* (1) to *strongly disagree* (5). A high score indicates that participants think that security recommendations in their organizations are soft and mild. The anchors the items that capture attitudes were based on the work of Osgood (1957). The items that captured the negative descriptive norms centered on participants' perceptions about others at work following security recommendations. The items were scored on a 5-point Likert-type scale from *strongly agree* (1) to *strongly disagree* (5). A high score means that participants think that others at work do not follow security recommendations. The items that captured the negative injunctive norms relative to following security recommendations asked participants how favorably they think other people at work would evaluate the action performed by the character in the scenario. The items were scored on a 5-point Likert-type scale from *strongly unfavorable* (1) to *strongly favorable* (5). A high score means that participants think that others at work would favorably evaluate not following security recommendations. The items that captured the no anticipated regret were based on the work of Buchanan et al. (2016). The items were modified to capture whether participants do not have feelings of regret if they were to act like the character in the scenario. The items were scored on a 5-point Likert-type scale from *strongly agree* (1) to *strongly disagree* (5). A high score means that the participants will not have feelings of regret if they did not follow security recommendations. The items that capture the intention to not follow security recommendations asked participants about their willingness of acting in the future as the character in scenarios failed to follow security recommendations and proceeded to email personal information at work. The items were scored on a 5-point Likert-type scale from *strongly agree* (1) to *strongly disagree* (5). A high score indicates intention to email personal information in the future as the character did, failing to follow security recommendations. The items that captured factors that refer to action (injunctive norms, anticipated regret, and intentions) were worded by asking respondents their perception of the character's action. These items were worded in this way to reduce social desirability following recommendations from ethics at work research (Trevino, 1992) and IS research (Siponen & Vance, 2014).

3.2.3 Survey Pretesting

Three consecutive samples ($n1 = 80$, $n2 = 80$, and $n3 = 400$) were collected to examine survey flow, items' social desirability, participants' memory and attention checks, and preliminary evidence of internal structure. Participants were recruited from Amazon Mechanical Turk (MTurk). Participants completed the survey in exchange for payment. The survey included (a) one of the scenarios developed previously; (b) the items that capture the variables in this study (security recommendations [SR] scale); (c) a social desirability scale (Hays et al., 1989) with five items scored from *definitely true* (1) to

definitely false (5); (d) several attention and memory checks; and (e) a demographic questionnaire. The social desirability scale was presented first, and then the SR scale. The items in the SR scale were presented in random order to prevent the ordering effect (Podsakoff et al., 2012). The attention and memory checks were presented randomly throughout the SR scale. The survey was administered via Qualtrics.

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."*

The scenario then describes a character with a benevolent value orientation at work that, in response to a colleague, proceeds to email personal information. This part of the scenario reads,

> *"John works at a manufacturing company. People at work believe he is a very supportive co-worker, always willing to help. John receives an email asking for some personal information from a colleague, and John, out of professional courtesy, decided to email the required information."*

At the end of the survey pretest, the correlation between the items and the composite score of the social desirability scale was weak for the most part, indicating that the item rewording was effective at reducing social desirability. The memory and attention checks detected poor quality responses and were deemed appropriate. After every pilot, the internal structure was preliminarily examined to guide item rewording and refinement. The final list of 36 improved items was used in the next factor exploration.

3.3 Factor Exploration

3.3.1 Participants

A new sample was collected for factor exploration. Participants were recruited from Amazon Mechanical Turk (MTurk). A total of 2,524 respondents attempted to submit the survey. After discarding responses that failed attention, memory, or participation check (unemployed or people who do not use an organizational email account), 307 males and 462 females ages 18 to 85 years were retained. Participants completed the survey in one of the following scenarios: 203 for Scenario 1, 208 for Scenario 2, 176 for Scenario 3, and 187 for Scenario 4. The scale with the most items was the evaluative attitudinal scale with 13 items. For a ratio of 10 responses per variable, a total of 130 respondents was necessary (Nunnally, 1994). Thus, the sample collected was considered appropriate.

3.3.2 Measures

The survey included four parts: the SR scale, items for participation and attention checks, a social desirability scale (Hays et al., 1989), a scale to test for convergent and discriminant validity (Williams's scale; Williams & Joinson, 2020), and a demographic questionnaire.

3.3.3 Protocol

The survey was presented to each respondent with the following introduction:

"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, one of the following scenarios was presented randomly to each respondent:

Scenario 1 (Sc1). *"John works at a manufacturing company. People at work believe he values having authority over people and resources, and he is always looking for opportunities to determine how those resources should be used. John receives an email asking for some personal information from his supervisor, and John, seeing this event as a possible opportunity for him to gain status at his company, decided to email the required information."*

Scenario 2 (Sc2). *"John works at a manufacturing company. People at work believe he is a very competent coworker, always wanting to perform well at what he does at work. John receives an email from someone at work asking to email some personal information as part of a task, and John, wanting to perform as efficiently as he normally does, decided to accomplish the task as required."*

Scenario 3 (Sc3). *"John works at a manufacturing company. People at work believe he is the type of person that likes to make his own decisions regarding work tasks, always wanting to determine how he organizes and executes them. John receives a request to share some personal information from someone at work. He figured that the best way to attend to this request was emailing the requested information, and he did."*

Scenario 4 (Sc4). *"John works at a manufacturing company. People at work believe he is a very supportive coworker, always willing to help. John receives an email asking for some personal information from a colleague, and John, out of professional courtesy, decided to email the required information."*

After the scenario, the SR scale, the social desirability scale, and Williams's scale (Williams & Joinson, 2020) were administered. The social desirability scale was presented first; then, the SR scale and Williams' scale were presented in random order. Participants answered the questions in random order.

3.3.4 Data Checking

The data were examined using RStudio software to identify missing data, of which there were none (RStudio Team, 2020). The Mahalanobis distance was calculated for each score and compared with a cutoff calculated with the chi-square value corresponding to 36 degrees of freedom (the number of items) and an alpha = 0.001 as recommended (Tabachnick, 2001). A score with a Mahalanobis distance bigger than the cutoff was deemed as an outlier. Sixty-nine outliers with Mahalanobis distance bigger than a chi-square value were removed, leaving 705 valid respondents; 182 correspond to scenario 01, 189 to Scenario 2, 159 to Scenario 3, and 175 to Scenario 4. The most numerous scale is the evaluative factor of attitudes (13 items) for this scale, and considering the less numerous sample (159), the ratio was 12 cases per variable, exceeding the recommended 10:1 ratio (Nunnally, 1994). The multivariate normality, linearity, and homogeneity assumptions were examined with no evidence of strong nonnormality.

3.3.5 Factor Analysis

A factor analysis was used to examine the factor structure of the 36 items and all scenarios. Factors were extracted using principal factor solution (PA). This method was chosen because with this method, only the variance that is shared with other observed variables is available for analysis, which is desirable for scale reduction (Osborne et al., 2008). Factors were rotated using an Oblimin rotation that allows factors to correlate (Tabachnick, 2001), which was expected given the similarity in the behavioral objects evaluated (security recommendations and not following them). Seven factors were extracted based on the model supporting this study. The following items were removed based on poor loadings (< 0.3), cross-loadings, and/or ambiguous loadings: six items from the scale that captured the evaluative aspect of attitudes (At04, At05, At07, At08, At09, At12), one from the potency aspect of attitudes (At19), one from descriptive norms (Sn23), one from the injunctive norms (Sn26), and two from anticipated regret (Ar29, Ar31). The researcher examined internal consistency for each of the scales using Cronbach's alpha. Correlations between social desirability and each of the items (variables) were also examined.

A seven-factor structure for 25 out of the 36 items was found. The solution fit the theoretical basis of this study. There was a consistent factor structure for all scenarios. Four items indicated mildness of security recommendations (MSR), four indicated the intention of not following security recommendations (IN), three items indicated the negative injunctive norms regarding following security recommendations (Inj), four items indicated the negative attitudes toward the importance of security recommendations (ATI), four items indicated the negative attitudes towards the completeness of security recommendations (ATC), three items indicated the negative descriptive norms relative to security recommendations (DN), and three items indicated no anticipated regret relative to not following security recommendations (AR). In all cases, Cronbach's alpha was adequate (> 0.7). Table 3.5 presents the factor correlation matrix and Cronbach's alpha for each data set (scenario). In Appendix A, items' loadings,

means, and standard deviation are provided for Scenarios 1, 2, 3, and 4. Table 3.6 provides this information for Scenario 1 only. Overall, loadings were in the range between good (> 0.55) and excellent (> 0.71) (Comrey & Lee, 2013). KMO was more than 0.7 for all items (Kaiser, 1974). Kurtosis and Skewness indexes were less than 3, as recommended (Hirschfeld & Von Brachel, 2014). The correlations between the items and the social desirability composite score were weak or in the low range of moderate for all items (Cohen, 1988).

Table 3.5

Factor Correlation Matrix and Cronbach's Alpha Per Scenario

		MSR	IN	Inj	ATI	ATC	DN	AR	Factor labels
MSR	Scen1	(0.89)							Mildness of security recommendations.
	Scen2	(0.86)							
	Scen3	(0.85)							
	Scen4	(0.87)							
IN	Scen1	0.08	(0.85)						Intention of not following security recommendations.
	Scen2	0.17	(0.92)						
	Scen3	-0.06	(0.79)						
	Scen4	-0.07	(0.91)						
Inj	Scen1	**-0.46**	**0.33**	(0.87)					Negative injunctive norms relative to following security recommendations
	Scen2	**-0.37**	**0.32**	(0.87)					
	Scen3	**-0.48**	**0.25**	(0.87)					
	Scen4	**-0.53**	**0.41**	(0.89)					
ATI	Scen1	0.00	**0.42**	0.12	(0.82)				Negative attitudes towards the importance of security recommendations.
	Scen2	0.09	**0.45**	0.22	(0.83)				
	Scen3	0.11	**0.38**	0.23	(0.83)				
	Scen4	0.02	**0.28**	0.10	(0.84)				
ATC	Scen1	0.21	**0.27**	0.01	**0.54**	(0.81)			Negative attitudes towards the completeness of security recommendations.
	Scen2	0.34	**0.32**	0.04	**0.40**	(0.84)			
	Scen3	0.39	**0.21**	-0.04	**0.48**	(0.87)			
	Scen4	0.20	**0.22**	-0.04	**0.63**	(0.85)			
DN	Scen1	0.06	**0.33**	0.03	**0.48**	**0.48**	(0.79)		Negative descriptive norms relative to security recommendations.
	Scen2	0.26	**0.46**	0.16	**0.47**	**0.59**	(0.84)		
	Scen3	0.19	**0.33**	0.05	**0.52**	**0.60**	(0.82)		
	Scen4	0.20	**0.25**	0.04	**0.43**	**0.51**	(0.77)		
AR	Scen1	0.09	**0.55**	0.20	0.26	0.23	0.26	(0.82)	No anticipated regret relative to not following security recommendations.
	Scen2	0.27	**0.65**	0.17	0.44	0.34	0.43	(0.88)	
	Scen3	0.04	**0.45**	0.16	0.40	0.18	0.25	(0.79)	
	Scen4	-0.01	**0.66**	0.21	0.40	0.30	0.31	(0.82)	

Note. Correlation 0.1 low, 0.3 moderate, 0.5 strong (Cohen, 1988). Scen: scenario. Cronbach's Alphas in parentheses.

Table 3.6

Factor Analysis Results for Scenario 1

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
At01	The recommendations my organization has in terms of handling personal information online are beneficial.	1.81	0.77	**0.83**	0.04	-0.01	0.01	0.07	0.06	-0.01
At02	The recommendations my organization has in terms of handling personal information online are complete.	1.98	0.83	-0.07	0.06	0.05	-0.05	0.13	0.01	**0.71**
At03	The recommendations my organization has in terms of handling personal information online are sufficient.	1.90	0.79	0.08	-0.02	-0.09	0.01	0.24	0.19	**0.53**
At06	The recommendations my organization has in terms of handling personal information online are important.	1.82	0.78	**0.36**	-0.21	0.10	0.00	0.03	0.12	0.26
At10	The recommendations my organization has in terms of handling personal information online are wise.	1.82	0.80	**0.45**	-0.02	0.01	0.03	0.28	0.05	0.13
At11	The recommendations my organization has in terms of handling personal information online are necessary.	1.79	0.77	**0.51**	-0.11	0.27	-0.02	-0.02	0.05	0.15
At13	The recommendations my organization has in terms of handling personal information online are precise.	2.02	0.74	0.31	0.15	-0.08	0.05	0.16	0.09	**0.33**
At14	The recommendations my organization has in terms of handling personal information online are hard.	2.69	1.22	-0.02	**0.89**	-0.02	-0.02	-0.03	0.01	0.03
At15	The recommendations my organization has in terms of handling personal information online are strong.	1.96	0.81	0.28	0.12	0.11	0.01	-0.11	-0.09	**0.61**
At16	The recommendations my organization has in terms of handling personal information online are severe.	2.59	1.17	-0.14	**0.72**	-0.08	-0.04	0.11	0.14	0.15
At17	The recommendations my organization has in terms of handling personal information online are constrained.	2.48	1.13	0.09	**0.79**	0.05	-0.10	0.06	0.01	-0.12
At18	The recommendations my organization has in terms of handling personal information online are complex.	2.64	1.14	0.05	**0.79**	0.07	0.01	-0.10	-0.10	0.03
Sn20	People at my work observe recommendations in terms of handling personal information.	1.98	0.77	0.25	-0.03	0.03	0.01	**0.30**	0.05	0.33
Sn21	People at my workplace follow recommendations in terms of handling personal information.	1.88	0.69	0.04	0.03	0.06	0.04	**0.78**	0.02	0.02
Sn22	People at my workplace act in a way that follows recommendations in terms of handling personal information.	1.92	0.81	0.19	-0.11	0.15	-0.08	**0.49**	-0.13	0.19
Sn24	How would people at your workplace be about John's decision?	2.95	1.21	0.01	-0.07	-0.07	**0.74**	-0.10	0.17	0.03
Sn25	How would people at your workplace feel about John's decision?	2.91	1.24	-0.01	-0.04	0.02	**0.85**	0.00	-0.04	-0.02
Sn27	How would people where you work be with John's decision?	2.92	1.20	0.00	0.02	0.04	**0.85**	0.07	-0.07	-0.03
Ar28	If you would have decided like John, answer whether the following statement is true to you. "Things would have gone better if I had chosen another option to respond to the request from my colleague."	2.03	0.91	0.02	0.14	0.39	0.17	0.14	**0.20**	0.03

Table 3.6 (continue)

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
Ar30	If you would have decided like John, answer whether the following statement is true to you. "I should have decided differently to respond to the request from my colleague."	1.95	0.94	0.14	0.05	0.14	0.05	0.02	**0.75**	0.00
Ar32	If you would have decided like John, answer whether the following statement is true to you. "Before responding this way to the request from my colleague, I should have chosen a different way."	1.87	0.86	-0.04	0.02	0.48	-0.01	0.03	**0.46**	0.08
In33	In similar situations, I will not decide as John did.	2.02	1.04	-0.02	-0.06	**0.53**	0.02	-0.04	0.32	0.04
In34	I intend not to do as John did in similar situations.	1.94	1.00	0.00	0.04	**0.76**	0.09	-0.02	-0.04	0.14
In35	I plan to not respond as John did in similar situations.	1.96	0.96	0.03	0.01	**0.71**	-0.03	0.14	0.04	-0.08
In36	I will not do as John did if I am in similar situations.	1.97	1.04	0.12	0.02	**0.66**	0.10	0.06	0.10	-0.06

Note. N=182. Oblimin rotation, principal factor as the method of extraction.
M: mean. *SD*: Std dev. *PA*: Principal factor. Cutoff: 0.32 poor, 0.45 fair, 0.55 good, 0.63 very good and 0.71 excellent (Osborne et al., 2008).

3.3.6 Convergent and Discriminant Validity Analysis

The researcher examined convergent and discriminant validity using Williams' scale (Williams & Joinson, 2020). The Williams scale captures the predictors of information seeking about phishing. The scale includes six dimensions: (a) perceived severity of the consequences of falling victim to a phishing attack, (b) perceived vulnerability of falling victim to a phishing attack, (c) anti-phishing techniques self-efficacy as means to prevent falling victim to a phishing attack, (d) anti-phishing techniques knowledge acquiring self-efficacy, (e) perceived ability to detect phishing emails, and (f) response cost regarding acquiring anti-phishing techniques knowledge. A moderate correlation between the factors of the SR scale and the dimensions of Williams' scale was considered evidence of convergent validity, and a low correlation was considered evidence of discriminant validity (DeVellis, 2017). The analysis was made across scenarios. Table 3.7 provides the convergent and discriminant analysis results.

The researcher expected the mildness of security recommendations (MSR) to correlate with the perceived vulnerability of falling victim to a phishing attack (W2). The rationale is that if employees perceive recommendations as mild, they will feel more exposed to potential phishing attacks. Equally, the MSR was expected to be orthogonal to the anti-phishing techniques self-efficacy (W3). W3 is not affected by the potential response of the organization to not following security recommendations

For the intention of not following security recommendations (IN), the researcher expected that if employees believe they have the ability to detect phishing emails (W5), then these two constructs would correlate. Similarly, the IN scale was expected to be orthogonal to the response cost regarding acquiring anti-phishing techniques knowledge (W6). The rationale is that when there is the motivation of not following security recommendations, the cost related to acquiring anti-phishing techniques becomes irrelevant.

It was expected that the negative injunctive norms relative to following security recommendations (Inj) would negatively correlate with the perceived vulnerability of falling victim to a phishing attack (W2). Employees not perceiving such vulnerability makes them believe that others evaluate following security recommendations as unnecessary. Equally, it was expected that Inj would be orthogonal to anti-phishing techniques knowledge acquiring self-efficacy (W4). If the employee thinks that others evaluate not following SR as favorable, the ability acquiring knowledge about anti-phishing techniques become irrelevant.

The negative evaluation of the importance of security recommendations (ATI) was expected to correlate with the perceived ability to detect phishing emails (W5). Security recommendations are unimportant to the extent that employee's self-perception of their ability to detect phishing emails is high. The ATI was expected to be orthogonal with the perceived vulnerability of falling victim to a phishing

attack (W2). If employees' self-perception of vulnerability to a phishing attack is low, the evaluation of the importance of security recommendations becomes irrelevant.

The researcher expected that the negative evaluation of the completeness of security recommendations (ATC) would correlate with the perceived ability to detect phishing emails (W5). A high employee self-evaluation of the ability to detect phishing emails makes the security recommendations incomplete, as the employee refers to her/his own knowledge and not to the recommendations provided by the organizations to prevent phishing attacks. Equally, it was expected that ATC would not associate with the perceived vulnerability of falling victim to a phishing attack (W2). The perception of falling victim to a phishing attack makes the perception of completeness of security recommendation irrelevant.

The researcher expected that the negative descriptive norms relative to security recommendations would correlate with the lack of perceived severity of the consequences of falling victim to phishing attacks (W1). Equally, it was expected that descriptive norms would be orthogonal to the response cost regarding acquiring anti-phishing techniques knowledge (W6). W6 makes descriptive norms regarding security recommendations irrelevant.

Finally, it was expected that absence of anticipated feeling of regret regarding not following security recommendations (AR) would correlate with the perceived low severity of the consequences of falling victim to phishing attacks (W1). Given a low perception of severity of consequences, employees will not feel regret for not following security recommendations. Equally, it was expected that AR would not be associated with the high response cost associated with acquiring anti-phishing techniques knowledge (W6). If the response cost is high, the self-evaluation of anticipated regret becomes irrelevant.

Overall, the indicated correlations were found across scenarios providing evidence of convergent validity for the SR scale. Equally, the expected orthogonality was found for the indicated constructs providing evidence of discriminant validity for the SR scale.

At the end of the factor exploration, a seven-factor solution was found across scenarios. The 25 items of the SR scale indicated seven factors. The SR scale exhibited good psychometric properties and was deemed as appropriate for confirming the measurement model in the next section.

Table 3.7

Correlation Coefficients Between Factors in This Study and Williams's Scale Dimensions

		MSR	IN	Inj	ATI	ATC	DN	AR	Subscale
W1	Scen1	-0.07	0.37***	0.20**	0.67***	0.48***	0.54***	0.41***	Perceive severity of the consequences of falling victim to a phishing attack.
	Scen2	-0.06	0.48***	0.21**	0.60***	0.35***	0.35***	0.43***	
	Scen3	-0.03	0.53***	0.18*	0.51***	0.25***	0.36***	0.54***	
	Scen4	-0.06	0.57***	0.23**	0.57***	0.42***	0.46***	0.51***	
W2	Scen1	0.74***	0.027	-0.47***	-0.041	0.16*	0.06	0.10	Perceived vulnerability of falling victim to a phishing attack.
	Scen2	0.60***	0.065	-0.37***	0.162*	0.22**	0.22**	0.10	
	Scen3	0.61***	-0.08	-0.48***	-0.01	0.14*	0.06	0.12	
	Scen4	0.71***	-0.064	-0.47***	0.058	0.20**	0.16*	0.0005	
W3	Scen1	0.002	0.41***	0.20**	0.63***	0.55***	0.58***	0.40***	Anti-phishing techniques self-efficacy as means to prevent falling victim to a phishing attack.
	Scen2	0.05	0.44***	0.19**	0.60***	0.44***	0.47***	0.52***	
	Scen3	0.011	0.51***	0.09	0.55***	0.35***	0.40***	0.50***	
	Scen4	-0.09	0.47***	0.19**	0.63***	0.49***	0.49***	0.58***	
W4	Scen1	0.10	0.31***	-0.07	0.56***	0.57***	0.57***	0.37***	Anti-phishing techniques knowledge acquiring self-efficacy.
	Scen2	0.20**	0.24***	-0.01	0.35***	0.46***	0.42***	0.31***	
	Scen3	0.26***	0.24**	-0.14*	0.37***	0.41***	0.41***	0.30***	
	Scen4	0.21**	0.27***	-0.07	0.45***	0.43***	0.42***	0.38***	
W5	Scen1	-0.02	0.43***	0.14*	0.65***	0.56***	0.59***	0.38***	Perceived ability to detect phishing emails.
	Scen2	0.16*	0.37***	0.078	0.45***	0.40***	0.44***	0.43***	
	Scen3	0.20***	0.33***	-0.13*	0.43***	0.36***	0.51***	0.28***	
	Scen4	0.07	0.32***	0.027	0.53***	0.45***	0.42***	0.40***	
W6	Scen1	0.77***	-0.031	-0.44***	-0.13*	0.14*	-0.007	0.11**	Response cost regarding acquiring anti-phishing techniques knowledge.
	Scen2	0.73***	0.068	-0.37***	0.09	0.22**	0.25***	0.12*	
	Scen3	0.70***	-0.077	-0.43***	-0.002	0.27***	0.18***	0.09	
	Scen4	0.80***	-0.006	-0.44***	0.02	0.21***	0.21**	0.07	

Note. 0.1 low, 0.3 moderate, 0.5 strong correlation (Cohen, 1988).
*$p < 0.1$, **$p < 0.01$, ***$p < 0.001$.

3.4 Confirmatory and Hypotheses Evaluation

A structural equation modeling (SEM) study can be executed in a two-step approach, among other alternatives (Hoyle, 2012; Schumacker, 2010). That was the case in the current research study. The first step was CFA and the second was structural analysis. The CFA in this study had two purposes: (a) to confirm that the measurement model fit the data appropriately for all scenarios and (b) to establish that the measurement model was invariant across samples (scenarios, additional questions, and demographics). The structural analysis had two parts: structural analysis and structural invariance analysis. The purpose of the structural analysis was to evaluate the hypothesized relations among the variables of interest (H1–H6), while structural invariance was used to evaluate the structural relations across groups separated by scenarios, Ads, and demographics. The purpose was to provide evidence that the structural relations hold across groups providing evidence to examine H7–H10. In the following sections, the researcher discusses the study's sample size requirements, participants, measures, protocol, data checking, and analyses. The results are presented in the next chapter.

3.4.1 Sample Size Requirements

The sample size for the fifth data collection was established to fulfill the requirement of SEM analysis. For SEM analysis, the literature suggests ten subjects per variable, or more than 200 subjects (Hoyle, 2012). The predictors' scale has a total of 25 items. Thus, more than 250 respondents were considered appropriate after providing evidence of measurement invariance per scenario and demographic groups. The sample necessary to examine measurement invariance across groups was established based on statistical power requirements. An *a priori* power analysis for the seven-factor measurement model (*df* = 254) with an effect size for the RMSEA of 0.05, an alpha of 0.05, and 0.8 statistical power resulted in a minimum sample size of 98 cases per group. Given the maximum number of groups, the sample size requirement was established to be 800 participants.

3.4.2 Participants

A final sample was collected for this part. A total of 5,611 U.S. workers attempted to take the survey, from which 721 valid responses were retained after screening out for participation and attention checks. Demographics were collected with quotas by age, gender, and level of education following the 2021 report from the U.S. Bureau of Labor Statistics (2021; see Table 3.1). The other demographics collected were work experience, job level, organization size (i.e., number of employees), and occupation area. Table 3.8 presents the sample's sociodemographic characteristics.

Table 3.8

Sample Characteristics (N = 721 Valid Responses)

Sample characteristic	*n*	%
Scenario		
Scenario 01	183	25%
Scenario 02	170	24%
Scenario 03	174	24%
Scenario 04	194	27%
Age		
Under 18	0	0.00%
18–24	30	4.16%
25–34	158	21.91%
35–44	177	24.55%
45–54	144	19.97%
55–64	153	21.22%
65 and over	59	8.18%
Gender		
Male	336	39.66%
Female	384	59.69%
Non-binary / third gender	1	0.26%
Prefer not to say	0	0.39%
Education		
Less than a high school diploma	2	0.28%
High school graduate, no college	139	19.28%
Some college, no degree	119	16.50%
Associate degree	88	12.21%
Bachelor’s degree	233	32.32%
Advance degree	140	19.42%
Work experience		
Less than 1 year	6	0.83%
Between 1 and 5 years	73	10.12%
Between 5 and 10 years	126	17.48%
More than 10 years	516	71.57%
Job level		
Entry level	90	12.48%
Mid-level	486	67.41%
Executive level	145	20.11%
Number of employees		
Between two and 10	48	6.66%
Between 11 and 50	88	15.37%
Between 51 and 100	89	31.52%
Between 101 and 500	150	29.46%
More than 500	346	20.28%
Occupation		
Management	82	11.37%
Business and financial operations	73	10.12%
Computer and mathematical	47	6.52%
Architecture and engineering	16	2.22%
Life, physical, and social science	12	1.66%
Community and social service	14	1.94%
Legal	16	2.22%
Education, training, and library	90	12.48%
Arts, design, entertainment, sports, and media	13	1.80%

Table 3.8 (continue)

Sample characteristic/occupation	*n*	%
Healthcare practitioners and technical	37	5.13%
Healthcare support	43	5.96%
Protective service	11	1.53%
Food preparation and serving related	18	2.50%
Building and grounds cleaning and maintenance	7	0.97%
Personal care and service	11	1.53%
Sales and related	58	8.04%
Office and administrative support	70	9.71%
Farming, fishing, and forestry	4	0.55%
Construction and extraction	31	4.30%
Installation, maintenance, and repair	19	2.64%
Production	26	3.61%
Transportation and material moving	23	3.19%

3.4.3 Measures

The survey included the SR scale; for consistency, the Williams' scale (Williams & Joinson, 2020) and the social desirability scale (Hays et al., 1989) were included, as well as items for participation and attention checks and demographics. In addition, respondents answered two yes/no questions , "does your organization have security systems in place?" (Ad01), and "does your organization monitor your email account?" (Ad03), and three open-ended questions. All materials can be found in Appendix B.

3.4.4 Protocol

The data collection took place in February 2022. The survey was administered using the Qualtrics online panels service. The survey presented one of four scenarios randomly assigned to each participant. After reading the scenario, the social desirability scale was administered; then the SR scale and Williams scales were presented in random order. All the items were presented in random order within each scale. All these precautions were taken to minimize the ordering effect (Podsakoff et al., 2012).

3.4.5 Data Checking

Of the 721 valid responses, 60 were coded as outliers (i.e., Mahalanobis distance higher than the cutoff [chi-square = 52.62, df=25, alpha = 0.001]; Tabachnick, 2001), leaving 661 valid responses: 183 for Scenario 1 (Sc1), 170 for Sc2, 174 for Sc3, and 194 for Sc4. The most numerous scales had four items. For these scales and the less numerous sample (170), the ratio of cases to variable exceeded the recommended 10:1 (Hoyle, 2012). There were no violations of multivariate normality (Z-value of skewness and kurtosis less than 3; Bentler & Wu, 2005). A Kaiser-Meyer-Olkin (KMO) of 0.84 (Cutoff > 0.6; Kaiser, 1974) granted a multifactorial solution.

3.4.6 Reliability and Internal Structure Analysis

The Cronbach's alpha for all factors in the measurement model was estimated. A reliability coefficient of more than 0.7 was considered appropriate (Nunnally, 1994). Items factor loads were examined, and a cutoff of more than 0.6 was deemed appropriate (Nunnally, 1994). For structural validity, the average variance extracted (AVE) was estimated and compared with the shared variance per pair of factors. An AVE more than 0.5 was deemed as evidence of (internal) convergent validity, and a root square of AVE higher than the shared variance per pair of factors as evidence of (internal) discriminant validity (Fornell & Larcker, 1981)

Adequate Cronbach's alpha was found for all seven factors across scenarios (more than 0.7). Items loads were more than 0.7 for the most part except for item At11 (Lambda = 0.549, for sc2), item At12 (Lambda = 0.544, for sc1), and item In24 (Lambda = 0.546, for sc4). Still, loads for these three items were acceptable and more than 0.7 in the other scenarios. AVE were more than 0.5 for the most part, except MSR for Scenario 1 (AVE = 0.4163) and Scenario 3 (0.46246). Thus, the scales correlated sufficiently to suggest convergent validity. The square root of AVE was higher than the shared variance by peers of factors, except for AR and IN. This evidence suggested that there was an overlap between the AR and IN. In the initial model, AR is a precursor of IN. The estimated regression parameter and overall effect size would be inflated if AR is retained with no discriminant validity evidence. Therefore, the construct AR was removed from the model. The structural validity analysis was repeated with six factors. Item At10 loaded less than 0.6 in at least one scenario, and At08 correlated with Sn13. Therefore, At10 and At08 were dropped from the analysis. The AVE was more than 0.5 for the most part in the modified six-factor solution, except for MSR in sc1 and sc3. MSR was retained, however, as there was evidence of convergent validity for sc2 and sc4. The AVE square root was higher than the shared correlation between the pair of factors for the most part. The AVE square root in sc1, sc3, and sc4 was lower than the shared correlation between ATC and ATI. This was expected as the items that capture these two constructs capture the evaluative factor of attitudes (Osgood, 1957). For this reason, ATI and ATC were retained in the measurement model. The AVE's square root for ATC was lower than the shared variance between ATC and DN for sc1, 2, and 3, but higher for sc4 and the other constructs across scenarios. Overall, there was acceptable evidence of internal structure for the six-factor solution. Table 3.9 provides loadings for the six-factor solution for the four independent samples (one per scenario). Table 3.10 provides Cronbach's alpha, AVE, and AVE's sqrt for all factors across scenarios for the modified six-factor solution. Figure 2 depicts the modified six-factor solution.

Table 3.9

Items' Loadings Per Scenario for the Modified Six-Factor Solution

		Scenario 1 (n=170)		Scenario 2 (n=153)		Scenario 3 (n=159)		Scenario 4 (n=179)	
Factor	Indicator	Ustd	Std	Ustd	Std	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.725	1.000	0.729	1.000	0.797	1.000	0.774
	At02	0.946	0.667	0.971	0.784	0.790	0.721	0.921	0.789
	At03	1.006	0.749	1.130	0.835	0.921	0.771	0.990	0.779
	At04	0.844	0.687	0.893	0.654	0.964	0.812	1.077	0.852
ATC	At05	1.000	0.792	1.000	0.825	1.000	0.757	1.000	0.830
	At06	0.925	0.769	0.872	0.771	1.083	0.756	0.872	0.797
	At07	1.110	0.835	1.016	0.808	1.007	0.728	1.043	0.817
MSR	At09	1.000	0.701	1.000	0.920	1.000	0.703	1.000	0.767
	At11	0.900	0.679	0.512	0.549	0.774	0.615	0.816	0.706
	At12	0.755	0.544	0.774	0.747	1.027	0.704	0.888	0.691
DN	Sn13	1.000	0.704	1.000	0.838	1.000	0.769	1.000	0.735
	Sn14	1.119	0.798	0.951	0.802	1.085	0.785	1.265	0.945
	Sn15	1.058	0.822	0.971	0.845	0.962	0.729	1.112	0.852
Inj	Sn16	1.000	0.805	1.000	0.861	1.000	0.836	1.000	0.897
	Sn17	0.870	0.696	0.884	0.782	1.056	0.843	0.846	0.732
	Sn18	0.986	0.859	0.964	0.833	1.110	0.876	0.874	0.763
IN	In22	1.000	0.736	1.000	0.712	1.000	0.884	1.000	0.847
	In23	0.958	0.829	0.883	0.678	0.827	0.698	0.872	0.697
	In24	1.004	0.778	1.048	0.749	0.735	0.546	0.933	0.806
	In25	0.950	0.763	1.174	0.857	0.985	0.842	0.910	0.829

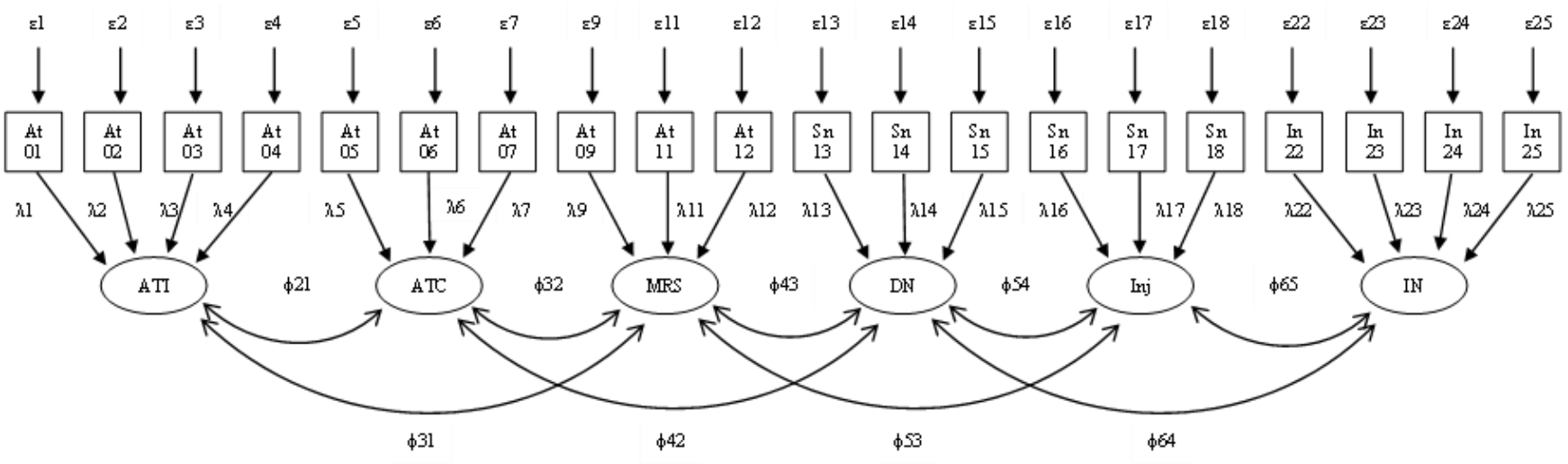
Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC: negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, Ustd: Unstandardized load, Std: Standardized load (cutoff > 0.6; Nunnally, 1994).

Table 3.10

Reliability and Internal Structure Results for the Modified Six-Factor Solution

Factor	Scenarios	Cronbach's alpha	AVE	ATI	ATC	MSR	DN	Inj	IN	Factor labels
ATI	Sc1	0.80007	0.50078	(0.70766)						Negative attitudes towards the importance of security recommendations
	Sc2	0.83746	0.56478	(0.75152)						
	Sc3	0.85550	0.60611	(0.77853)						
	Sc4	0.87454	0.63853	(0.79908)						
ATC	Sc1	0.83977	0.64245	0.90300	(0.80153)					Negative attitudes towards the completeness of security recommendations.
	Sc2	0.84139	0.64479	0.74100	(0.80299)					
	Sc3	0.79164	0.55790	0.87400	(0.74693)					
	Sc4	0.85415	0.66599	0.89100	(0.81608)					
MSR	Sc1	0.67373	0.41631	0.00000	0.07200	(0.64522)				Mildness of security recommendations.
	Sc2	0.78016	0.59509	-0.11200	0.12600	(0.77142)				
	Sc3	0.71195	0.46246	-0.04000	0.08200	(0.68004)				
	Sc4	0.76318	0.52401	0.08600	0.25700	(0.72389)				
DN	Sc1	0.81723	0.59769	0.80200	0.81300	0.10400	(0.77311)			Negative Descriptive norms relative to security recommendations.
	Sc2	0.86551	0.68568	0.73200	0.86300	0.12700	(0.82806)			
	Sc3	0.80397	0.58045	0.75700	0.86400	0.02700	(0.76187)			
	Sc4	0.87226	0.71770	0.66200	0.66900	0.27100	(0.84717)			
Inj	Sc1	0.82805	0.61706	0.61600	0.44200	-0.08700	0.52900	(0.78553)		Negative injunctive norms regarding following security recommendations.
	Sc2	0.86377	0.68349	0.35500	0.27600	-0.23800	0.42000	(0.82674)		
	Sc3	0.88700	0.72631	0.38400	0.23000	-0.17200	0.18200	(0.85224)		
	Sc4	0.83637	0.63769	0.34400	0.25200	-0.22600	0.21200	(0.79856)		
IN	Sc1	0.85537	0.59851	0.66400	0.44900	-0.09100	0.50400	0.80700	(0.77364)	Intention of not following security recommendations.
	Sc2	0.83755	0.56714	0.62300	0.43200	-0.15600	0.49300	0.55500	(0.75309)	
	Sc3	0.81925	0.54423	0.65500	0.45700	-0.04200	0.47700	0.55900	(0.73772)	
	Sc4	0.86939	0.62844	0.63700	0.48000	0.14400	0.43000	0.52600	(0.79274)	

Note. Cronbach's alpha cutoff > 0.7 (Nunnally, 1994), *AVE:* Average variance extracted, cut off > 0.5 (Fornell & Larcker, 1981)
In parenthesis, AVE square root, cut off > AVE for each pair of constructs (Fornell & Larcker, 1981)



Note:

ATI: Negative attitudes towards the importance of security recommendations (SR)

ATC: Negative attitudes towards the completeness of SR

MSR: Mildness of SR

DN: Negative descriptive norms relative to SR

Inj: Negative injunctive norms relative to following SR

IN: Intentions of not following SR

NOTE. Not all ϕs are shown., but all factors are correlated

Squares: Indicators

Circles: Factors

Figure 2: Modified Six-Factor Measurement Model

3.4.7 Confirmatory Factor Analysis (CFA)

A confirmatory factor analysis (CFA) was performed per sample to confirm that the hypothesized model fit the data appropriately (Brown, 2015; Hoyle, 2012). Table 3.11 presents the results. The CFA was performed using maximum likelihood (ML) estimation in RStudio software (RStudio Team, 2020). The estimation method was selected because it is robust when there are no violations of multivariate normality (Hoyle, 2012). The measurement model is presented in Figure 2. It consisted of six correlated factors underlying 25 indicators. The researcher assessed model fit using the chi-square statistic (Jöreskog, 1969). The chi-square statistic evaluates the absolute badness of model fit, but is sensitive to sample size (Brown, 2015; Hoyle, 2012). With a sufficiently large sample size, a test of significance can reject the model. For that reason, the chi-square statistic was supplemented by the root mean square of approximation (RMSEA), comparative fit index (CFI), and the standardized root square residual (SRMR; Brown, 2015; Hoyle, 2012). The RMSEA is a measure of the badness of fit per degree of freedom. Thus, RMSEA penalizes for model complexity. Values lower than 0.06 indicate close model fit (Steiger & Lind, 1980). The CFI is a measure of goodness of fit with a theoretical range of 0 to 1 and a cutoff of 0.95. A CFI higher than the cutoff indicates a close model fit (Bentler, 1990). Finally, the SRMR is a measure of the badness of fit. Values lower than 0.08 indicate a close model fit (Bentler & Wu, 2005). The researcher inspected the factor loadings, standard errors, and z-scores for appropriate signs and magnitude.

Initially, a correlated solution was examined for all samples. All parameters except the covariances between MSR and the other five factors were statistically significant. A second uncorrelated model was examined for all samples, but the fit indexes deteriorated. Therefore, the correlated solution was retained. The unstandardized factor loadings illustrate the strength of the latent variable/indicator relationship based on the indicator unit's scale. The standardized illustrate the same as the unstandardized on similar units. Table 3.12 summarizes item loads and fit indexes for the six-factors solution for each scenario. The results of the independent CFA analysis per scenario follow.

Scenario 1. The modified six-factor correlated model provided a good model fit (chi-square (χ^2) = 191.904, *df* = 155, *p* = 0.023, CFI = 0.977, RMSEA = 0.037 (90% CI = 0.015 – 0.054), SRMR = 0.045). The chi-square (χ^2) was not significant (at *p*-value > 0.01), the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. All indicators loaded more than 0.6 except AT12 (0.5440), which was retained because it loaded strongly for the rest of the scenarios.

Scenario 2. The modified six-factor correlated model provided a good model fit (chi-square (χ^2) = 178.318, *df* = 155, *p* = 0.097, CFI = 0.985, RMSEA = 0.031 (90% CI = 0.000 – 0.051), SRMR = 0.053). The chi-square ($\chi2$) was not significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. All indicators loaded more than 0.6 except At11 (0.549) for Sc2, which was retained because it loaded acceptably for this scenario and more than 0.6 for the rest.

Scenario 3. The modified six-factor correlated model provided a good model fit (chi-square (χ^2) = 197.436, *df* = 155, *p* = 0.012, CFI = 0.973, RMSEA = 0.041 (90% CI = 0.021 – 0.058), SRMR = 0.051). The chi-square (χ2) was not significant (at a *p*-value < 0.01), the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. All indicators loaded more than 0.6 except In24 (0.546) for Sc3, which was retained because it loaded acceptably for this scenario and more than 0.6 for the rest.

Scenario 4. The modified six-factor correlated model provided a good model fit (chi-square (χ2) = 191.498, df = 155, p = 0.025, CFI = 0.982, RMSEA = 0.036 (90% CI = 0.014 – 0.052), SRMR = 0.048). The chi-square (χ2) was not significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. All indicators loaded more than 0.6.

Table 3.11

Fit Indexes and Item Loadings Per Scenario for the Modified Six-Factor Solution

		Scenario 1		Scenario 2		Scenario 3		Scenario 4	
Factor	Indicator	Ustd	Std	Ustd	Std	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.725	1.000	0.729	1.000	0.797	1.000	0.774
	At02	0.946	0.667	0.971	0.784	0.790	0.721	0.921	0.789
	At03	1.006	0.749	1.130	0.835	0.921	0.771	0.990	0.779
	At04	0.844	0.687	0.893	0.654	0.964	0.812	1.077	0.852
ATC	At05	1.000	0.792	1.000	0.825	1.000	0.757	1.000	0.830
	At06	0.925	0.769	0.872	0.771	1.083	0.756	0.872	0.797
	At07	1.110	0.835	1.016	0.808	1.007	0.728	1.043	0.817
MSR	At09	1.000	0.701	1.000	0.920	1.000	0.703	1.000	0.767
	At11	0.900	0.679	0.512	0.549	0.774	0.615	0.816	0.706
	At12	0.755	0.544	0.774	0.747	1.027	0.704	0.888	0.691
DN	Sn13	1.000	0.704	1.000	0.838	1.000	0.769	1.000	0.735
	Sn14	1.119	0.798	0.951	0.802	1.085	0.785	1.265	0.945
	Sn15	1.058	0.822	0.971	0.845	0.962	0.729	1.112	0.852
Inj	Sn16	1.000	0.805	1.000	0.861	1.000	0.836	1.000	0.897
	Sn17	0.870	0.696	0.884	0.782	1.056	0.843	0.846	0.732
	Sn18	0.986	0.859	0.964	0.833	1.110	0.876	0.874	0.763
IN	In22	1.000	0.736	1.000	0.712	1.000	0.884	1.000	0.847
	In23	0.958	0.829	0.883	0.678	0.827	0.698	0.872	0.697
	In24	1.004	0.778	1.048	0.749	0.735	0.546	0.933	0.806
	In25	0.950	0.763	1.174	0.857	0.985	0.842	0.910	0.829

Note. Negative attitudes toward the importance of security recommendations (SR), *ATC:* negative attitudes toward the completeness of SR, *MSR:* Mildness of SR, *DN:* Negative descriptive norms, *Inj:* Negative injunctive norms, *IN:* Intentions of not following SR. *Ustd:* Unstandardized load. *Std:* Standardized load. chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), *CFI:* comparative fit index, cutoff > 0.95 (Bentler, 1990), *RMSEA:* root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), *SRMR:* Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Scenario 1 (N=170): chi-square ($\chi 2$) = 191.904, df = 155, p = 0.023, CFI = 0.977, RMSEA = 0.037 (90% CI = 0.015 – 0.054), SRMR = 0.045.
Scenario 2 (N=153): chi-square ($\chi 2$) = 178.318, df = 155, p = 0.097, CFI = 0.985, RMSEA = 0.031 (90% CI = 0.000 – 0.051), SRMR = 0.053.
Scenario 3 (N=159): chi-square ($\chi 2$) = 197.436, df = 155, p = 0.012, CFI = 0.973, RMSEA = 0.041 (90% CI = 0.021 – 0.058), SRMR = 0.051.
Scenario 4 (N=179): chi-square ($\chi 2$) = 191.498, df = 155, p = 0.025, CFI = 0.982, RMSEA = 0.036 (90% CI = 0.014 – 0.052), SRMR = 0.048.

3.4.8 Factorial Invariance Analyses

The previous CFA analyses indicated that the measurement model fit the data appropriately for each scenario independently. The factorial invariance analysis ensured that the measurement model is invariant across scenarios, demographics, and additional questions (Ads). In other words, factorial invariance provides evidence that the measurement model operates the same across groups (Brown, 2015; Gana & Broc, 2019; Hoyle, 2012).

The researcher examined the factor invariance using a multigroup CFA (MG-CFA; Brown, 2015; Hirschfeld & Von Brachel, 2014). Model invariance was examined in three stages: configural invariance, metric invariance, and scalar invariance. Configural invariance tests that the samples have the same structure (i.e., the same items load into the same factors; Brown, 2015). Metric invariance tests that the loads are similar for all groups (Brown, 2015). Finally, scalar invariance tests that the item intercepts are similar for all groups (Brown, 2015). The comparison of nested models was based on the chi-square difference test and changes in the CFI values (Brown, 2015; Hoyle, 2012). A nonsignificant change in the chi-square statistic and a difference in the CFI values lower than 0.01 between models were reported to be robust MG invariance (Hirschfeld & Von Brachel, 2014). The sample size per scenario, additional questions, and group of gender and job level was retained as the original data collection. The sample for the remaining demographics was distributed into different groups to achieve similar sample sizes sufficient for a CFA and the power requirements for the measurement model (n min = 98). Table 3.12 shows the counts and percentages for each group. Appendix C provides a description of all factorial invariance analyses. Overall, it was found that the measurement model was configural, scalar, and metric invariant across groups. With evidence of an unbiased measurement model, the analysis moved to examine the structural relations in the model.

Table 3.12

Counts Per Group (N = 661, No Outliers)

	N	%
Scenario		
Scenario 01	170	26
Scenario 02	153	23
Scenario 03	159	24
Scenario 04	179	27
Age		
Age1 (18–34 years old)	166	25
Age3 (35–44 years old)	167	25
Age4 (45–54 years old)	131	20
Age5 (55 years old and over)	197	30
Gender		
Male	301	46
Female	360	54
Education		
Edu1 (High school graduate, no college, and less than a high school diploma)	124	19
Edu3 (Some college, no degree and associate degree)	192	29
Edu5 (Bachelor's degree)	217	33
Edu6 (Advance degree)	128	19
Work experience		
Exp1 (Less than 10 years)	184	28
Exp4 (More than 10 years)	477	72
Job level		
L1 (Entry and mid-levels)	530	80
L3 (Executive level)	131	20
Number of employees		
Size1 (Between two and 100 members)	202	31
Size4 (Between 101 and 500 members)	138	21
Size5 (More than 500 members)	321	49
Ad01 question		
"yes"	476	72
"no"	185	28
Ad02 question		
"yes"	447	68
"no"	214	32

3.4.9 Structural Analysis

With evidence of good measurement model fit and factorial invariance across samples, the analysis focused on the structural relation to evaluate hypotheses H1–H6. The structural analysis included the measurement and structural models. The estimation was performed in R (RStudio Team, 2020) using ML, as this is robust when there are no violations of multivariate normality (Hoyle, 2012). Model-data fit was assessed by the chi-square statistic (Jöreskog, 1969), supplemented by the root mean square of approximation (RMSEA, cutoff < 0.6), comparative fit index (CFI, cutoff > 0.95), and the standardized root square residual (SRMR, cutoff < 0.08; Brown, 2015; Hoyle, 2012). The results of this analysis are presented in the next chapter.

3.4.10 Structural Invariance Analyses

After evaluating the structural relations, the structural invariance examined whether the relations hold across groups separated by scenarios, demographics, and additional questions (H7–H10) with baseline data from the 661 valid responses separated by groups. The structural invariance check routine (Gana & Broc, 2019) was as follows. Model fit was examined for the unconstrained model (freeing the regression coefficients across groups). Fit indexes CFI more than 0.95, RMSEA less than 0.6, and SRMS less than 0.8 were considered evidence of good model fit. The unconstrained model was then compared with five different models, each one freeing one regression coefficient. A nonsignificant chi-square difference ($\chi 2$) and CFI overlapping (Delta CFI less than 0.01) were considered evidence of invariance relative to the freed regression coefficient. In contrast, a significant chi-square difference ($\chi 2$) was considered evidence of a difference in the regression coefficient across groups for the freed regression coefficient parameter. The regression parameters reported are for the structural invariant model, constraining the regression coefficients that do not cause a difference between modes and freeing those that do. Appendix D provides a description of structural invariance across groups. The results are presented in the next chapter.

CHAPTER 4
RESULTS

4.1 Items' Descriptive Statistics

Appendix E provides the items' descriptive statistics for the original seven-factor solution with baseline data separated by scenarios, additional questions (Ads), and demographics. Skewness and kurtosis were within acceptable limits (< 3; Bentler & Wu, 2005). The variance-covariance matrices are provided per scenario in Appendix F. The matrices were computed with a maximum likelihood (ML) estimator using the saturated model in RStudio (RStudio Team, 2020).

4.2 Descriptive Statistics

Table 4.1 provides descriptive statistics for the six-factors solution. The researcher found that U.S. workers in general agree that security recommendations in their organizations are important or necessary, and complete or sufficient. They neither agree nor disagree with security recommendations being hard or severe. Some agree that others at work follow security recommendations, and that others perceive as unfavorable an act that does not follow those recommendations. Finally, U.S. workers agree in following SR in the future. The following sections provide a detailed description per factor and across samples.

Table 4.1

Factors' Descriptive Statistics (N = 661)

Factor (1-5 Likert)	M	SD
ATI: Negative attitudes towards the importance of SR	1.68	0.62
ATC: Negative attitudes towards the completeness of SR	1.98	0.78
MSR: Mildness of SR	2.89	0.93
DN: Negative descriptive norms relative to SR	1.94	0.74
Inj: Negative injunctive norms relative to following SR	2.21	0.94
IN: Intention of not following SR	1.67	0.71

Note. ATI, ATC, MSR, DN, *and* IN *f*rom *strongly agree* (1) to *strongly disagree* (5). Inj from *strongly unfavorable* (1) to *strongly favorable* (5).
All items were score in a 5-point Likert scale.
SR: Security recommendations.

4.2.1 Negative Attitudes Towards the Importance (ATI) of Security Recommendations (SR)

There was no significant difference in the ATI score across scenarios, age groups, gender, work experience, job level, and organization size. The ATI score was significantly different across groups with different education levels (at $p < 0.1$; F-statistic = 2.246, $df = 657$, p-value = 0.0818). People with a high school diploma or less had a significantly higher ATI score. Relative to the yes/no questions (Does your organization provide secure systems for data sharing? [Ad01] and does your organization monitor your email account? [Ad02]), the ATI score was significantly higher for those that answered "no" than for those that answered "yes" for both (Ad01: F-statistic = 27.26, $df = 659$, p-value < 0.001; Ad02: F-statistic = 18.82, $df = 659$, p-value < 0.001). Table 4.2 provides descriptive statistics for ATI per group.

Table 4.2

Descriptive Statistics and Comparison Across Groups for ATI

ATI: Scenarios	Est.	SE	t val	Pr(>|t|)	ATI: Age	Est.	SE	t val	Pr(>|t|)	ATI: Level of education	Est.	SE	t val	Pr(>|t|)
Achievement (intercept)	1.6814	0.0503	33.4270	<0.001	18-34 (intercept)	1.6687	0.0483	34.5500	<0.001	Advance degree	1.6602	0.0547	30.3350	<0.001
Benevolence	-0.0012	0.0685	-0.0180	0.9860	35-44	0.0244	0.0682	0.3580	0.7200	Bachelor's degree	0.0138	0.0690	0.2000	0.8415
Power	0.0172	0.0693	0.2470	0.8050	45-54	0.0107	0.0727	0.1470	0.8830	High school or less	0.1423	0.0780	1.8230	0.0687
Self-direction	-0.0226	0.0705	-0.3200	0.7490	55 and over	0.0103	0.0656	0.1560	0.8760	Some college	-0.0391	0.0707	-0.5530	0.5805
F-statistic = 0.112, df=657, p-value = 0.9531					F-statistic = 0.04329, df=657, p-value = 0.98					F-statistic = 2.246, df=657, p-value = 0.0818				
ATI: Gender	Est.	SE	t val	Pr(>|t|)	ATI: Work experience	Est.	SE	t val	Pr(>|t|)	ATI: Job level	Est.	SE	t val	Pr(>|t|)
Female (intercept)	1.7049	0.0327	52.1070	<0.001	Less than 10 years (intercept)	1.6984	0.0458	37.0810	<0.001	Entry and middle (intercept)	1.6958	0.0270	62.9100	<0.001
Male	-0.0545	0.0485	-1.1250	0.2610	More than 10 years	-0.0254	0.0539	-0.4710	0.6380	Executive	-0.0793	0.0606	-1.3100	0.1910
F-statistic = 1.265, df=659, p-value = 0.2611					F-statistic = 0.222, df=659, p-value = 0.6375					F-statistic = 1.717, df=659, p-value = 0.1905				
ATI: Secure systems?	Est.	SE	t val	Pr(>|t|)	ATI: Monitoring?	Est.	SE	t val	Pr(>|t|)					
No (intercept)	1.87838	0.04477	41.958	<0.001	No (intercept)	1.8294	0.0419	43.6800	<0.001					
Yes	-0.27544	0.05276	-5.221	<0.001	Yes	-0.2209	0.0509	-4.3380	<0.001					
F-statistic = 27.26, df=659, p-value < 0.001					F-statistic = 18.82, df=659, p-value < 0.001									
ATI: Organization size	Est.	SE	t val	Pr(>|t|)										
1-100 (intercept)	1.7116	0.0437	39.1630	<0.001										
101-500	-0.0087	0.0686	-0.1270	0.8990										
more than 500	-0.0613	0.0558	-1.0990	0.2720										
F-statistic = 0.7223, df=658, p-value = 0.486														

Note. Est: Estimate, SE: standard error, t-val: T- value. ATI: Negative attitudes toward the importance of security recommendations.

4.2.2 Negative Attitudes Towards the Completeness (ATC) of Security Recommendations (SR)

There was no significant difference in the ATC score across scenarios, level of education, gender, work experience, and organization size. The difference was significant in terms of age groups (*F*-statistic = 2.856, *df* = 657, *p*-value = 0.03642), in that older people had higher ATC scores than people 18–34 years old. Regarding job level, the difference in the ATC was significant between entry and mid-levels and executive level (*F*-statistic = 5.976, *df* = 659, *p*-value = 0.0177); specifically, people in executive roles had lower ATC scores than people in entry and mid-level roles. Relative to the yes/no questions (Does your organization provide secure systems for data sharing? [Ad01] and does your organization monitor you email account? [Ad02]), the ATC score was significantly higher for those that answered "no" than for those that answered "yes" for both (Ad01: *F*-statistic = 29.87, *df* = 659, *p*-value < 0.001; Ad02: *F*-statistic = 21.03, *df* = 659, *p*-value < 0.001). Table 4.3 provides descriptive statistics for ATC across groups.

Table 4.3

Descriptive Statistics and Comparison Across Groups for ATC

ATC: Scenarios	Est.	SE	t val	Pr(>|t|)	ATC: Age	Est.	SE	t val	Pr(>|t|)	ATC: Level of education	Est.	SE	t val	Pr(>|t|)
Achievement (intercept)	1.9564	0.0633	30.9320	<0.001	18-34 (intercept)	1.8293	0.0604	30.3110	<0.001	Advance degree	2.0495	0.0691	29.6600	<0.001
Benevolence	0.0287	0.0861	0.3330	0.7390	35-44	0.1847	0.0852	2.1670	0.0306	Bachelor's degree	-0.0910	0.0871	-1.0440	0.2970
Power	0.0553	0.0872	0.6350	0.5260	45-54	0.2038	0.0909	2.2420	0.0253	High school or less	-0.0549	0.0985	-0.5570	0.5780
Self-direction	0.0100	0.0886	0.1130	0.9100	55 and over	0.2164	0.0819	2.6410	0.0085	Some college	-0.0981	0.0892	-1.1000	0.2720
F-statistic = 0.1579, df=657, p-value = 0.9246					F-statistic = 2.856, df=657, p-value = 0.03642					F-statistic = 0.4915, df=657, p-value = 0.6883				
ATC: Gender	Est.	SE	t val	Pr(>|t|)	ATC: Work experience	Est.	SE	t val	Pr(>|t|)	ATC: Job level	Est.	SE	t val	Pr(>|t|)
Female (intercept)	1.9963	0.0412	48.4820	<0.001	Less than 10 years (intercept)	1.8478	0.0573	32.2570	<0.001	Entry and middle (intercept)	2.018	0.034	59.708	<0.001
Male	-0.0340	0.0610	-0.5560	0.5780	More than 10 years	0.1843	0.0674	2.7330	0.0064	Executive	-0.186	0.076	-2.445	0.015
F-statistic = 0.3095, df=659, p-value = 0.5782					F-statistic = 0.3095, df=659, p-value = 0.5782					F-statistic = 5.976, df=659, p-value = 0.0177				
ATC: Secure systems?	Est.	SE	t val	Pr(>|t|)	ATC: Monitoring?	Est.	SE	t val	Pr(>|t|)					
No (intercept)	2.241	0.056	39.888	<0.001	No (intercept)	2.1791	0.0526	41.4390	<0.001					
Yes	-0.362	0.066	-5.465	<0.001	Yes	-0.2932	0.0640	-4.5850	<0.001					
F-statistic = 29.87, df=659, p-value < 0.001					F-statistic = 21.03, df=659, p-value < 0.001									
ATC: Organization size	Est.	SE	t val	Pr(>|t|)										
1-100 (intercept)	1.9719	0.0550	35.8420	<0.001										
101-500	0.0329	0.0864	0.3810	0.7030										
more than 500	0.0042	0.0702	0.0590	0.9530										
F-statistic = 0.08387, df=658, p-value = 0.9196														

Note. Est: Estimate, SE: standard error, t-val: T- value. ATC: Negative attitudes toward the completeness of security recommendations.

4.2.3 Mildness of Security Recommendations (SR)

There was no significant difference in the MSR score across scenarios. Regarding age groups, the difference was significant (*F*-statistic = 11.72, *df* = 657, *p*-value < 0.001), in that the ATC score was higher for older people than the group's mean (18–34 years old). Regarding education, the MSR score was significantly different across groups (*F*-statistic = 4.279, *df* = 657, *p*-value = 0.005275). People with a high school diploma or less had a lower MSR score than people with advanced degrees. The MSR score was significantly different across gender (*F*-statistic = 4.537, *df* = 659, *p*-value = 0.03355); specifically, females had a higher ATC score than males. In groups separated by work experience, the difference in the MSR was significant (*F*-statistic = 64.71, *df* = 659, *p*-value < 0.001), in that people with more than 10 years of work experience had a higher ATC score than people with less than 10 years of experience. In terms of groups separated by job level, the difference in the MSR score was significant (*F*-statistic = 10.38, *df* = 659, *p*-value = 0.001337); people in executive positions had a lower ATC score than people in entry and mid-level positions. Relative to the yes/no questions (Does your organization provide secure systems for data sharing? [Ad01] and does your organization monitor your email account? [Ad02]), the ATC score was significantly higher for those that answered "no" than for those that answered "yes" for both questions (Ad01: *F*-statistic = 33.41, *df* = 659, *p*-value < 0.001; Ad02: *F*-statistic = 30.16, *df* = 659, *p*-value < 0.001). Table 4.4 provides descriptive statistics for MSR and comparative results across groups.

Table 4.4

Descriptive Statistics and Comparison Per Group for MSR

MSR: Scenarios	Est.	SE	t val	Pr(>|t|)	MSR: Age	Est.	SE	t val	Pr(>|t|)	MSR: Level of education	Est.	SE	t val	Pr(>|t|)
Achievement (intercept)	2.8606	0.0753	38.0010	<0.001	18-34 (intercept)	2.6044	0.0704	36.9810	<0.001	Advance degree	2.8620	0.0815	35.1050	<0.001
Benevolence	0.0221	0.1025	0.2160	0.8290	35-44	0.2279	0.0995	2.2920	0.0222	Bachelor's degree	0.1073	0.1028	1.0440	0.2970
Power	0.0336	0.1038	0.3230	0.7470	45-54	0.3040	0.1060	2.8670	0.0043	High school or less	-0.2249	0.1162	-1.9350	0.0534
Self-direction	0.0577	0.1055	0.5470	0.5850	55 and over	0.5597	0.0956	5.8550	<0.001	Some college	0.1172	0.1053	1.1130	0.2659
F-statistic = 0.1043, df=657, p-value = 0.9576					F-statistic = 11.72, df=657, p-value < 0.001					F-statistic = 4.279, df=657, p-value = 0.005275				
MSR: Gender	Est.	SE	t val	Pr(>|t|)	MSR: Work experience	Est.	SE	t val	Pr(>|t|)	MSR: Job level	Est.	SE	t val	Pr(>|t|)
Female (intercept)	2.9593	0.0488	60.5900	<0.001	Less than 10 years (intercept)	2.442	0.065	37.330	<0.001	Entry and middle (intercept)	2.9465	0.0401	73.5190	<0.001
Male	-0.1542	0.0724	-2.1300	0.0335	More than 10 years	0.619	0.077	8.044	0.000	Executive	-0.2901	0.0900	-3.2220	0.0013
F-statistic = 4.537, df=659, p-value = 0.03355					F-statistic = 64.71, df=659, p-value < 0.001					F-statistic = 10.38, df=659, p-value = 0.001337				
MSR: Secure systems?	Est.	SE	t val	Pr(>|t|)	MSR: Monitoring?	Est.	SE	t val	Pr(>|t|)					
No (intercept)	3.216	0.067	48.220	<0.001	No (intercept)	3.170	0.062	50.993	<0.001					
Yes	-0.454	0.079	-5.780	<0.001	Yes	-0.415	0.076	-5.492	<0.001					
F-statistic = 33.41, df=659, p-value < 0.001					F-statistic = 30.16, df=659, p-value < 0.001									
MSR: Organization size	Est.	SE	t val	Pr(>|t|)										
1-100 (intercept)	2.8630	0.0649	44.1180	<0.001										
101-500	-0.1867	0.1019	-1.8330	0.0673										
more than 500	0.1339	0.0828	1.6160	0.1066										
F-statistic = 5.945, df=658, p-value = 0.002763														

Note. Est: Estimate, SE: standard error, t-val: T- value. MSR: Mildness of security recommendations.

4.2.4 Negative Descriptive Norms (DN) Relative to Security Recommendations (SR)

There was no significant difference in the DN score across scenarios, level of education, and gender. Regarding age groups, the difference was significant (*F*-statistic = 2.338, *df* = 657, *p*-value = 0.07249), in that older people had a higher DN score than the intercept (18–34 years old). In terms of groups separated by work experience, the difference was significant (*F*-statistic = 6.296, *df* = 659, *p*-value = 0.00796); specifically, people with more than 10 years of work experience had a higher DN score than people with less than 10 years of experience. Regarding groups separated by job level, the difference in the DN score was significant (*F*-statistic = 3.397, *df* = 659, *p*-value = 0.06577), indicating that people in executive roles had a lower DN score than people in entry and mid-level roles. In terms of groups separated by organization size, the difference was significant (*F*-statistic = 3.226, *df* = 658, *p*-value = 0.04034), in that members of organizations with 101–500 employees had a higher DN score than members of organizations of both, small (1–100 members) and big organizations (more than 500). Relative to the yes/no questions (Does your organization provide secure systems for data sharing? [Ad01] and does your organization monitor your email account? [Ad02]), the ATC score was significantly higher for those that answered “no” than for those that answer yes for both (Ad01: *F*-statistic = 27.35, *df* = 659, *p*-value < 0.001; Ad02: *F*-statistic = 40.76, *df* = 659, *p*-value < 0.001). Table 4.5 provides descriptive statistics for DN and comparative results across groups.

Table 4.5

Descriptive Statistics and Comparison for DN

DN: Scenarios	Est.	SE	t val	Pr(>|t|)	DN: Age	Est.	SE	t val	Pr(>|t|)	DN: Level of education	Est.	SE	t val	Pr(>|t|)
Achievement (intercept)	1.878	0.059	31.570	<0.001	18-34 (intercept)	1.8353	0.0569	32.2460	<0.001	Advance degree	1.9557	0.0652	30.0180	<0.001
Benevolence	0.128	0.081	1.575	0.116	35-44	0.0748	0.0804	0.9310	0.3521	Bachelor's degree	-0.0279	0.0821	-0.3400	0.7340
Power	0.053	0.082	0.651	0.515	45-54	0.1748	0.0857	2.0400	0.0417	High school or less	-0.0202	0.0929	-0.2180	0.8280
Self-direction	0.070	0.083	0.835	0.404	55 and over	0.1816	0.0773	2.3500	0.0191	Some college	0.0009	0.0841	0.0100	0.9920
F-statistic = 0.846, df=659, p-value = 0.469					F-statistic = 2.338, df=657, p-value = 0.07249					F-statistic = 0.06955, df=657, p-value = 0.9762				
DN: Gender	Est.	SE	t val	Pr(>|t|)	DN: Work experience	Est.	SE	t val	Pr(>|t|)	DN: Job level	Est.	SE	t val	Pr(>|t|)
Female (intercept)	1.9815	0.0387	51.1580	<0.001	Less than 10 years (intercept)	1.8279	0.0540	33.8440	<0.001	Entry and middle (intercept)	1.9692	0.0319	61.7450	<0.001
Male	-0.0845	0.0574	-1.4720	0.1420	More than 10 years	0.1595	0.0636	2.5090	0.0123	Executive	-0.1320	0.0716	-1.8430	0.0658
F-statistic = 2.166, df=659, p-value = 0.1416					F-statistic = 6.296, df=659, p-value = 0.00796					F-statistic = 3.397, df=659, p-value = 0.06577				
DN: Secure systems?	Est.	SE	t val	Pr(>|t|)	DN: Monitoring?	Est.	SE	t val	Pr(>|t|)					
No (intercept)	2.178	0.053	41.080	<0.001	No (intercept)	2.199	0.049	45.040	<0.001					
Yes	-0.327	0.062	-5.230	<0.001	Yes	-0.379	0.059	-6.384	<0.001					
F-statistic = 27.35, df=659, p-value < 0.001					F-statistic = 40.76, df=659, p-value < 0.001									
DN: Organization size	Est.	SE	t val	Pr(>|t|)										
1-100 (intercept)	1.8515	0.0516	35.8960	<0.001										
101-500	0.2041	0.0810	2.5210	0.0120										
more than 500	0.1008	0.0658	1.5300	0.1260										
F-statistic = 3.226, df=658, p-value = 0.04034														

Note. Est: Estimate, SE: standard error, t-val: T- value. DN: Negative descriptive norms relative to security recommendations.

4.2.5 Negative Injunctive Norms (Inj) Relative to Following Security Recommendations (SR)

There was no significant difference in the Inj score across scenarios and the yes/no question Ad02 (Secure systems?). The difference was significant in terms of age groups (F-statistic = 4.619, df = 657, p-value = 0.003305), indicating that older people had lower Inj scores than younger people. The difference was significant in terms of education (F-statistic = 5.838, df = 657, p-value = 0.0006138), revealing that people with less education had lower Inj scores than those with advanced degrees. In terms of groups of gender, the difference was significant (F-statistic = 6.449, df = 659, p-value = 0.01133); specifically, females had lower Inj scores than males. In groups separated by work experience, the difference was significant (F-statistic = 30.14, df = 659, p-value < 0.001), in that people with more than 10 years of work experience had a lower Inj score than people with less than 10 years of experience. In groups separated by job level, the difference was significant (F-statistic = 15, df = 659, p-value < 0.001); people in executive roles had higher Inj scores than those in entry and mid-level roles. The difference was significant in groups separated by organization size (F-statistic = 6.805, df = 658, p-value = 0.001188); members of organizations with more than 500 employees had a lower Inj score than the employees of medium and small organizations. Relative to the yes/no questions (Does your organization have secure systems in place? [Ad01]), there was no significant difference between those that have them and those that do not (F-statistic = 0.1664, df = 659, p-value = 0.6835 [Ad01]). For the questions that asked, does your organization monitor your email account? (Ad02), the Inj score was significantly higher for those that answered “no” than for those that answered “yes” (F-statistic = 3.375, df = 659, p-value = 0.0537). Table 4.6 provides descriptive statistics for Inj and comparative results across groups.

Table 4.6

Descriptive Statistics and Comparison Per Group for Inj

Inj: Scenarios	Est.	SE	t val	Pr(>|t|)
Achievement (intercept)	2.2375	0.0760	29.4220	<0.001
Benevolence	-0.0513	0.1036	-0.4950	0.6210
Power	-0.0453	0.1048	-0.4320	0.6660
Self-direction	-0.0027	0.1065	-0.0250	0.9800
F-statistic = 0.1384, df=657, p-value = 0.937				

Inj: Age	Est.	SE	t val	Pr(>|t|)
18-34 (intercept)	2.3374	0.0723	32.3400	<0.001
35-44	-0.0020	0.1021	-0.0200	0.9842
45-54	-0.1694	0.1088	-1.5570	0.1200
55 and over	-0.3086	0.0981	-3.1450	0.0017
F-statistic = 4.619, df=657, p-value = 0.003305				

Inj: Level of education	Est.	SE	t val	Pr(>|t|)
Advance degree	2.500	0.082	30.457	<0.001
Bachelor's degree	-0.346	0.104	-3.347	0.001
High school or less	-0.272	0.117	-2.320	0.021
Some college	-0.427	0.106	-4.030	0.000
F-statistic = 5.838, df=657, p-value = 0.0006138				

Inj: Gender	Est.	SE	t val	Pr(>|t|)
Female (intercept)	2.1269	0.0493	43.1610	<0.001
Male	0.1854	0.0730	2.5390	0.0113
F-statistic = 6.449, df=659, p-value = 0.01133				

Inj: Work experience	Est.	SE	t val	Pr(>|t|)
Less than 10 years (intercept)	2.5272	0.0677	37.3100	<0.001
More than 10 years	-0.4377	0.0797	-5.4900	<0.001
F-statistic = 30.14, df=659, p-value < 0.001				

Inj: Job level	Est.	SE	t val	Pr(>|t|)
Entry and middle (intercept)	2.141	0.040	53.067	<0.001
Executive	0.355	0.091	3.921	0.000
F-statistic = 15, df=659, p-value < 0.001				

Inj: Secure systems?	Est.	SE	t val	Pr(>|t|)
No (intercept)	2.1874	0.0691	31.6710	<0.001
Yes	0.0332	0.0814	0.4080	0.6830
F-statistic = 0.1664, df=659, p-value = 0.6835				

Inj: Monitoring?	Est.	SE	t val	Pr(>|t|)
No (intercept)	2.3131	0.0640	36.1170	<0.001
Yes	-0.1505	0.0779	-1.9330	0.0537
F-statistic = 3.375, df=659, p-value = 0.0537				

Inj: Organization size	Est.	SE	t val	Pr(>|t|)
1-100 (intercept)	2.238	0.065	34.172	<0.001
101-500	0.204	0.103	1.989	0.047
more than 500	-0.142	0.084	-1.700	0.090
F-statistic = 6.805, df=658, p-value = 0.001188				

Note. Est: Estimate, SE: standard error, t-val: T- value. Inj: Negative injunctive norms relative to following security recommendations.

4.2.6 Intentions (IN) of Not Following Security Recommendations (SR)

There was no significant difference across scenarios, age, level of education, job level, organization size, and the yes/no question Ad02 (Secure systems?). In terms of groups of gender, the difference was significant (F-statistic = 3.313, df = 659, p-value = 0.06917), indicating that females had lower IN scores than males. In terms of groups separated by work experience, the difference was significant (F-statistic = 2.811, df = 659, p-value = 0.09407), in that people with more than 10 years of work experience had a lower IN score than people with less than 10 years of experience. Relative to the yes/no question, "does your organization have secure systems in place?" (Ad01), there was no significant difference among respondents (F-statistic = 2.155, df = 659, p-value = 0.1425). Relative to the question "does your organization monitor your email account?" (Ad02), the IN score was significantly higher for those that answered "no" than for those that answered "yes" (F-statistic = 15.98, df = 659, p-value < 0.001). Table 4.7 provides descriptive statistics for IN and comparative results across groups.

Table 4.7

Descriptive Statistics and Comparison for IN

IN: Scenarios	Est.	SE	t val	Pr(>|t|)	IN: Age	Est.	SE	t val	Pr(>|t|)	IN: Level of education	Est.	SE	t val	Pr(>|t|)
Achievement (intercept)	1.7206	0.0573	30.0080	<0.001	18-34 (intercept)	1.7139	0.0549	31.1970	<0.001	Advance degree	1.6797	0.0625	26.8730	<0.001
Benevolence	-0.0684	0.0781	-0.8750	0.3820	35-44	0.0122	0.0776	0.1570	0.8750	Bachelor's degree	-0.0357	0.0788	-0.4530	0.6510
Power	-0.0265	0.0790	-0.3350	0.7380	45-54	-0.0307	0.0827	-0.3710	0.7110	High school or less	0.1207	0.0891	1.3550	0.1760
Self-direction	-0.0869	0.0803	-1.0820	0.2790	55 and over	-0.1225	0.0746	-1.6420	0.1010	Some college	-0.0560	0.0807	-0.6940	0.4880
F-statistic = 0.4934, df=659, p-value = 0.98					F-statistic = 1.379, df=657, p-value = 0.2481					F-statistic = 1.777, df=657, p-value = 0.1502				
IN: Gender	Est.	SE	t val	Pr(>|t|)	IN: Work experience	Est.	SE	t val	Pr(>|t|)	IN: Job level	Est.	SE	t val	Pr(>|t|)
Female (intercept)	1.72014	0.03727	46.15000	<0.001	Less than 10 years (intercept)	1.74864	0.05215	33.529	<0.001	Entry and middle (intercept)	1.6684	0.0308	54.1860	<0.001
Male	-0.10054	0.05523	-1.82000	0.06920	More than 10 years	-0.10294	0.06139	-1.677	0.0941	Executive	0.0301	0.0692	0.4350	0.6640
F-statistic = 3.313, df=659, p-value = 0.06917					F-statistic = 2.811, df=659, p-value = 0.09407					F-statistic = 0.1891, df=659, p-value = 0.6638				
IN: Secure systems?	Est.	SE	t val	Pr(>|t|)	IN: Monitoring?	Est.	SE	t val	Pr(>|t|)					
No (intercept)	1.7392	0.0520	33.4220	<0.001	No (intercept)	1.832	0.048	38.253	<0.001					
Yes	-0.0900	0.0613	-1.4680	0.1430	Yes	-0.233	0.058	-3.998	<0.001					
F-statistic = 2.155, df=659, p-value = 0.1425					F-statistic = 15.98, df=659, p-value < 0.001									
IN: Organization size	Est.	SE	t val	Pr(>|t|)										
1-100 (intercept)	1.699	0.050	34.062	<0.001										
101-500	0.000	0.078	0.000	1.000										
more than 500	-0.051	0.064	-0.805	0.421										
F-statistic = 0.432, df=658, p-value = 0.6494														

Note. Est: Estimate, SE: standard error, t-val: T- value. IN: Intention of not following security recommendations.

4.3 Structural Analysis Results (H1–H6)

The invariant measurement model and the structural model were examined together with baseline data from 661 valid responses. Model fit was good for the complete model (chi-square ($\chi 2$) = 208.508, df = 155, p = 0.003, CFI = 0.992, RMSEA = 0.023 (90% CI = 0.014 – 0.030), SRMR = 0.030). The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The model explains 59.5% of the variance over the intention to follow security recommendations. Table 4.8 summarizes the structural analysis results and their correspondence with hypotheses H1–H6.

Table 4.8

Structural Model (H1–H6)

Hypothesis	Standardize	Unstandardized	SE	P(>|z|)	Evaluation	Note
H1: ATI ->IN	0.727	0.846	0.134	0.000	Confirmed	-
H2: ATC->IN	-0.379	-0.361	0.120	0.003	Disconfirmed	Opposite direction than hypothesized
H3: MSR ->IN	0.099	0.074	0.033	0.024	Confirmed	-
H4: DN->IN	0.100	0.105	0.081	0.193	Disconfirmed	-
H5: Inj ->IN	0.410	0.311	0.035	0.000	Confirmed	-
H6: AR->IN	-	-	-	-	Not evaluated	It was not possible to discriminate between AR and IN

Note. Model: chi-square ($\chi 2$) (df=155, *N*=661)=208.508, *p* value = 0.003. Null: chi-square ($\chi 2$) (*df*=190, *N*=661)=6654.364. CFI = 0.992 (Cutoff > 0.95), RMSEA (0.023; 90%CI [0.014 – 0.030])(cutoff < 0.06), SRMR = 0.030 (cutoff < 0.8). ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. $\mathbf{R^2 = 0.595}$

Regarding the evaluation and potency of security recommendations, the current researcher found that the negative attitudes toward the importance of security recommendations were positively associated with the intention of not following those recommendations (H1 confirmed). If an employee thinks that security recommendations are unnecessary or unimportant, then there is a higher likelihood that the employee will not follow those recommendations. The negative attitudes toward the completeness of security recommendations were negatively associated with the intention of not following those

recommendations (H2 disconfirmed). If an employee thinks that security recommendations are incomplete or insufficient, then there is a higher likelihood that the employee will follow those security recommendations. The mildness of security recommendations was weakly and positively associated with the intention of not following those recommendations (H3 confirmed). If an employee thinks that security recommendations are mild and soft, there is a higher likelihood that the employee will not follow those recommendations.

It was also found that subjective norms play a mixed role. The negative descriptive norms relative to security recommendations were not associated with the intention of not following those recommendations (H4 disconfirmed). An employee's perception of others at work not following security recommendations does not imply a higher likelihood that the employee will not follow those recommendations. On the other hand, the negative injunctive norms relative to following security recommendations were positively associated with the intention of not following those recommendations (H5 confirmed). The more favorable an employee thinks that others at work evaluate not following security recommendations, the higher the likelihood that the employee will not follow those recommendations. Finally, evaluating the hypotheses related to anticipated regret was not possible. In the analysis of the internal structure, the researcher found that anticipated regret strongly correlated with intentions to the point that it was impossible to discriminate between these two constructs.

4.4 Structural Invariance Analyses Results (H7–H10)

Once the structural relations were evaluated with all the data, the relations were evaluated across scenarios, demographics, and additional questions. These analyses provided evidence to test hypotheses H7–H10. In the previous analysis, the researcher found that there is no association between the negative descriptive norms and the intentions; therefore, the role of the situation, secure systems, monitoring, and demographics over this association were not evaluated.

4.4.1 The Role of Individual Value Orientation at Work (H7)

The researcher found that the negative attitudes toward the importance of security recommendations were positively associated with the intention of not following those recommendations across scenarios (H7.1 disconfirmed). If an employee thinks that security recommendations are unimportant, then there is a higher likelihood that the employee will not follow those recommendations across situations that enact different value orientations at work. The negative attitudes toward the completeness of security recommendations were negatively associated with the intention of not following those recommendations across scenarios (H7.2 disconfirmed). If an employee thinks that security recommendations are incomplete, then there is a higher likelihood that the employee will follow those recommendations in situations that enact different value orientations at work. Relative to the mildness of

severity of security recommendations (MSR), the researcher found that its association with the intention of not following security recommendations was modified by the value orientation enacted in specific situations (H7.3 confirmed). The association was moderate for the scenario that enacts benevolence, and it was not significant for the other three scenarios. In situations that enact benevolence, the more employees think that security recommendations are mild and soft, there is a higher likelihood that the employee will not follow those recommendations. In contrast, in situations that enact power, achievement, or self-direction, the perceived mildness of security recommendations does not influence the likelihood of not following those recommendations.

The negative injunctive norms relative to following security recommendations was positively associated with the intention of not following those recommendations across scenarios that enact different value orientations (H7.5 disconfirmed). The more favorable the employee thinks others will evaluate not following security recommendations, the likelihood that the employee will not follow those recommendations across situations that enact different value orientations at work is higher. Table 4.9 presents a summary of the results for Hypothesis 7.

Table 4.9

Regression Coefficients Across Scenarios from the Structural Invariant Model (H7)

	Sc1				Sc2				Sc3				Sc4			
Estimate	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.748	0.870	0.127	0.000	0.706	0.870	0.127	0.000	0.724	0.870	0.127	0.000	0.763	0.870	0.127	0.000
ATC ->IN	-0.449	-0.369	0.107	0.001	-0.356	-0.369	0.107	0.001	-0.330	-0.369	0.107	0.001	-0.390	-0.369	0.107	0.001
*MSR ->IN	-0.052	-0.038	0.058	0.512	0.091	0.062	0.055	0.262	0.095	0.076	0.063	0.228	0.229	0.176	0.058	0.003
DN ->IN	0.080	0.080	0.076	0.293	0.071	0.080	0.076	0.293	0.067	0.080	0.076	0.293	0.079	0.080	0.076	0.293
Inj ->IN	0.431	0.323	0.035	0.000	0.418	0.323	0.035	0.000	0.413	0.323	0.035	0.000	0.407	0.323	0.035	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (*df*=716, *N*=661)=857.109, p value < 0.001. Null: chi-square ($\chi 2$) (df=760, *N*=661)=7519.549. CFI = 0.979 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.035; 90%CI [0.025 – 0.043])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.057 (cutoff < 0.8) (Bentler & Wu, 2005). $R(sc1)^2 = 0.681,\ R(sc2)^2 = 0.568, R(sc3)^2 = 0.594, R(sc4)^2 = 0.575.$

Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups.

4.4.2 The Role of Having Security Systems in Place (Ad01) (H8)

It was found that for employees that have secure systems in place the negative attitudes toward the importance of security recommendations were positively associated with the intention of not following those recommendations. In contrast, there was no association for those that do not have secure systems in place (H8.1 confirmed). If an employee thinks that security recommendations are unimportant and there are secure systems in place, then there is a higher likelihood that the employee will not follow those recommendations. In contrast, if there are no systems in place, the negative evaluation of the completeness of security recommendations does not increase the likelihood of not following those recommendations. The negative attitudes toward the completeness of security recommendations were negatively associated with the intention of not following those recommendations, but there was no association for employees that do not have secure systems in place (H8.2 confirmed). If an employee thinks that security recommendations are incomplete, then there is a higher likelihood of not following security recommendations if there are systems in place to help them execute their tasks securely. If there are no systems in place, the likelihood of not following security recommendations is not affected by the employee negative evaluation of the completeness of security recommendations. Relative to the mildness of severity of security recommendations (MSR), the researcher found that the existence of secure systems modified its association with the intention of not following security recommendations (H8.3 confirmed). There was no association for employees who do not have systems in contrast with those who have them where the association was consistent with the overall results. If the employees are aware of the existence of secure systems and they think that security recommendations are mild, there is a higher likelihood that the employee will not follow those recommendations. In contrast, if the employee does not have security systems in place, the employee's perception of mild SR does not affect the likelihood that the employee will not follow security recommendations.

It was also found that the negative injunctive norms were positively associated with the intention of not following security recommendations; however, the effect was significantly stronger for those that do not have security systems than for those that do (H8.5 disconfirmed). The more favorable the employee thinks others evaluate not following security recommendations, the higher the likelihood that the employee will not follow security recommendations. This likelihood is higher if there are no security systems in place. Table 4.10 presents a summary of the results for Hypothesis 8.

Table 4.10

Regression Coefficients for Both Those That Have Secure Systems and Those That Do Not (AD01) (H8)

	Yes				No			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
*ATI ->IN	0.797	1.054	0.180	0.000	0.404	0.401	0.221	0.069
*ATC->IN	-0.410	-0.425	0.149	0.004	-0.176	-0.160	0.172	0.352
*MSR ->IN	0.148	0.108	0.041	0.009	-0.039	-0.038	0.076	0.620
DN->IN	0.076	0.084	0.081	0.300	0.080	0.084	0.081	0.300
*Inj->IN	0.406	0.297	0.039	0.000	0.536	0.479	0.090	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=339, *N*=661)=448.569, p value < 0.001. Null: chi-square ($\chi 2$) (df=380, *N*=661)=6797.444. CFI = 0.983 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.031; 90%CI [0.023 – 0.039])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.042 (cutoff < 0.8 (Bentler & Wu, 2005)). $R(\text{yes})^2 = 0.606$. $R(\text{no})^2 = 0.630$.

Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups.

4.4.3 The Role of Monitoring (Ad02) (H9)

This researcher found that the negative attitudes towards the importance of security recommendations were positively associated with the intention to not follow those recommendations for both employees whose email accounts are monitored and those whose accounts are not (H9.1 disconfirmed). If an employee thinks that security recommendations are unimportant, then there is a higher likelihood that the employee will not follow those recommendations regardless of whether their email account is monitored. It was also found that the negative attitudes toward the completeness of security recommendations were negatively associated with the intention of not following those recommendations, but the association was more negative for those whose email accounts are monitored (H9.2 disconfirmed, the opposite of what the researcher predicted). If employees think that security recommendations are incomplete and know that their email accounts are not monitored, there is a higher likelihood of not following security recommendations. Relative to the mildness of security recommendations (MSR), the researcher found that when considering monitoring there was not association with the intention of not following security recommendations (H9.3 disconfirmed). The evaluation of mildness of security recommendations does not affect the likelihood of not following security recommendations when monitoring is considered.

In addition, the negative injunctive norms were positively associated with the intention of not following security recommendations, but the effect was significantly stronger for those employees whose emails accounts were not monitored (H9.5 disconfirmed). The more favorable employees think that others will evaluate not following security recommendations, there is a higher the likelihood that the employee will not follow those recommendations; this likelihood is significantly higher if their email accounts are not monitored. Table 4.11 presents a summary of the results for Hypothesis 9.

Table 4.11

Regression Coefficients for Both, Employees Whose Email Accounts Are Monitored and Those Whose Are Not (Ad02) (H9)

	Yes				No			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI->IN	0.746	0.868	0.135	0.000	0.749	0.868	0.135	0.000
*ATC->IN	-0.345	-0.321	0.118	0.006	-0.625	-0.623	0.153	0.000
MSR->IN	0.073	0.049	0.033	0.144	0.049	0.049	0.033	0.144
DN->IN	0.087	0.097	0.082	0.236	0.093	0.097	0.082	0.236
*Inj->IN	0.356	0.244	0.038	0.000	0.659	0.610	0.081	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=341, *N*=661)=420.949, p value = 0.002. Null: chi-square ($\chi 2$) (df=380, *N*=661)=6702.113. CFI = 0.987 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.027; 90%CI [0.017 – 0.035])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.041 (cutoff < 0.8 (Bentler & Wu, 2005)). $\mathrm{R(yes)}^2 = 0.579$. $\mathrm{R(no)}^2 = 0.680$.

Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. E: Hypothesis evaluation. C: Confirmed. D: Disconfirmed. O: Opposite direction. N: Not evaluated.

*Parameter significantly different across groups.

4.4.4 The Role of Demographics (H10)

It was found that the negative attitudes toward the importance (ATI) of security recommendations were positively associated with the intention of not following those recommendations across all demographics with the exception of job level, where the association was significantly different. The association was stronger for employees in managerial positions than for entry and mid-job levels. If an employee thinks that the security recommendations are unimportant, there is a higher likelihood that the employee will not follow those recommendations and the likelihood is higher for employees in managerial positions.

The negative attitudes toward the completeness (ATC) of security recommendations were negatively associated with the intention of not following those recommendations for age groups, gender, job level, and organization size. The association was significantly different across groups with different education levels and work experience. The association was significantly more negative for people with bachelor's degrees and less for people with advanced degrees. The association was negative for people with more than 10 years of experience; there was no association for people with less than 10 years of experience.

The mildness security recommendations (MSR) was positively associated with the intention of not following security recommendations across age groups and organization size. The association was significantly different across groups with different levels of education. The association was moderate for people with lower and higher level of education, and there was no association for people with some college and bachelor's degrees. There was no association when groups were separated by gender, work experience, and job level.

The association between the negative injunctive norms and the intention of not following security recommendations was consistent with the overall results across all demographics, but the association was significantly different across age groups, gender, work experience, job level, and organization size. The association was stronger for people aged between 35 and 44 years old, females, people with more work experience, those at entry and mid-job levels, and those employed at big organizations. Tables 4.12–4.17 present the results per demographics. Table 4.18 and Figure 3 are summaries of the results.

Table 4.12

Regression Coefficients Per Age Group for the Structural Invariant Model

	Age1				Age3				Age4				Age5			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI->IN	0.835	0.979	0.138	0.000	0.776	0.979	0.138	0.000	0.841	0.979	0.138	0.000	0.887	0.979	0.138	0.000
ATC->IN	-0.415	-0.489	0.121	0.000	-0.519	-0.489	0.121	0.000	-0.501	-0.489	0.121	0.000	-0.574	-0.489	0.121	0.000
MSR->IN	0.134	0.104	0.035	0.003	0.150	0.104	0.035	0.003	0.119	0.104	0.035	0.003	0.121	0.104	0.035	0.003
DN->IN	0.094	0.121	0.076	0.111	0.111	0.121	0.076	0.111	0.117	0.121	0.076	0.111	0.128	0.121	0.076	0.111
*Inj->IN	0.300	0.214	0.059	0.000	0.517	0.378	0.059	0.000	0.463	0.386	0.071	0.000	0.365	0.317	0.062	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=716, *N*=661)=894.970, p value < 0.001. Null: chi-square ($\chi 2$) (df=760, *N*=661)=7511.854. CFI = 0.973 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.039; 90%CI [0.030 – 0.047])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.060 (cutoff < 0.8 (Bentler & Wu, 2005)) Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups

$R(age1)^2 = 0.527, R(age3)^2 = 0.597., R(age4)^2 = 0.768, R(age5)^2 = 0.647.$

Table 4.13

Regression Coefficients Per Gender for the Structural Invariant Model

	Female				Male			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI->IN	0.680	0.839	0.133	0.000	0.800	0.839	0.133	0.000
ATC->IN	-0.379	-0.383	0.118	0.001	-0.444	-0.383	0.118	0.001
MSR ->IN	0.069	0.059	0.032	0.069	0.097	0.059	0.032	0.069
DN->IN	0.082	0.089	0.078	0.253	0.090	0.089	0.078	0.253
*Inj->IN	0.505	0.434	0.046	0.000	0.330	0.211	0.043	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=339, *N*=661)=411.865, p value = 0.004. Null: chi-square ($\chi 2$) (df=380, *N*=661)=6975.193. CFI = 0.989 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.026; 90%CI [0.015 – 0.034])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.039 (cutoff < 0.8 (Bentler & Wu, 2005)) Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups. $R(female)^2 = 0.690. R(age3)^2 = 0.510.$

Table 4.14

Regression Coefficients Per Level of Education for the Structural Invariant Model

	Edu1				Edu3				Edu5				Edu6			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.821	0.924	0.146	0.000	0.764	0.924	0.146	0.000	0.815	0.924	0.146	0.000	0.725	0.924	0.146	0.000
*ATC->IN	-0.489	-0.506	0.165	0.002	-0.409	-0.404	0.141	0.004	-0.551	-0.541	0.145	0.000	-0.334	-0.286	0.124	0.021
*MSR ->IN	0.241	0.200	0.086	0.020	-0.003	-0.002	0.061	0.972	0.081	0.061	0.050	0.228	0.325	0.233	0.071	0.001
DN->IN	0.077	0.092	0.081	0.260	0.087	0.092	0.081	0.260	0.090	0.092	0.081	0.260	0.082	0.092	0.081	0.260
Inj->IN	0.447	0.360	0.038	0.000	0.397	0.360	0.038	0.000	0.461	0.360	0.038	0.000	0.523	0.360	0.038	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=713, *N*=661)=838.824, p-value = 0.001. Null: chi-square ($\chi 2$) (df=760, *N*=661)=7502.311. CFI = 0.981 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.033; 90%CI [0.022 – 0.041])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.056 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups. $R(edu1)^2 = 0.698, R(edu3)^2 = 0.588, R(edu5)^2 = 0.620, R(edu6)^2 = 0.599$.

Table 4.15

Regression Coefficients Per Work Experience for the Structural Invariant Model

	Exp1				Exp4			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.621	0.763	0.130	0.000	0.674	0.763	0.130	0.000
*ATC->IN	-0.038	-0.045	0.155	0.773	-0.414	-0.375	0.109	0.001
MSR ->IN	0.058	0.043	0.033	0.194	0.053	0.043	0.033	0.194
DN->IN	0.039	0.052	0.074	0.479	0.052	0.052	0.074	0.479
*Inj->IN	0.325	0.220	0.050	0.000	0.521	0.436	0.047	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=341, *N*=661)=407.810, p value = 0.007. Null: chi-square ($\chi 2$) (df=380, *N*=661)=6877.103. CFI = 0.990 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.024; 90%CI [0.013 – 0.033])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.041 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. *Indicate parameter significantly different across groups. $R(exp1)^2 = 0.542. R(exp4)^2 = 0.648$.

Table 4.16

Regression Coefficients Per Job Level for the Structural Invariant Model

	Job1				Job3			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
*ATI ->IN	0.636	0.734	0.131	0.000	0.847	1.068	0.160	0.000
ATC->IN	-0.373	-0.351	0.114	0.002	-0.335	-0.351	0.114	0.002
MSR ->IN	0.059	0.048	0.034	0.151	0.077	0.048	0.034	0.151
DN->IN	0.117	0.124	0.079	0.118	0.111	0.124	0.079	0.118
*Inj->IN	0.466	0.382	0.041	0.000	0.273	0.183	0.060	0.002

Note. Structural invariant model: chi-square ($\chi 2$) (df=341, *N*=661)=455.135, p value < 0.001. Null: chi-square ($\chi 2$) (df=380, *N*=661)=6995.771. CFI = 0.983 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.032; 90%CI [0.024 – 0.039])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.039 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups. $\mathrm{R(job1)}^2 = 0.598. \mathrm{R(job3)}^2 = 0.621.$

Table 4.17

Regression Coefficients Per Organization Size for the Structural Invariant Model

	Size1				Size4				Size5			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.770	0.852	0.126	0.000	0.728	0.852	0.126	0.000	0.711	0.852	0.126	0.000
ATC->IN	-0.402	-0.370	0.115	0.001	-0.425	-0.370	0.115	0.001	-0.369	-0.370	0.115	0.001
MSR ->IN	0.105	0.065	0.031	0.037	0.103	0.065	0.031	0.037	0.074	0.065	0.031	0.037
DN->IN	0.115	0.121	0.082	0.142	0.121	0.121	0.082	0.142	0.110	0.121	0.082	0.142
*Inj->IN	0.398	0.268	0.048	0.000	0.355	0.237	0.058	0.000	0.415	0.367	0.051	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=523, *N*=661)=683.785, p value < 0.001. Null: chi-square ($\chi 2$) (df=570, *N*=661)=7255.767. CFI = 0.976 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.037; 90%CI [0.029 – 0.045])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.051 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Indicate parameter significantly different across groups. $\mathrm{R(size1)}^2 = 0.614. \mathrm{R(size4)}^2 = 0.464. \mathrm{R(size5)}^2 = 0.633.$

Table 4.18

Summary of Findings

Hypotheses	Evaluation	Note
H1: ATI -> IN	Confirmed	-
H2: ATC -> IN	Disconfirmed	Opposite direction than hypothesized
H3: MSR-> IN	Confirmed	-
H4: DN -> IN	Disconfirmed	-
H5: Inj -> IN	Confirmed	-
H6: AR -> IN	Not evaluated	It was not possible to discriminate between AR and IN
The role of work value orientation		
H7.1: ATI -> IN modified by WV	Disconfirmed	-
H7.2: ATC -> IN modified by WV	Disconfirmed	-
H7.3: MSR -> IN modified by WV	Confirmed	-
H7.4: DN -> IN modified by WV	Not evaluated	DN was not associated with IN
H7.5: Inj -> IN modified by WV	Disconfirmed	-
H7.6: AR -> IN modified by WV	Not evaluated	It was not possible to discriminate between AR and IN
The role of secure systems		
H8.1: ATI -> IN stronger if secure systems available	Confirmed	-
H8.2: ATC -> IN stronger if secure systems available	Confirmed	-
H8.3: MSR -> IN stronger if secure systems available	Confirmed	-
H8.4: DN -> IN stronger if secure systems available	Not evaluated	DN was not associated with IN
H8.5: Inj -> IN stronger if secure systems available	Disconfirmed	Opposite direction than hypothesized
H8.6: AR -> IN stronger if secure systems available	Not evaluated	It was not possible to discriminate between AR and IN
The role of monitoring		
H9.1: ATI -> IN weaker if monitoring	Disconfirmed	-
H9.2: ATC -> IN weaker if monitoring	Confirmed	-
H9.3: MSR -> IN weaker if monitoring	Disconfirmed	-
H9.4: DN -> IN weaker if monitoring	Not evaluated	DN was not associated with IN
H9.5: Inj -> IN weaker if monitoring	Disconfirmed	Opposite direction than hypothesized
H9.6: AR -> IN weaker if monitoring	Not evaluated	It was not possible to discriminate between AR and IN
The role of demographics		
H10.1: age -> IN	NS	
H10.1a: ATI -> IN modified by age	Disconfirmed	
H10.1b: ATC -> IN modified by age	Disconfirmed	
H10.1c: MSR -> IN modified by age	Disconfirmed	
H10.1d: DN -> IN modified by age	Not evaluated	DN was not associated with IN

Table 4.18 (continue)

The role of demographics		
Hypotheses	Evaluation	Note
H10.1e: Inj -> IN modified by age	Confirmed	
H10.1f: AR -> IN modified by age	Not evaluated	It was not possible to discriminate between AR and IN
H10.2: gender -> IN	NS	
H10.2a: ATI -> IN modified by gender	Disconfirmed	
H10.2b: ATC -> IN modified by gender	Disconfirmed	
H10.2c: MSR -> IN modified by gender	Disconfirmed	
H10.2d: DN -> IN modified by gender	Not evaluated	DN was not associated with IN
H10.2e: Inj -> IN modified by gender	Confirmed	
H10.2f: AR -> IN modified by gender	Not evaluated	It was not possible to discriminate between AR and IN
H10.3: education -> IN	NS	
H10.3a: ATI -> IN modified by education	Disconfirmed	
H10.3b: ATC -> IN modified by education	Confirmed	
H10.3c: MSR -> IN modified by education	Confirmed	
H10.3d: DN -> IN modified by education	Not evaluated	DN was not associated with IN
H10.3e: Inj -> IN modified by education	Disconfirmed	
H10.3f: AR -> IN modified by education	Not evaluated	It was not possible to discriminate between AR and IN
H10.4: work experience -> IN	NS	
H10.4a: ATI -> IN modified by work experience	Disconfirmed	
H10.4b: ATC -> IN modified by work experience	Confirmed	
H10.4c: MSR -> IN modified by work experience	Disconfirmed	
H10.4d: DN -> IN modified by work experience	Not evaluated	DN was not associated with IN
H10.4e: Inj -> IN modified by work experience	Confirmed	
H10.4f: AR -> IN modified by work experience	Not evaluated	It was not possible to discriminate between AR and IN
H10.5: organization size -> IN	NS	
H10.5a: ATI -> IN modified by organization size	Disconfirmed	
H10.5b: ATC -> IN modified by organization size	Disconfirmed	
H10.5c: MSR -> IN modified by organization size	Disconfirmed	
H10.5d: DN -> IN modified by organization size	Not evaluated	DN was not associated with IN
H10.5e: Inj -> IN modified by organization size	Confirmed	
H10.5f: AR -> IN modified by organization size	Not evaluated	It was not possible to discriminate between AR and IN
H10.6: job level -> IN	NS	

Table 4.18 (continue)

The role of demographics		
Hypotheses	Evaluation	Note
H10.6a: ATI -> IN modified by job level	Confirmed	
H10.6b: ATC -> IN modified by job level	Disconfirmed	
H10.6c: MSR -> IN modified by job level	Disconfirmed	
H10.6d: DN -> IN modified by job level	Not evaluated	DN was not associated with IN
H10.6e: Inj -> IN modified by job level	Confirmed	
H10.6f: AR -> IN modified by job level	Not evaluated	It was not possible to discriminate between AR and IN

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. WV: Work values. NS: Not significant.

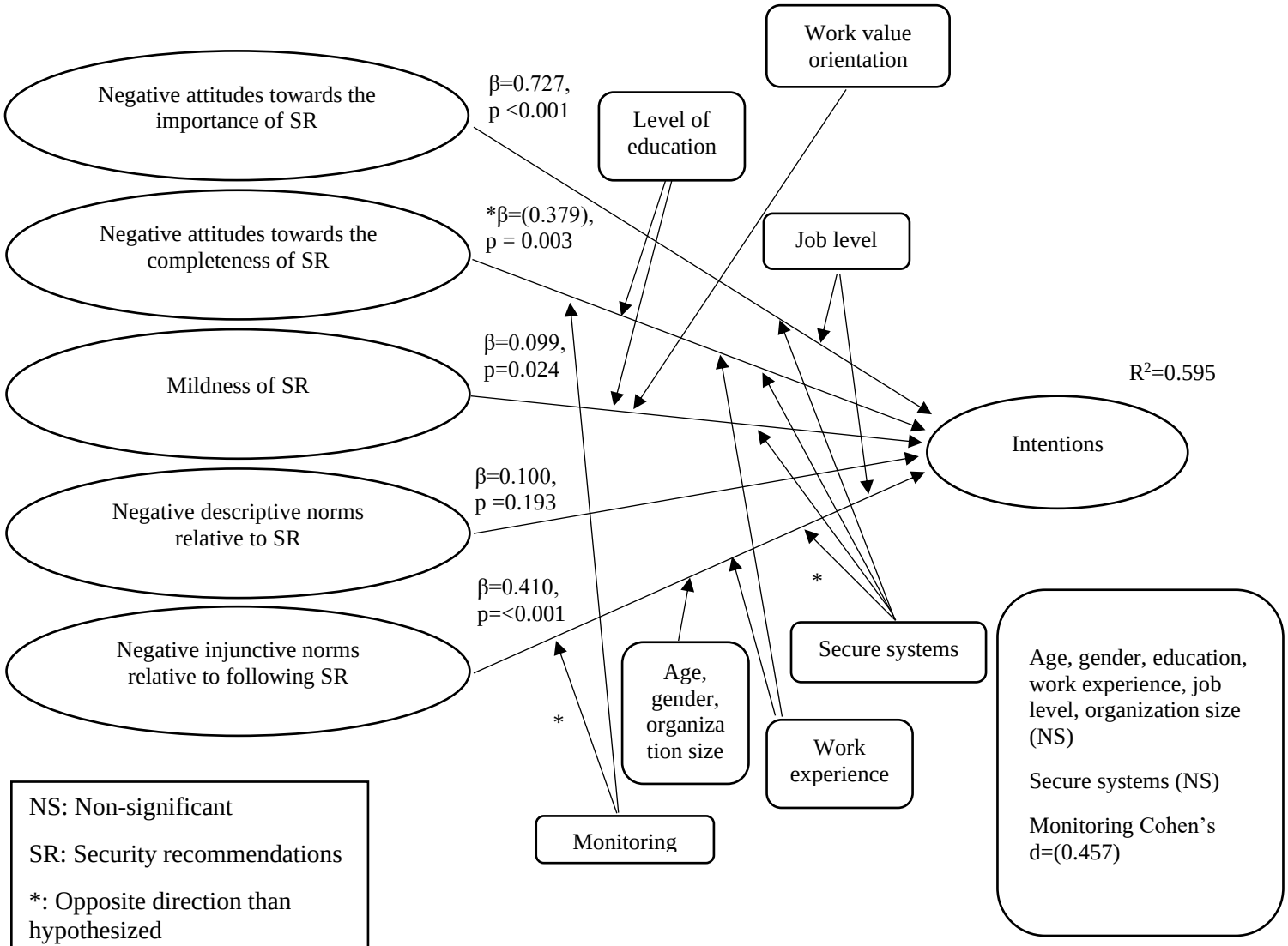


Figure 3: Results

CHAPTER 5
DISCUSSION

In this chapter, the researcher presents the key findings, discusses their implications, considers the limitations of this research study, and outlines future research opportunities.

5.1 Negative Evaluation of Formal and Informal Norms Relative to Security Recommendations (SR) as Predictors of the Intention (IN) of Not Following Them

The researcher found that the more employees regard security recommendations as unimportant or unnecessary, the less likely it is that they will follow them. Interventions that increase awareness of the importance of security recommendations, besides specifying security procedures, can positively affect the organizations' cybersecurity posture. This evidence aligns with that presented in other works (i.e., Walser et al., 2021) in which the scholars found the legitimacy of security procedures as a predictor of ISP compliance. The results of this study expand the understanding of the predictors of IS actions in the workplace by considering attitudes toward security policy provisions instead of attitudes towards acting (i.e., Vafaei-Zadeh et al., 2019) or complying with security policy (Bulgurcu et al., 2010; Ifinedo, 2012). The survey included one additional open-ended question that asked participants why security recommendations in handling personal information at work are essential. The potential risks of falling victim to scams and protecting the privacy of information are common reasons, as expected; however, low intenders also mentioned safety. This evidence implies that some employees perceive security incidents as the beginning of events that transcend the cyberworld and can compromise the integrity of people and infrastructure. Low intenders also mentioned following rules inside and outside the organization. Employees see security recommendations as important and necessary because of the risk of scams and their value orientation at work to conformity. This evidence further emphasizes the role of value orientation at work in the cybersecurity posture in organizations. Another reason cited by low intenders was the awareness that technical systems are not perfect. Future interventions should emphasize this point so that employees do not rely entirely on what the IT department can do and take responsibility for protecting information at work.

The negative evaluation of the completeness of security recommendations was negatively associated with the intention of not following them. Employees perceived the importance of security recommendations differently than their completeness. The consistent results across scenarios were puzzling. The survey asked participants what makes security recommendations for handling personal information at work complete and sufficient. Overall, low intenders perceive a set of recommendations as complete when they (a) inform consequences and are justified, (b) reflect organizational support with

constant reminders and training, (c) reflect technical support with high IT availability and measures such as monitoring what is sent and received by email, and (d) motivate socialization about security events with security meetings. The evidence might suggest that providing a lean set of instructions accompanied by legitimization processes and supporting systems and processes can be more effective than overburdening employees with more rules and regulations that might be seen as excessive.

Relative to the mildness of security recommendations, the current researcher found that the more employees evaluate security recommendations as mild and soft, the less likely they will follow them. This evidence is supported by the extant IS literature focusing on deterrence as a strategy for ISP compliance (Lowry & Moody, 2013). A combination of approaches to guide the intention of ISP compliance, one that emphasizes the legitimacy of SP and the other that emphasizes deterrence, has been suggested elsewhere (Chen et al., 2013). The survey asked respondents what would make security recommendations severe. Respondents mentioned terms such as “termination” or “get fired.” These combined findings suggest that coercive interventions related to recommendations determine, in part, compliance with SP; however, the association between MSR and intention was weaker than the effect of evaluating the importance and social norms.

Employees’ perceptions that others at work do not follow security recommendations do not affect the likelihood of not following those recommendations. The results were consistent across scenarios, demographics, and regardless of whether employees have secure systems or are monitored. These findings suggest that descriptive norms do not play a role in predicting intention to follow SR and align with the IS literature focusing on normative beliefs or injunctive norms (Cram et al., 2019). Descriptive norms, however, were correlated with the two evaluative aspects of attitudes. An interaction effect between norms and attitudes suggested elsewhere (Albrecht & Carpenter, 1976) could confirm the irrelevance of descriptive norms as a predictor of IS action. In theory, descriptive (DN) and injunctive (Inj) norms can correlate or not and have the same or opposite direction depending on the behavioral object (Fishbein & Ajzen, 2010). In this study, injunctive norms predict following SR, and DN correlated with Inj differently across scenarios. Future researchers studying this topic should clarify the role of work values enacted in specific situations and how they influence the interaction between DN and Inj as predictors of the intention to follow SR.

Relative to injunctive norms, the current researcher found that the more favorable employees think others judge an act against security recommendations, the less likely they will follow those recommendations. The results were consistent across scenarios, demographics, and whether employees have secure systems and know they are being monitored. These findings suggest that other people’s evaluation of an act that fails to follow security recommendations is a vital deterrence of insecure actions beyond the evaluation of formal security norms. Implementing socialization processes at work where

coworkers share mutual experiences about cyber incidents will potentially impact ISP compliance. This implication contrasts with the focus on informing security procedures and suggests engaging in a proactive approach with communication strategies that keep employees informed about other employees near misses that could have caused a cyber-incident at work.

Finally, it was not possible to evaluate the role of the absence of anticipated regret (AR) relative to not following security recommendations as a predictor of the intention of not following them because these two factors overlapped consistently across scenarios. The items that were used to capture AR came from a study that evaluated two factors of regret (Buchanan et al., 2016). The intention of action, however, was not captured in the mentioned study. Therefore, it was unclear whether intentions and anticipated regret would correlate. The overlap between the two constructs could have been because the items that captured AR reformulated for this study were not reworded appropriately, although they showed good psychometric properties. It is also possible that AR is a construct that, in this context, is not different than intentions. AR has been suggested as possible inclusion in the reasoned action approach (Fishbein & Ajzen, 2010), and it is an additional predictor of intention to comply with security policy (Sommestad et al., 2015b). The findings of the current project suggest that AR does not differentiate from IN when both constructs are defined relative the same behavioral object. It is also possible that AR is not a predictor of intentions, but rather a direct predictor of IS actions. Future researchers should investigate this last point.

5.2 The Role of Work Values

For the most part, work value orientations did not affect the association between the negative evaluation of formal and informal norms with the intention of not following security recommendations. There were significant differences, however, in the prediction of the intention of not following recommendations from the perception of their mildness (MSR). MSR was not a significant predictor of the intention for scenarios enacting power, achievement, and self-direction, but it was, in the scenario enacting benevolence. These findings suggest that when employees are in situations where they choose between benevolence or conformity/security, the latter is a stronger motivator. This was not the case, however, in situations where they reported their intention to act in a self-serving way. In the structure of basic human values, Schwartz (1992) categorized them in two dimensions: (a) self-transcendence to self-enhancement and (b) openness to change to conservation. Benevolence is one value part of self-transcendence, power and achievement are part of self-enhancement, and self-direction is part of openness to change. There was no association with MSR and the intention of not following SR when respondents read a scenario that reflected values that are part of orientation other than self-transcendence. Differences across scenarios in the covariance matrix further suggest the role of work values. The only

covariance consistent across scenarios was the descriptive norms of intention. For the rest, there were differences across scenarios. The role of work values as moderators of the predictors and intentions of IS actions has not been extensively explored in the IS literature. The findings in this study constitute preliminary evidence of the moderator effect of work values between employee evaluation of organizational structures and IS action in the workplace. Future research is needed in this direction to determine whether IS actions reflect values such as security or conformity in the workplace.

5.3 The Role of Secure Systems

The perceived unimportance of security recommendations was higher for employees that do not have secure systems than those that do. Although there was no significant difference in the intention of not following security recommendations between the two groups, the relation between the perception of recommendations' unimportance and the intention of not following them was stronger for employees who have secure systems than those that do not. Twenty-eight percent of respondents reported that their organizations do not have such systems. According to standard recommendations (Landoll, 2016), organizations must ensure that their employees have the tools to perform tasks securely and to inform them about their existence. These findings point out that the evaluation of security recommendations and the intention to follow them will be positively affected by the employee perception of the organization's efforts to put support systems in place and inform employees about their existence. Future research relative to secure systems could center on their ease of use, minimizing the impact of their use on productivity, and communication strategies to inform their existence.

The perceived incompleteness of security recommendations was higher for employees who do not have secure systems than those that do. The association between this negative evaluation and the intention of not following recommendations was negative for those with secure systems, and there was no association for those without them. These results were surprising. In organizations with systems to securely interchange information, the completeness of security recommendations was a negative predictor of the IN to follow SR. A future research question can explore which systems part of the technical provisions of security policy affect the perception of completeness of security policy. Perhaps the evaluation of completeness of recommendations was a negative predictor of the intention to follow SR because it is perceived as unnecessary, suggesting an interaction effect between the importance and the completeness of security recommendations with the evaluation of secure systems.

The employee perception of the mildness of security recommendations was higher for those that do not have secure systems than those that do. There was a positive association between the mildness of security recommendations and the intention of not following them for employees with secure systems. Still, there was no association for those that do not. Employees' evaluation of organizational structures as

severe affects the intention to follow them to the extent that support systems are in place. The lack of them influenced the perceived severity, making it irrelevant to the prediction of the intention of not following recommendations. Organizations that put in place secure systems will positively impact the intention of following recommendations to the extent that those recommendations are accompanied by the specification of punishment if not following them. The impact of the importance of recommendations over intention, however, was stronger than the impact of the severity of recommendations. Interventions that put in place secure systems will affect the perceived severity of recommendations, but if security systems are justified, following recommendations will follow the need for recommendations. Future scholars should further examine the role of secure systems and employee evaluation and their impact on the overall evaluation of organizational structure regarding information security.

Finally, a negative evaluation of others regarding following security recommendations was higher for employees that do not have secure systems in place than those that do. Also, the association between that evaluation and the intention of not following security recommendations was weaker for those with security systems. This evidence can be explained by the possibility that subjective norms become more relevant in the absence of secure systems. When secure systems are in place, employees refer less to other people's evaluations to form their intention to follow recommendations. Confirming these hypotheses brings opportunities for further research.

5.4 The Role of Monitoring

The negative attitudes toward the importance of security recommendations were lower for employees that are aware that they are monitored. The association between this evaluation and the intention of not following recommendations was consistent, regardless of whether employees were or were not monitored. The intention to follow recommendations was not different between the two groups. This was surprising and contrasts with findings relative to attitudes toward monitoring at the workplace and prediction of security compliance (Spitzmüller & Stanton, 2006). Results relative to reactive effects of monitoring have been found elsewhere (Lowry & Moody, 2013); however, monitoring did not affect the intention of not following recommendations. Employees' awareness of monitoring reflects that the organization is paying attention to information security, increasing the employee perception of the importance of security recommendations. The evidence suggests that monitoring alone will not affect intention, but it should be accompanied by the organizational action and reaction to what has been monitored.

Employees' negative evaluation of the completeness of recommendation was higher for employees that are not monitored. In addition, the association between this evaluation and the intention of not following security recommendations was negative and stronger for those who are not monitored.

Monitoring contributed positively to the perception of completeness of security recommendations, but this completeness negatively affects the intention to follow those recommendations. Perhaps knowing that monitoring is in place but believing that the organization is not reacting with the inputs of that monitoring, leads to a negative evaluation of organizational response. Future researchers should explore a possible conflict between the expectations of managers and employees regarding monitoring. Suppose that monitoring is in place for liability purposes and not to help employees in case of a mistake. In that case, a misalignment of management-employee expectations regarding monitoring could be a precursor to potential insecure actions.

The perception of the mildness of security recommendations and the intention to not follow them were higher for employees that are not monitored. And when the existence of monitoring systems was considered, there was no association between this perception and the intention of not following those recommendations. Thus, monitoring alone was a predictor of following SR. Monitoring was perceived as part of more severe recommendations, but this evaluation did not affect security compliance. In these circumstances, it is possible that employees think that organization monitoring is evidence that the organization is taking care of the security, and the security is not part of the employee's duties. Future scholars should clarify the effects of monitoring on empowering employees regarding security and how the perception of monitoring and control affects the psychological ownership of security at work.

Finally, the negative evaluation of others relative to following security recommendations was lower for employees that are not monitored than those who are, and the association between this perception and the intention of not following security recommendations was stronger for those employees that are not monitored. In the absence of monitoring, employees rely more on subjective norms; in its presence, employees rely on the organizational response. This is in line with the findings of Ebot (2018).

5.5 The Role of Demographics

The association between the importance of security recommendations and the intention to follow them was consistent with the overall results except for job level. The association was stronger for people in managerial positions than for entry and mid-job levels. More access to strategically important information that people in managerial roles have would explain these findings. The results align with previous findings (Williams et al., 2018). People in more operative roles invest most of their time in accomplishing tasks, and perhaps the importance of information security is not discussed from a strategic point of view with these demographic groups. As Williams et al. (2018) cited, people in managerial roles are more susceptible to suffering cyberattacks (i.e., spear-fishing). It is suggested to emphasize the strategic importance of information security at all levels of the organization so that this general perception becomes a driving force for all members.

The association between the perception of completeness of security recommendations and the intention to follow them was consistent with the overall results across age groups, gender, job level, and organization size. When analyzing for education level, the effect was significantly more negative for people with less education and not significant for people with advanced degrees. For people with more education, the negative evaluation of the completeness of recommendations did not affect their intention of not following them. These findings suggest that interventions focus on less educated employees that have not developed general awareness about information security in their organizations. When analyzing the results by work experience, the association was negative for people with more than 10 years of experience, and there was no association for people with less than 10 years of experience. People with more experience at work may be more used to following specific procedures, and the possibility of more rules and regulations negatively affects the intention to follow those recommendations. Further research is needed to clarify these findings.

When considering demographics, the effect of mild security recommendations on the intention of not following them were diverse. The association was consistent with the overall results across age groups and organization sizes. For people with a low level of education and those with advanced degrees, MSR was a strong predictor of the intention to follow SR, but it was not for people with associate and college degrees. These findings suggest that deterrence effectively guides intention to follow SR for people more susceptible to potential corrective actions of insecure acts. Fear of consequences resulting from organizational actions seems not to affect the MSR-IN association in professionals—52% of the workforce, according to last year's labor statistics report (U.S. Bureau of Labor Statistics, 2021). These findings imply that future interventions should consider complementary approaches to deterrence, especially among professionals and when security policy cannot be strictly enforced. Finally, there was no association between MSR and intention when considering gender, work experience, and job level. This evidence suggests the effect of deterrence should be examined considering these demographics.

The association between other's negative evaluation of following security recommendations and the intention to follow those recommendations was consistent with the overall results across demographics. The association was stronger for people between 35 and 44 years old, females, people with more work experience, entry and mid-job levels, and employees of big organizations. These findings suggest that other people's evaluation of action seems more critical for mature workers. Also, the gender difference suggests that socializing near misses, for example, can motivate following recommendations in females more effectively than males. Also, experienced workers might rely more on other people's evaluation of acts at work when reporting their intention to follow security recommendations. People in executive roles typically have more experience and education; however, when controlling for job level, people with executive roles' intentions to follow SR are less affected by others' evaluation of

noncompliance actions. It is logical to assume that executive-level people will be more aware of security, policy, compliance, and strategy, further suggesting the critical role of the legitimacy of security efforts in this demographic group's organization. The strongest effect among different organization sizes was for organizations with more than 500 members. Perhaps a more frequent interaction with more diverse groups made this effect stronger in big organizations, in contrast with small organizations where there are fewer references. The availability of resources to communicate security incidents might explain the Inj-IN strongest effect found for this demographic compared to small and mid-size organizations. Additional research is needed to clarify these hypotheses.

5.6 Limitations

There were several limitations that influenced this research study. First, the evaluated action was sharing personal information by email in response to a colleague in a work context enacting different work values. There are myriad possible IS actions. In the context of IS, research has been implemented for studying several specific behaviors or categories of behaviors. The contextualization of this study, however, shed light on determinants of several IS actions that shared characteristics with the studied behaviors. These processes can be generalized to other behaviors in similar research designs. A future opportunity for research is to confirm the predictive capability of the proposed contextualized model to other behaviors. Another area of future research is how one set of behavior relates to another and whether an intervention that targets one will affect the other. This possibility has been suggested elsewhere (Fishbein et al., 2007).

Second, in its initial development, the theory of basic human values lists 11 values (Schwartz, 1992); this research project enacted only four. A limitation and future area of research is to investigate other value orientations and their role in predicting IS actions. Another future research opportunity is to investigate whether IS actions express security and conformity. If they are, another research opportunity is how situations and actions that reflect other opposite values to conformity and security affect ISP compliance.

Third, this research project investigated only the additive nature of several predictors of the intention to follow SR. A future research opportunity is to investigate the interactive effect between attitudes and subjective norms relative to SR as predictors of IN. Authors have suggested this interaction (Acock & DeFleur, 1972; Albrecht & Carpenter, 1976), which is an unexplored area in IS research.

Fourth, the hypotheses posited in this research project were around the prediction of intention to follow SR and no actual IS actions. There is evidence of IN as a predictor of action in behavioral and IS research. Other predictors of action beyond intentions have been found. Studying other predictors of action instead of intention in IS research posits challenges that should be addressed by future research.

Fifth, this research project, grounded on the reasoned action approach, investigated mainly two predictors of intentions. These two factors were found to be formed by five subfactors. AR was added as an additional predictor to the main predictors of intentions to follow SR; however, AR overlapped with the IN to follow SR in discriminant validity analysis. Other variables can increase the predictive capability of future models. Past behaviors and habits have been found as a predictor that potentially can discriminate from the current predictors considered in the reasoned actions approach. These additional variables were not included in this research project, and studying their relevance is potential future research.

Sixth, the model proposed in this research project targets a volitional IS action (i.e., not sharing personal information by email as recommended in SP provisions). The model's applicability to nonvolitional actions that depend on the self-evaluation of capabilities and skills and the evaluation of environmental conditions that allow specific actions should be confirmed in future research studies.

Seventh, in the reasoned action approach, attitudes (AT) and subjective norms (SN) are predictors of intention (IN). In turn, behavioral and normative beliefs are formative indicators of AT and SN. Beliefs were not included in this study. Bulgurcu et al. (2010) found that some beliefs grounded on deterrence theory are formative indicators of the attitudes toward complying with SP; however, other behavioral and normative beliefs can potentially be included. Beliefs relative to the inconvenience of following specific security provisions in specific situations or beliefs relative to the importance of information security at work, and others, could be examined in future research. More contextualized interviews could explore beliefs as formatives of attitudes and subjective norms. Future research should consider security at work and that employees live in day-by-day situations where they need to perform all sorts of tasks. It will also be informative to include the value orientation in organizations, so the alignment of action-work value is more evident.

The eighth limitation is that not all possible demographic groups were captured. An area of future research is how the results differ from organizations that, by their nature (e.g., defense), are more sensitive to information security incidents.

Ninth, even though the hypotheses in this study were grounded on the theory that empirically and rationally support the precedence of attitudes and subjective norms over intentions, an experimental approach will be necessary to claim the causal relations explored in this research study.

Tenth, although several precautions were taken to control for social desirability and ordering effects, and conclusions were made after verifying the validity of the measurement model and psychometric properties, survey research is based on self-reporting. Capturing actual IS behaviors is challenging for the low incidence of events and privacy concerns. Although self-reporting is a helpful tool for reporting preliminary findings in social science, the findings of future studies with designs that

combine these results with other research designs (i.e., qualitative research designs) are likely to enhance relevance and applicability for practitioners.

CHAPTER 6
CONCLUSIONS

In this research project based on the reasoned action approach, the current researcher found that a negative evaluation of formal and informal norms predicts the intention of not following those recommendations. Three different aspects form the attitudes toward security recommendations: attitudes towards the importance (ATI), completeness (ATC), and severity (MSR). The negative perception of importance of SR relates to the intention of not following recommendations. In contrast, the negative perception of the completeness of SR negatively relates to the intentions of not following recommendations. Finally, the mildness of security recommendations is a poor predictor of the intentions of not following recommendations; moreover, its effect depends on the situation, the presence of secure systems, monitoring employees, and demographics. The negative evaluation of others following secure recommendations is not a predictor of the intention to follow SR. Employees' perception of others negatively evaluating following security predicts not following those recommendations.

Overall, the current findings represent preliminary evidence of the relation between the evaluation of organizational structures as predictors of the intention of IS action. This perspective suggests a change of focus from the evaluation of action or the evaluation of policy compliance, to the evaluation of the systems that the organization have in place as precursors of IS action. This perspective suggests other alternatives to examine the employee security compliance. For example, the beliefs that deter downloading pirate software (i.e., regarding its potential risks and benefits) could be complemented by the beliefs that support the evaluation of what the organizations is doing to provide the software needed to perform tasks, or how promptly the IT department responds to suspicious activities.

The researcher preliminarily explored the role of work values at work as a moderator of the association between the employee evaluation of formal and informal norms and the intention to comply with recommendations. The difference in the effect of the perception of mild secure recommendations over the intention to follow recommendations, as well as the almost complete change in the covariates across scenarios that enacted a different value orientation, suggest that work values play a role in the precursors-intentions relations. This finding should be further explored, but preliminary results suggests that behavioral change can be effective in the long term if interventions incorporate security as part of the organizational culture. Previous findings in the extant literature have advanced the understanding of countless tools that can be implemented in training programs. Scholars have cited management involvement is fundamental for improving the cybersecurity posture. Investment in processes and mechanisms, including supporting systems and awareness sessions, will be part of overall efforts to organizational change towards security. In this sense, value interventions can be a guiding tool.

Both, the presence of secure systems that help employees accomplish tasks in compliance with recommendations and monitoring had a moderator effect on the employee evaluation of formal and informal norms relative to security recommendations and the intention to follow them. This evidence suggests that the absence of both positively affect the intention of not following recommendations. The effects found, however, suggest that employees' understanding of the purpose of these systems could be different than intended by management.

Overall, acknowledging the limitations of this study, the findings were able to answer the research questions. Several new research questions have arisen, some of them as direct results of findings and others due to the limitations of this research project. Other research investigations using differing designs could provide complementary evidence of the predictors of IS-related actions.

Although more evidence is needed, the current researcher recommends that information security interventions include legitimation and socialization processes. Legitimation relative to the importance of security policy provisions and socialization relative to reporting incidents reaching all organization members. Furthermore, it is recommended to identify the most critical work values in organizations. Successful interventions would progressively align acts with values if those values reflected security as part of the organizational culture.

The implications of the findings in this study align with the results of previous research that provide insights for studying cybersecurity as a socio-technical problem. The cybersecurity problem is addressed by several disciplines, but all are helping the development of secure cyberspace. From the engineering management perspective, cybersecurity is considered with its technical and human aspects. Just as the safety community has been doing for decades, cybersecurity in organizations and society includes technical, social, and psychological elements. The cybersecurity community should include more diverse drivers of secure actions—and, in doing so, contribute to helping draft more sophisticated and effective security policies at organizational and governmental levels. Through this research project, the researcher aimed to contribute to this effort. Finally, this project was developed with the belief that people are the stewards of security in organizations, not the weakest link. Employees that are aware for the need of information security are the first line of defense against cyberattacks. This is especially important in today's organizations, in which the complexity of work and countless procedures can further complicate organizational policy compliance.

REFERENCES

Aaron, G., & Rasmussen, R. (2017). *Global Phishing Survey*. Anti-Phishing Working Group.

Abelson, R. P., Kinder, D. R., Peters, M. D., & Fiske, S. T. (1982). Affective and semantic components in political person perception. *Journal of Personality and Social Psychology, 42*(4), 619. https://doi.org/10.1037/0022-3514.42.4.619

Acock, A. C., & DeFleur, M. L. (1972). A configurational approach to contingent consistency in the attitude-behavior relationship. *American Sociological Review, 37*(6), 714–726. https://doi.org/10.2307/2093582

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, *52*, 27. https://doi.org/10.1146/annurev.psych.52.1.27

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I., & Driver, B. L. (1991). Prediction of leisure participation from behavioral, normative, and control beliefs: An application of the theory of planned behavior. *Leisure Sciences*, *13*(3), 185–204. https://doi.org/10.1080/01490409109513137

Ajzen, I., & Fishbein, M. (1973). Attitudinal and normative variables as predictors of specific behavior. *Journal of Personality and Social Psychology*, *27*(1), 41. https://doi.org/10.1037/h0034440

Alain Tambe, E. (2018). Using stage theorizing to make anti-phishing recommendations more effective. *Information and Computer Security*, *26*(4), 401–419. http://dx.doi.org/10.1108/ICS-06-2017-0040

Albarracin, D. (2019). *The handbook of attitudes: Volume 1: Basic principles* (2nd ed.). Routledge.

Albarracin, D., Johnson, B., Fishbein, M., & Muellerleile, P. A. (2001). Theories of reasoned action and planned behavior as models of condom use: A meta-analysis. *Psychological Bulletin, 27*, 142–161. https://www.apa.org/pubs/journals/bul

Albrecht, S. L., & Carpenter, K. E. (1976). Attitudes as predictors of behavior versus behavior intentions: A convergence of research traditions. *Sociometry*, *39*(1), 1–10. https://doi.org/10.2307/2786586

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, *100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, *40*(4), 471–499. https://doi.org/10.1348/014466601164939

Atkinson, J. W. (1964). *An introduction to motivation*. Van Nostrand.

Aurigemma, S., & Mattson, T. (2019a). Effect of long-term orientation on voluntary security actions. *Information and Computer Security*, *27*(1), 122–142. https://doi.org/10.1108/ICS-07-2018-0086

Aurigemma, S., & Mattson, T. (2019b). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems*, *20*(12), 1700–1742. https://doi.org/10.17705/1jais.00583

Bandura, A. (1977). Self- efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, *22*(1), 31–60. https://doi.org/10.2307/249677

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*, 145–159. https://doi.org/10.1016/j.cose.2013.05.006

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. https://doi.org/10.17705/1jais.00506

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*. https://www.emerald.com/insight/publication/issn/0957-6053

Beck, L., & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality*, *25*(3), 285–301. https://doi.org/10.1016/0092-6566(91)90021-H

Becker, G. S., & Landes, W. M. (1974). *Essays in the economics of crime and punishment*. NBER Books.

Bednall, T. C., Bove, L. L., Cheetham, A., & Murray, A. L. (2013). A systematic review and meta-analysis of antecedents of blood donation behavior and intentions. *Social Science & Medicine*, *96*, 86–94. https://doi.org/10.1016/j.socscimed.2013.07.022

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, *107*(2), 238. https://www.apa.org/pubs/journals/bul

Bentler, P. M., & Wu, E. J. C. (2005). *EQS 6.1 for Windows*: *Structural equations program manual.* Multivariate Software.

Blumstein, A. (1978). *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. National Academy Press.

Boss, S., Galletta, D., Lowry, P., Moody, G., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837. https://doi.org/10.25300/MISQ/2015/39.4.5

Brehm, J. W. (1966). *A theory of psychological reactance*. Academic Press.

Brown, T. A. (2015). *Confirmatory factor analysis for applied research*. Guilford Press.

Buchanan, J., Summerville, A., Lehmann, J., & Reb, J. (2016). The Regret Elements Scale: Distinguishing the affective and cognitive components of regret. *Judgment and Decision Making*, *11*(3), 275–286. https://psycnet.apa.org/record/2016-27105-006

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Burns, S., & Roberts, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention & Community Safety*, *15*, 48–64. https://doi.org/10.1057/cpcs.2012.13

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Calic, D., Pattinson, M. R., Parsons, K., Butavicius, M. A., & McCormac, A. (2016). *Naïve and accidental behaviours that compromise information security: What the experts think*. Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, *58*(8), 1158–1172. https://doi.org/10.1177/0018720816665025

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2013). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Cialdini, R. B. (1993). *The psychology of persuasion*. Harper Business.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.

Comrey, A. L., & Lee, H. B. (2013). *A first course in factor analysis*. Psychology Press.

Consiglio, C., Cenciotti, R., Borgogni, L., Alessandri, G., & Schwartz, S. H. (2017). The WVal: A new measure of work values. *Journal of Career Assessment*, *25*(3), 405–422. https://doi.org/10.1177/1069072716639691

Cooke, R., Dahdah, M., Norman, P., & French, D. P. (2016). How well does the theory of planned behaviour predict alcohol consumption? A systematic review and meta-analysis. *Health Psychology Review*, *10*(2), 148–167. https://doi.org/10.1080/17437199.2014.947547

Cooke, R., & French, D. P. (2008). How well do the theory of reasoned action and theory of planned behaviour predict intentions and attendance at screening programmes? A meta-analysis. *Psychology & Health*, *23*(7), 745–765. https://doi.org/10.1080/08870440701544437

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). SAGE.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. https://doi.org/10.1111/isj.12173

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

De Falco, M. (2012). *Stuxnet fact report*. NATO Cooperative Cyber Defence Centre of Excellence.

Department of Homeland Security. (2003). *The national strategy to secure cyberspace*. Author.

DeVellis, R. F. (2017). *Scale development theory and applications* (4th ed.). SAGE.

De Vivo, M., Hulbert, S., Mills, H., & Uphill, M. (2016). Examining exercise intention and behaviour during pregnancy using the Theory of Planned Behaviour: A meta-analysis. *Journal of Reproductive and Infant Psychology*, *34*(2), 122–138. https://doi.org/10.1080/02646838.2015.1118022

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*. https://doi.org/10.17705/1jais.00133

Djajadikerta, H. G., Roni, S. M., & Trireksani, T. (2015). Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. *Information & Management*, *52*(8), 1012–1024. https://doi.org/10.1016/j.im.2015.07.008

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). *Decision strategies and susceptibility to phishing*. ACM Digital Library.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). *Behavioral response to phishing risk.* ACM Digital Library.

Eagly, A. H. (1993). *The psychology of attitudes*. Harcourt Brace/Jovanovich College Publishers.

Ebot, A. T. (2018). Using stage theorizing to make anti-phishing recommendations more effective. *Information and Computer Security*, *26*(4), 401–419. http://dx.doi.org/10.1108/ICS-06-2017-0040

Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (SEBIS).* ACM Digital Library.

Etzioni, A. (1961). *A comparative analysis of complex organizations on power, involvement, and their correlates*. Free Press.

FBI. (2019). *2019 internet crime report*. Author.

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19–31. https://doi.org/10.1016/j.ijhcs.2018.12.004

Ferrer, R. A., Taber, J. M., Klein, W. M. P., Harris, P. R., Lewis, K. L., & Biesecker, L. G. (2015). The role of current affect, anticipated affect and spontaneous self-affirmation in decisions to receive self-threatening genetic risk information. *Cognition and Emotion*, *29*(8), 1456–1465. https://doi.org/10.1080/02699931.2014.985188

Fishbein, M. (1975). *Belief, attitude, intention, and behavior an introduction to theory and research*. Addison-Wesley.

Fishbein, M. (2000). The role of theory in HIV prevention. *AIDS Care*, *12*(3), 273–278. https://doi.org/10.1080/09540120050042918

Fishbein, M., & Ajzen, I. (1977). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Addison-Welsey.

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior the reasoned action approach*. Psychology Press.

Fishbein, M., Ajzen, I., Albarracin, D., & Hornik, R. C. (2007). *Prediction and change of health behavior applying the reasoned action approach*. Lawrence Erlbaum Associates.

Fishbein, M., Cappella, J., Hornik, R., Sayeed, S., Yzer, M., & Ahern, R. (2002). The role of theory in developing effective anti-drug public service announcements In W. D. Crano & M. Burgoon (Eds.), *Mass media and drug prevention: Classic and contemporary theories and research* (pp. 89–117). Lawrence Erlbaum Associates.

Fishbein, M., & Cappella, J. N. (2006). The role of theory in developing effective health communications. *Journal of Communication*, *56*(Suppl 1), S1–S17. https://doi.org/10.1111/j.1460-2466.2006.00280.x

Fishbein, M., & Yzer, M. C. (2003). Using theory to design effective health behavior interventions. *Communication Theory*, *13*(2), 164–183. https://doi.org/10.1111/j.1468-2885.2003.tb00287.x

Fisher, J. D., & Fisher, W. A. (1992). Changing AIDS-risk behavior. *Psychological Bulletin*, *111*(3), 455. https://www.apa.org/pubs/journals/bul

Fiske, S. T., Gilbert, D. T., & Lindzey, G. (2010). *Handbook of social psychology* (5th ed.). John Wiley & Sons.

Fleming, P., Watson, S. J., Patouris, E., Bartholomew, K. J., & Zizzo, D. J. (2017). Why do people file share unlawfully? A systematic review, meta-analysis and panel study. *Computers in Human Behavior*, *72*, 535–548. https://doi.org/10.1016/j.chb.2017.02.014

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.2307/3151312

Gana, K., & Broc, G. (2019). *Structural equation modeling with Lavaan*. John Wiley & Sons.

Glasman, L. R., & Albarracín, D. (2006). Forming attitudes that predict future behavior: A meta-analysis of the attitude-behavior relation. *Psychological Bulletin*, *132*(5), 778–822. https://doi.org/10.1037/0033-2909.132.5.778

Gragg, D. (2004). *A multi-level defense against social engineering* (White paper). SANS.

Gregory, D. M. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://www.cell.com/heliyon/home

Hagger, M. S., Chatzisarantis, N., & Biddle, S. (2002). A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables. *Journal of Sport & Exercise Psychology*, *24*(1), 3–32. https://doi.org/10.1123/jsep.24.1.3

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Han, T.-I., & Stoel, L. (2017). Explaining socially responsible consumer behavior: A meta-analytic review of theory of planned behavior. *Journal of International Consumer Marketing*, *29*(2), 91–103. https://doi.org/10.1080/08961530.2016.1251870

Hays, R. D., Hayashi, T., & Stewart, A. L. (1989). A five-item measure of socially desirable response Set. *Educational and Psychological Measurement*, *49*(3), 629–636. https://doi.org/10.1177/001316448904900315

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security*, *4*(4), 3–20. https://doi.org/10.1080/2333696X.2008.10855849

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hirschfeld, G., & Von Brachel, R. (2014). Improving multiple-group confirmatory factor analysis in R: A tutorial in measurement invariance with continuous and ordinal indicators. *Practical Assessment, Research, and Evaluation*, *19*(1), 7. https://scholarworks.umass.edu/pare/

Hoyle, R. H. (2012). *Handbook of structural equation modeling*. Guilford Press.

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), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Institute of Medicine. (2002). *Committee on communication for behavior change in the 21st century: Improving the health of diverse populations*. National Academies Press.

ISO/IEC. (2012). *Information technology - Security techniques - Information security management systems.* International Organizational of Standardization/International Electrotechnical Commission.

ISO/IEC. (2013). *Information technology - security techniques - code of practice for information security controls*. International Organization for Standardization/International Electrotechnical Commission.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://cacm.acm.org/

Janis, I. L. (1977). *Decision making a psychological analysis of conflict, choice, and commitment*. Free Press.

Jansen, J. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*(2), 165–180. https://doi.org/10.1108/ICS-03-2017-0018

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Jöreskog, K. G. (1969). A general approach to confirmatory maximum likelihood factor analysis. *Psychometrika*, *34*(2), 183–202. https://www.springer.com/journal/11336

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, *39*(1), 31–36. https://www.springer.com/journal/11336

Kraus, S. J. (1995). Attitudes and the prediction of behavior: A meta-analysis of the empirical literature. *Personality and Social Psychology Bulletin*, *21*(1), 58–75. https://doi.org/10.1177/0146167295211007

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 1–31. https://doi.org/10.1145/1754393.1754396

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, *23*(2), 361–373. https://doi.org/10.1007/s10796-019-09977-z

Landoll, D. J. (2016). *Information security policies, procedures, and standards: A practitioner's reference*. CRC Press/Taylor & Francis Group.

Larose, R., & Rifon, N. J. (2007). Promoting I-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, *41*(1), 127–149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, 103084–103084. https://doi.org/10.1016/j.apergo.2020.103084

Leonard, M., Graham, S., & Bonacum, D. (2004). The human factor: The critical importance of effective teamwork and communication in providing safe care. *Quality & Safety in Health Care*, *13*(Suppl 1), 85–90. https://doi.org/10.1136/qhc.13.suppl_1.i85

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 1. https://aisel.aisnet.org/jais/

Lowry, P. B., & Moody, G. D. (2013). *Explaining opposing compliance motivations towards organizational information security policies.* Proceedings of the 46th Hawaii International Conference on System Sciences.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433–463. https://doi.org/10.1111/isj.12043

Matza, D. (1964). *Delinquency and drift. From the research program of the Center for the Study of Law and Society, University of California, Berkeley*. John Wiley & Sons.

McDermott, M. S., Oliver, M., Simnadis, T., Beck, E. J., Coltman, T., Iverson, D., Caputi, P., & Sharma, R. (2015). The theory of planned behaviour and dietary patterns: A systematic review and meta-analysis. *Preventive Medicine*, *81*, 150–156. https://doi.org/10.1016/j.ypmed.2015.08.020

McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J. (2011). Prospective prediction of health-related behaviours with the Theory of Planned Behaviour: A meta-analysis. *Health Psychology Review*, *5*(2), 97–144. https://doi.org/10.1080/17437199.2010.521684

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235

Menard, P., Warkentin, M., & Lowry, P. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, 147. https://doi.org/10.1016/j.cose.2018.01.020

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x

Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, *94*, 154–175. https://doi.org/10.1016/j.chb.2018.12.036

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nunnally, J. C. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Ogden, J. (2003). Some problems with social cognition models: A pragmatic and conceptual analysis. *Health Psychology*, *22*(4), 424. https://doi.org/10.1037/0278-6133.22.4.424

Olmstead, K., & Smith, A. (2017, January 26). Americans and cybersecurity. *Pew Research Center.* https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Osborne, J. W., Costello, A. B., & Kellow, J. T. (2008). Best practices in exploratory factor analysis. In *Best practices in quantitative methods* (pp. 86–99). SAGE.

Osgood, C. E. (1957). *The measurement of meaning*. University of Illinois Press.

Ouchi, W. G., & Maguire, M. A. (1975). Organizational control: Two functions. *Administrative Science Quarterly*, *20*(4), 559–569. https://doi.org/10.2307/2392023

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance*. Proceedings of the 40th Annual Hawaii International Conference on System Sciences.

Parsons, K., Agata, M., Pattinson, M., Butavicius, M., & Jerran, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334. https://doi.org/10.1108/IMCS-10-2013-0078

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51. https://www.journals.elsevier.com/computers-and-security

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, *52*, 194–206. https://doi.org/10.1016/j.cose.2015.02.008

Patel, P., Sarno, D. M., Lewis, J. E., Shoss, M., Neider, M. B., & Bohil, C. J. (2019). Perceptual representation of spam and phishing emails. *Applied Cognitive Psychology*, *33*(6), 1296–1304. https://doi.org/10.1002/acp.3594

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In *Communication and persuasion* (pp. 1–24). Springer.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. *Academy of Management Review*, *26*(2), 298–310. https://doi.org/10.2307/259124

Plotnikoff, R. C., Costigan, S. A., Karunamuni, N., & Lubans, D. R. (2013). Social cognitive theories used to explain physical activity behavior in adolescents: A systematic review and meta-analysis. *Preventive Medicine*, *56*(5), 245–253. https://doi.org/10.1016/j.ypmed.2013.01.013

Podsakoff, P. M., Mackenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*(1), 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*(4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09

Purkait, S. (2012). Phishing counter measures and their effectiveness: Literature review. *Information Management & Computer Security*, *20*(5), 382–420. http://dx.doi.org/10.1108/09685221211286548

Rich, A., Brandes, K., Mullan, B., & Hagger, M. S. (2015). Theory of planned behavior and adherence in chronic illness: A meta-analysis. *Journal of Behavioral Medicine*, *38*(4), 673–688. https://doi.org/10.1007/s10865-015-9644-3

Riebl, S. K., Estabrooks, P. A., Dunsmore, J. C., Savla, J., Frisard, M. I., Dietrich, A. M., Peng, Y., Zhang, X., & Davy, B. M. (2015). A systematic literature review and meta-analysis: The Theory

of Planned Behavior's application to understand and predict nutrition-related behaviors in youth. *Eating Behaviors*, *18*, 160–178. https://doi.org/10.1016/j.eatbeh.2015.05.016

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health Education Monographs*, *2*(4), 354–386. https://doi.org/10.1177/109019817400200405

RStudio Team. (2020). *RStudio: Integrated development for R.* PBC.

Sandberg, T., & Conner, M. (2008). Anticipated regret as an additional predictor in the theory of planned behaviour: A meta-analysis. *British Journal of Social Psychology*, *47*(4), 589–606. https://doi.org/10.1348/014466607X258704

Scalco, A., Noventa, S., Sartori, R., & Ceschi, A. (2017). Predicting organic food consumption: A meta-analytic structural equation model based on the theory of planned behavior. *Appetite*, *112*, 235–248. https://doi.org/10.1016/j.appet.2017.02.007

Schaffer, D. R., & Debb, S. M. (2019). Validation of the Online Security Behaviors and Beliefs Questionnaire with college students in the United States. *Cyberpsychology, Behavior, and Social Networking*, *22*(12), 766–770. https://home.liebertpub.com/publications/cyberpsychology-behavior-and-social-networking/

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723–757. https://doi.org/10.1080/07421222.2020.1790187

Schumacker, R. E. (2010). *A beginner's guide to structural equation modeling* (3rd ed.). Routledge.

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. *Advances in Experimental Social Psychology*, *25*, 1–65. https://doi.org/10.1016/S0065-2601(08)60281-6

Schwartz, S. H. (2003). A proposal for measuring value orientations across nations. *Questionnaire Package of the European Social Survey*, *259*(290), 261. https://www.europeansocialsurvey.org/methodology/ess_methodology/source_questionnaire/

Searle, J. R. (1983). *Intentionality: An essay in the philosophy of mind*. Cambridge University Press.

Sheeran, P. (2001). *Intention-behavior relations: A conceptual and empirical review*. John Wiley & Sons.

Sheeran, P., & Taylor, S. (1999). Predicting intentions to use condoms: A meta-analysis and comparison of the theories of reasoned action and planned behavior. *Journal of Applied Social Psychology*, *29*(8), 1624–1675. https://doi.org/10.1111/j.1559-1816.1999.tb02045.x

Sheeran, P., & Webb, T. L. (2016). The intention-behavior gap. *Social and Personality Psychology Compass*, *10*(9), 503–518. https://doi.org/10.1111/spc3.12265

Shein, E. (2011). The gods of phishing. *Infosecurity*, *8*(2), 28–31. https://doi.org/10.1016/S1754-4548(11)70023-7

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). *Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish* (Vol. 229). https://doi.org/10.1145/1280680.1280692

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, *15*(3), 325–343. https://consumerresearcher.com/

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. https://www.sciencedirect.com/journal/information-and-management

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289–305. https://doi.org/10.1057/ejis.2012.59

Sommestad, T., & Hallberg, J. (2013). *A review of the theory of planned behaviour in the context of information security policy compliance* (Vol. 405). https://doi.org/10.1007/978-3-642-39218-4_20

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H., & Hallberg, J. (2015a). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46. https://doi.org/10.4018/IJISP.2015010102

Sommestad, T., Karlzén, H., & Hallberg, J. (2015b). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200–217. https://doi.org/10.1108/ICS-04-2014-0025

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*, *59*(4), 344–353. https://www.tandfonline.com/toc/ucis20/current

Spitzmüller, C., & Stanton, J. M. (2006). Examining employee compliance with organizational surveillance and monitoring. *Journal of Occupational and Organizational Psychology*, *79*(2), 245–272. https://bpspsychub.onlinelibrary.wiley.com/doi/abs/10.1348/096317905X52607

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, *54*(3), 70–75. https://cacm.acm.org/

Stanislaw, H., & Todorov, N. (1999). Calculation of signal detection theory measures. *Behavior Research Methods, Instruments, & Computers*, *31*(1), 137–149. https://doi.org/10.3758/BF03203473

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://www.journals.elsevier.com/computers-and-security

Starfelt Sutton, L. C., & White, K. M. (2016). Predicting sun-protective intentions and behaviours using the theory of planned behaviour: A systematic review and meta-analysis. *Psychology & Health*, *31*(11), 1272–1292. https://doi.org/10.1080/08870446.2016.1204449

Steiger, J. H., & Lind, J. C. (1980). *Statistically based tests for the number of common factors*. Proceedings of the Annual Meeting of the Psychometric Sociality, Iowa.

Sun, J. C.-Y., Yu, S.-J., Lin, S. S. J., & Tseng, S.-S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249–257. https://doi.org/10.1016/j.chb.2016.02.004

Tabachnick, B. G. (2001). *Using multivariate statistics* (4th ed.). Allyn and Bacon.

Terranova Security. (2020). *2020 phishing benchmark report*. Author.

Topa, G., & Moriano, J. A. (2010). Theory of planned behavior and smoking: meta–analysis and SEM model. *Substance Abuse and Rehabilitation*, *1*, 23–33. https://doi.org/10.2147/SAR.S15168

Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, *2*(2), 121–136. https://doi.org/10.2307/3857567

Tyson, M., Covey, J., & Rosenthal, H. E. S. (2014). Theory of planned behavior interventions for reducing heterosexual risk behaviors: A meta-analysis. *Health Psychology*, *33*(12), 1454–1467. https://doi.org/10.1037/hea0000047

U.S. Bureau of Labor Statistics. (2021). *Employment status of the civilian population*. Author.

Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes*, *48*(8), 1565–1585. https://doi.org/10.1108/K-05-2018-0226

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Walser, R., Cram, W. A., Bernroider, E. W. N., & Wiener, M. (2021). Control choices and enactments in IS development projects: Implications for legitimacy perceptions and compliance intentions. *Information & Management*, *58*(7), 103522. https://www.sciencedirect.com/journal/information-and-management

Weber, S. (2017). Coercion in cybersecurity: What public health models reveal. *Journal of Cybersecurity*, *3*(3), 173–183. https://doi.org/10.1093/cybsec/tyx005

Whitman, M. (2008). Security policy: From design to maintenance. *Advances in Management Information Systems*, *11*, 123–151. https://aisel.aisnet.org/amcis2017/AdvancesIS/

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, *6*(1), tyaa001. https://doi.org/10.1093/cybsec/tyaa001

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives: Examining the influence of disgruntlement on computer abuse intentions. *Information Systems Journal*, *28*(2), 266–293. https://doi.org/10.1111/isj.12129

Workman, M. (2008a). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Workman, M. (2008b). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://asistdl.onlinelibrary.wiley.com/journal/23301643

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Wright, R. T., Ensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*(2), 385. https://pubsonline.informs.org/journal/isre

Yao, M., & Linz, D. (2008). Predicting self-protections of online privacy. *Cyberpsychology & Behavior*, *11*, 615–617. https://doi.org/10.1089/cpb.2007.0208

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behavior*, *23*(5), 605–633. https://onlinelibrary.wiley.com/journal/10991379

APPENDICES

A. FACTOR ANALYSES RESULTS FOR ALL SCENARIOS

(From Chapter 3 / 3.3.5 Factor Analysis)

Table A1

Factor Analysis Results for Scenario 1

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
At01	The recommendations my organization has in terms of handling personal information online are beneficial.	1.81	0.77	**0.83**	0.04	-0.01	0.01	0.07	0.06	-0.01
At02	The recommendations my organization has in terms of handling personal information online are complete.	1.98	0.83	-0.07	0.06	0.05	-0.05	0.13	0.01	**0.71**
At03	The recommendations my organization has in terms of handling personal information online are sufficient.	1.90	0.79	0.08	-0.02	-0.09	0.01	0.24	0.19	**0.53**
At06	The recommendations my organization has in terms of handling personal information online are important.	1.82	0.78	**0.36**	-0.21	0.10	0.00	0.03	0.12	0.26
At10	The recommendations my organization has in terms of handling personal information online are wise.	1.82	0.80	**0.45**	-0.02	0.01	0.03	0.28	0.05	0.13
At11	The recommendations my organization has in terms of handling personal information online are necessary.	1.79	0.77	**0.51**	-0.11	0.27	-0.02	-0.02	0.05	0.15
At13	The recommendations my organization has in terms of handling personal information online are precise.	2.02	0.74	0.31	0.15	-0.08	0.05	0.16	0.09	**0.33**
At14	The recommendations my organization has in terms of handling personal information online are hard.	2.69	1.22	-0.02	**0.89**	-0.02	-0.02	-0.03	0.01	0.03
At15	The recommendations my organization has in terms of handling personal information online are strong.	1.96	0.81	0.28	0.12	0.11	0.01	-0.11	-0.09	**0.61**
At16	The recommendations my organization has in terms of handling personal information online are severe.	2.59	1.17	-0.14	**0.72**	-0.08	-0.04	0.11	0.14	0.15
At17	The recommendations my organization has in terms of handling personal information online are constrained.	2.48	1.13	0.09	**0.79**	0.05	-0.10	0.06	0.01	-0.12
At18	The recommendations my organization has in terms of handling personal information online are complex.	2.64	1.14	0.05	**0.79**	0.07	0.01	-0.10	-0.10	0.03
Sn20	People at my work observe recommendations in terms of handling personal information.	1.98	0.77	0.25	-0.03	0.03	0.01	**0.30**	0.05	0.33
Sn21	People at my workplace follow recommendations in terms of handling personal information.	1.88	0.69	0.04	0.03	0.06	0.04	**0.78**	0.02	0.02
Sn22	People at my workplace act in a way that follows recommendations in terms of handling personal information.	1.92	0.81	0.19	-0.11	0.15	-0.08	**0.49**	-0.13	0.19

Table A1 (continue)

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
Sn24	How would people at your workplace be about John's decision?	2.95	1.21	0.01	-0.07	-0.07	**0.74**	-0.10	0.17	0.03
Sn25	How would people at your workplace feel about John's decision?	2.91	1.24	-0.01	-0.04	0.02	**0.85**	0.00	-0.04	-0.02
Sn27	How would people where you work be with John's decision?	2.92	1.20	0.00	0.02	0.04	**0.85**	0.07	-0.07	-0.03
Ar28	If you would have decided like John, answer whether the following statement is true to you." Things would have gone better if I had chosen another option to respond to the request from my colleague."	2.03	0.91	0.02	0.14	0.39	0.17	0.14	**0.20**	0.03
Ar30	If you would have decided like John, answer whether the following statement is true to you. "I should have decided differently to respond to the request from my colleague."	1.95	0.94	0.14	0.05	0.14	0.05	0.02	**0.75**	0.00
Ar32	If you would have decided like John, answer whether the following statement is true to you. "Before responding this way to the request from my colleague, I should have chosen a different way."	1.87	0.86	-0.04	0.02	0.48	-0.01	0.03	**0.46**	0.08
In33	In similar situations, I will not decide as John did.	2.02	1.04	-0.02	-0.06	**0.53**	0.02	-0.04	0.32	0.04
In34	I intend not to do as John did in similar situations.	1.94	1.00	0.00	0.04	**0.76**	0.09	-0.02	-0.04	0.14
In35	I plan to not respond as John did in similar situations.	1.96	0.96	0.03	0.01	**0.71**	-0.03	0.14	0.04	-0.08
In36	I will not do as John did if I am in similar situations.	1.97	1.04	0.12	0.02	**0.66**	0.10	0.06	0.10	-0.06

Note. N=182. Oblimin rotation, principal (axis) factor as the method of extraction.
M: mean. *SD*: Std dev. *PA*: Principal (axis) factor

Table A2

Factor Analysis Results for Scenario 2

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
At01	The recommendations my organization has in terms of handling personal information online are beneficial.	1.80	0.76	0.16	-0.05	0.10	0.05	**0.38**	0.30	0.02
At02	The recommendations my organization has in terms of handling personal information online are complete.	1.93	0.83	0.21	0.04	0.06	0.01	0.00	**0.60**	-0.04
At03	The recommendations my organization has in terms of handling personal information online are sufficient.	1.95	0.87	0.02	0.01	-0.05	-0.10	0.07	**0.65**	0.14
At06	The recommendations my organization has in terms of handling personal information online are important.	1.69	0.77	0.16	-0.06	0.02	0.06	**0.61**	0.01	0.02
At10	The recommendations my organization has in terms of handling personal information online are wise.	1.72	0.74	0.19	0.09	-0.02	0.05	**0.43**	0.05	0.22
At11	The recommendations my organization has in terms of handling personal information online are necessary.	1.71	0.80	-0.03	0.03	0.05	0.02	**0.74**	0.10	0.11
At13	The recommendations my organization has in terms of handling personal information online are precise.	2.01	0.91	0.09	-0.01	0.07	0.01	0.12	**0.66**	0.00
At14	The recommendations my organization has in terms of handling personal information online are hard.	2.51	1.26	0.03	**0.83**	-0.08	-0.02	-0.01	0.01	0.02
At15	The recommendations my organization has in terms of handling personal information online are strong.	1.94	0.87	0.21	0.01	0.19	0.00	0.10	**0.49**	-0.09
At16	The recommendations my organization has in terms of handling personal information online are severe.	2.33	1.13	-0.09	**0.56**	0.02	0.05	-0.11	0.37	0.19
At17	The recommendations my organization has in terms of handling personal information online are constrained.	2.29	1.05	0.04	**0.83**	0.06	-0.07	0.06	-0.13	-0.02
At18	The recommendations my organization has in terms of handling personal information online are complex.	2.48	1.24	0.01	**0.76**	0.01	-0.05	-0.03	0.04	-0.05
Sn20	People at my work observe recommendations in terms of handling personal information.	1.81	0.79	**0.75**	0.03	0.03	-0.03	0.05	0.03	0.05
Sn21	People at my workplace follow recommendations in terms of handling personal information.	1.83	0.79	**0.69**	0.01	0.00	0.06	0.02	0.13	0.11
Sn22	People at my workplace act in a way that follows recommendations in terms of handling personal information.	1.83	0.85	**0.38**	0.30	0.16	0.03	0.16	0.16	-0.09
Sn24	How would people at your workplace be about John's decision?	2.85	1.34	0.04	-0.02	0.05	**0.84**	-0.03	-0.03	-0.03
Sn25	How would people at your workplace feel about John's decision?	2.88	1.31	-0.02	-0.09	0.01	**0.74**	0.07	-0.02	-0.05
Sn27	How would people where you work be with John's decision?	2.80	1.30	-0.03	0.03	-0.04	**0.89**	0.00	0.00	0.04

Table A2 (continue)

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
Ar28	If you would have decided like John, answer whether the following statement is true to you. "Things would have gone better if I had chosen another option to respond to the request from my colleague."	1.80	0.87	0.13	0.07	0.05	0.05	0.09	0.03	**0.59**
Ar30	If you would have decided like John, answer whether the following statement is true to you. "I should have decided differently to respond to the request from my colleague."	1.88	0.89	0.04	0.14	0.24	0.03	0.22	-0.10	**0.52**
Ar32	If you would have decided like John, answer whether the following statement is true to you. "Before responding this way to the request from my colleague, I should have chosen a different way."	1.87	0.84	0.05	-0.08	0.12	-0.01	0.03	0.05	**0.72**
In33	In similar situations, I will not decide as John did.	1.89	1.02	-0.08	0.07	**0.82**	0.06	0.07	0.09	0.03
In34	I intend not to do as John did in similar situations.	2.01	1.05	-0.05	-0.06	**0.88**	-0.02	0.13	-0.02	-0.02
In35	I plan to not respond as John did in similar situations.	1.96	1.07	0.13	0.00	**0.70**	0.05	-0.10	0.01	0.11
In36	I will not do as John did if I am in similar situations.	1.97	1.06	0.10	0.01	**0.80**	0.01	-0.14	-0.02	0.09

Note. N=182. Oblimin rotation, principal (axis) factor as the method of extraction.
M: mean. *SD:* Std dev. *PA:* Principal (axis) factor

Table A3

Factor Analysis Results for Scenario 3

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
At01	The recommendations my organization has in terms of handling personal information online are beneficial.	1.82	0.76	0.11	-0.05	-0.11	-0.06	**0.68**	0.12	0.11
At02	The recommendations my organization has in terms of handling personal information online are complete.	2.14	0.95	**0.68**	0.07	0.15	-0.04	-0.03	-0.03	0.07
At03	The recommendations my organization has in terms of handling personal information online are sufficient.	2.00	0.93	**0.59**	-0.03	0.17	-0.04	0.01	-0.14	0.30
At06	The recommendations my organization has in terms of handling personal information online are important.	1.70	0.73	0.02	-0.03	0.03	0.00	**0.80**	0.05	-0.05
At10	The recommendations my organization has in terms of handling personal information online are wise.	1.76	0.83	0.05	0.06	0.09	0.07	**0.66**	-0.13	0.09
At11	The recommendations my organization has in terms of handling personal information online are necessary.	1.63	0.68	-0.15	0.00	0.25	0.04	**0.43**	0.11	0.22
At13	The recommendations my organization has in terms of handling personal information online are precise.	2.09	0.91	**0.74**	0.05	0.03	0.01	0.14	0.05	-0.04
At14	The recommendations my organization has in terms of handling personal information online are hard.	2.65	1.26	-0.02	**0.79**	-0.02	-0.09	-0.04	0.00	0.04
At15	The recommendations my organization has in terms of handling personal information online are strong.	1.96	1.00	**0.73**	0.03	-0.16	0.02	0.05	0.12	0.05
At16	The recommendations my organization has in terms of handling personal information online are severe.	2.37	1.19	0.30	**0.55**	0.06	-0.03	0.01	0.00	-0.01
At17	The recommendations my organization has in terms of handling personal information online are constrained.	2.29	1.03	-0.07	**0.71**	-0.08	-0.06	0.01	0.13	0.06
At18	The recommendations my organization has in terms of handling personal information online are complex.	2.56	1.24	0.05	**0.83**	0.02	-0.03	0.00	-0.03	-0.05
Sn20	People at my work observe recommendations in terms of handling personal information.	1.89	0.83	0.24	0.06	0.01	0.02	0.14	0.14	**0.42**
Sn21	People at my workplace follow recommendations in terms of handling personal information.	1.94	0.84	0.05	-0.01	0.01	-0.06	0.03	0.02	**0.84**
Sn22	People at my workplace act in a way that follows recommendations in terms of handling personal information.	1.90	0.83	0.13	0.18	-0.03	0.18	0.21	-0.05	**0.50**
Sn24	How would people at your workplace be about John's decision?	2.75	1.31	0.04	-0.07	-0.06	**0.85**	-0.04	0.05	0.00
Sn25	How would people at your workplace feel about John's decision?	2.69	1.24	-0.01	-0.12	-0.01	**0.73**	-0.06	0.12	0.07

Table A3 (continue)

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
Sn27	How would people where you work be with John's decision?	2.77	1.32	-0.05	0.00	0.10	**0.80**	0.10	-0.11	-0.09
Ar28	If you would have decided like John, answer whether the following statement is true to you. "Things would have gone better if I had chosen another option to respond to the request from my colleague."	1.77	0.82	0.02	0.14	0.06	0.06	0.19	**0.56**	-0.01
Ar30	If you would have decided like John, answer whether the following statement is true to you. "I should have decided differently to respond to the request from my colleague."	1.72	0.80	0.07	0.02	0.15	0.05	0.06	**0.68**	0.00
Ar32	If you would have decided like John, answer whether the following statement is true to you. "Before responding this way to the request from my colleague, I should have chosen a different way."	1.65	0.76	-0.01	-0.03	0.34	0.07	-0.02	**0.46**	0.22
In33	In similar situations, I will not decide as John did.	1.77	0.83	0.04	-0.16	**0.70**	-0.12	0.09	0.19	-0.01
In34	I intend not to do as John did in similar situations.	1.79	0.87	-0.03	0.02	**0.47**	0.24	0.07	0.02	0.17
In35	I plan to not respond as John did in similar situations.	1.83	0.92	-0.04	0.18	**0.51**	0.13	0.07	0.06	0.04
In36	I will not do as John did if I am in similar situations.	1.83	0.87	0.13	0.04	**0.63**	0.13	0.00	0.09	0.01

Note. N=182. Oblimin rotation, principal (axis) factor as the method of extraction.
M: mean. *SD*: Std dev. *PA*: Principal (axis) factor

Table A4

Factor analysis Results for Scenario 4

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
At01	The recommendations my organization has in terms of handling personal information online are beneficial.	1.76	0.78	0.19	-0.12	0.02	-0.06	0.21	0.07	**0.44**
At02	The recommendations my organization has in terms of handling personal information online are complete.	1.90	0.84	**0.56**	-0.01	-0.21	0.01	0.1	0.22	0.08
At03	The recommendations my organization has in terms of handling personal information online are sufficient.	1.79	0.82	**0.64**	0.1	0.05	-0.03	-0.04	-0.01	0.16
At06	The recommendations my organization has in terms of handling personal information online are important.	1.69	0.73	-0.02	-0.02	-0.05	0.1	0.19	0.1	**0.62**
At10	The recommendations my organization has in terms of handling personal information online are wise.	1.73	0.78	0.05	0.03	0.06	-0.02	-0.05	0.04	**0.85**
At11	The recommendations my organization has in terms of handling personal information online are necessary.	1.67	0.83	0.35	-0.17	0.15	-0.08	0.06	-0.02	**0.38**
At13	The recommendations my organization has in terms of handling personal information online are precise.	1.90	0.86	**0.75**	-0.02	0.15	-0.05	0.1	-0.07	0.02
At14	The recommendations my organization has in terms of handling personal information online are hard.	2.55	1.27	0.05	**0.79**	0.04	-0.12	-0.12	0.05	-0.08
At15	The recommendations my organization has in terms of handling personal information online are strong.	1.79	0.79	**0.63**	0.11	-0.02	0.07	0.14	0.1	0.08
At16	The recommendations my organization has in terms of handling personal information online are severe.	2.35	1.15	0.08	**0.81**	-0.04	0.07	0.11	-0.1	0.15
At17	The recommendations my organization has in terms of handling personal information online are constrained.	2.31	1.03	0.07	**0.59**	0.1	-0.22	0.01	0.08	-0.05
At18	The recommendations my organization has in terms of handling personal information online are complex.	2.53	1.22	-0.11	**0.81**	-0.02	-0.04	0.08	0.01	-0.05
Sn20	People at my work observe recommendations in terms of handling personal information.	1.79	0.73	0.31	0.01	-0.02	0.09	**0.39**	0.08	0.03
Sn21	People at my workplace follow recommendations in terms of handling personal information.	1.87	0.74	0.01	0.07	0.12	-0.07	**0.8**	-0.01	0.07
Sn22	People at my workplace act in a way that follows recommendations in terms of handling personal information.	1.77	0.71	0.13	0.02	-0.07	0.05	**0.65**	0.1	-0.05
Sn24	How would people at your workplace be about John's decision?	2.97	1.33	0.02	0	-0.04	**0.9**	-0.03	0.04	0.01
Sn25	How would people at your workplace feel about John's decision?	3.01	1.33	0.01	-0.12	0.14	**0.76**	-0.02	-0.06	-0.05
Sn27	How would people where you work be with John's decision?	2.97	1.31	-0.06	-0.01	0.07	**0.77**	0.03	0.02	0.02

Table A4 (continue)

Item	Description	M	SD	PA1	PA2	PA3	PA4	PA5	PA6	PA7
Ar28	If you would have decided like John, answer whether the following statement is true to you. "Things would have gone better if I had chosen another option to respond to the request from my colleague."	1.74	0.87	0.16	0.1	0.06	0.1	-0.06	**0.67**	0.03
Ar30	If you would have decided like John, answer whether the following statement is true to you. "I should have decided differently to respond to the request from my colleague."	1.74	0.87	-0.04	-0.07	0.11	-0.04	0.1	**0.77**	-0.03
Ar32	If you would have decided like John, answer whether the following statement is true to you. "Before responding this way to the request from my colleague, I should have chosen a different way."	1.68	0.82	-0.05	-0.01	0.06	0.01	-0.01	**0.8**	0.1
In33	In similar situations, I will not decide as John did.	1.84	0.98	-0.06	-0.02	**0.82**	0.03	-0.01	0.02	0.1
In34	I intend not to do as John did in similar situations.	1.78	0.94	0.14	-0.03	**0.76**	0.01	0.03	0.07	-0.03
In35	I plan to not respond as John did in similar situations.	1.77	0.95	-0.07	0.02	**0.73**	0.09	0.12	0.06	-0.06
In36	I will not do as John did if I am in similar situations.	1.76	0.90	0.08	0.05	**0.75**	0.07	-0.04	0.11	0.05

Note. N=182. Oblimin rotation, principal (axis) factor as the method of extraction.
M: mean. *SD:* Std dev. *PA:* Principal (axis) factor

B. MATERIALS

(From Chapter 3 / 3.4.3 Measures)

Table B1

Scenarios

Introduction
Emailing personal information is typically not recommended in organizational policies, as it could lead to security incidents. Some organizations have secure systems in place that allow employees to access and share personal information if that is required. However, due to a lack of resources or privacy concerns, it is difficult for organizations to monitor whether employees email personal information or whether they use secure systems to do it. Besides, people deal with day-by-day situations such as the following:
Scenario 01, Value enacted: Power. N=183
"John works at a manufacturing company. People at work believe he values having authority over people and resources, always wanting to determine how those resources should be used. John receives an email asking for some personal information from his supervisor, and John, seeing this event as a possible opportunity for him to gain status at his company, decided to email the required information."
Scenario 02, Value enacted: Achievement. N=170
"John works at a manufacturing company. People at work believe he is a very competent co-worker, always wanting to perform well at what he does at work. John receives an email from someone at work asking to email some personal information as part of a task, and John, wanting to perform as efficiently as he normally does, decided to accomplish the task as required."
Scenario 03, Value enacted: Self-direction. N=174
"John works at a manufacturing company. People at work believe he is the type of person that likes to make his own decisions regarding work tasks, always wanting to determine how he organizes and executes them. John receives a request to share some personal information from someone at work. He figured that the best way to answer to this request was emailing the requested information, and he did."
Scenario 04, Value enacted: Benevolence. N=194
"John works at a manufacturing company. People at work believe he is a very supportive co-worker, always willing to help. John receives an email asking for some personal information from a colleague, and John, out of professional courtesy, decided to email the required information."

Table B2

Predictor's Scale

Item	Description	Scale and range
At01	The recommendations my organization has in terms of handling personal information online are beneficial.	strongly agree (1) to strongly disagree (5)
At02	The recommendations my organization has in terms of handling personal information online are important.	
At03	The recommendations my organization has in terms of handling personal information online are wise.	
At04	The recommendations my organization has in terms of handling personal information online are necessary.	
At05	The recommendations my organization has in terms of handling personal information online are complete.	
At06	The recommendations my organization has in terms of handling personal information online are sufficient.	
At07	The recommendations my organization has in terms of handling personal information online are precise.	
At08	The recommendations my organization has in terms of handling personal information online are strong.	
At09	The recommendations my organization has in terms of handling personal information online are hard.	
At10	The recommendations my organization has in terms of handling personal information online are severe.	
At11	The recommendations my organization has in terms of handling personal information online are constrained.	
At12	The recommendations my organization has in terms of handling personal information online are complex.	
Sn13	People at my work observe recommendations in terms of handling personal information.	
Sn14	People at my workplace follow recommendations in terms of handling personal information.	
Sn15	People at my workplace act in a way that follows recommendations in terms of handling personal information.	
Sn16	How would people at your workplace be about John's decision?	strongly unfavorable (1) to strongly favorable (5)
Sn17	How would people at your workplace feel about John's decision?	
Sn18	How would people where you work be with John's decision?	
Ar19	If you would have decided like John, answer whether the following statement is true to you. "Things would have gone better if I had chosen another option to respond to the request from my colleague."	strongly agree (1) to strongly disagree (5)
Ar20	If you would have decided like John, answer whether the following statement is true to you. "I should have decided differently to respond to the request from my colleague."	
Ar21	If you would have decided like John, answer whether the following statement is true to you. "Before responding this way to the request from my colleague, I should have chosen a different way."	
In22	In similar situations, I will not decide as John did.	
In23	I intend not to do as John did in similar situations.	
In24	I plan to not respond as John did in similar situations.	
In25	I will not do as John did if I am in similar situations.	

Table B3

Additional Questions

Closed-ended questions	
Ad01	Does your organization have in place a secure webpage or other similar systems that allow employees to enter and get personal information at work?
Ad02	Does your organization monitor what you send by email?
Yes or no options	
Open-ended questions	
Ad03	In your opinion, why are important and necessary the recommendations your organization provides in terms of handling personal information online?
Ad04	From your point of view, what makes complete, precise, and sufficient the recommendations that your organization provides in terms of handling personal information online?
Ad05	In your view, what makes severe, hard, and constrained the recommendations that your organization provides in terms of handling personal information online?

Table B4

Williams's Scale (Williams & Joinson, 2020)

Item	Description
W01	Losing data privacy as a result of responding to a phishing email would be a serious problem for me.
W02	If I were to fall victim to a phishing email, the consequences could be severe.
W03	I believe that falling victim to a phishing email is serious.
W04	Being exposed to computer viruses or malicious applications as a result of responding to a phishing email would be a serious problem for me.
W05	Having my online identity stolen as a result of responding to a phishing email would be a serious problem for me.
W06	It is possible that I will fall victim to a phishing attack.
W07	It is possible that I will fall victim to a phishing email.
W08	I am at risk of falling victim to a phishing email.
W09	I feel that I could be vulnerable to phishing emails.
W10	It is likely that I will fall victim to a phishing email.
W11	If I keep up to date with phishing techniques, I am less likely to fall victim to a phishing email.
W12	Keeping up to date with phishing techniques will prevent me from falling victim to phishing emails.
W13	If I keep up to date with phishing techniques, I will lessen my chances of responding to a phishing email.
W14	It would be easy for me to keep up to date with phishing techniques.
W15	I am able to keep up to date with phishing techniques.
W16	I feel confident in my ability to keep up to date with phishing techniques.
W17	I feel confident in my ability to spot phishing emails.
W18	I am able to spot phishing emails.
W19	I think that I could spot a phishing email by myself.
W20	Trying to keep up to date with phishing techniques would cause me too many problems.
W21	Keeping up to date with phishing techniques takes a large amount of time.
W22	Keeping up to date with phishing techniques requires significant effort.

Note. Items were scored in a 5-points Likert scale from *strongly agree* (1) to *strongly disagree* (5)

Table B5

Social Desirability Scale (Hays et al., 1989)

Item	Description
Sd01	I am always courteous even with people who are disagreeable:
Sd02	There have been occasions when I took advantage of someone:
Sd03	I sometimes try to get even rather than forgive and forget:
Sd04	I sometimes feel resentful when I do not get my way:
Sd05	No matter who I am talking to, I am always a good listener:

Note. Options: (1) *Definitely true* to (5) *definitely false*. For Items 1 and 5, option 1 is score 1, and the other options, 0. For items 2, 3, and 4, option 5 is scored 1, and the other options 0.

C. FACTORIAL INVARIANCE ANALYSES ACROSS SAMPLES

(From Chapter 3 / 3.4.8 Factorial Invariance Analysis)

C1 Factorial Invariance Analysis Across Scenarios

The modified six-factor solution was cross-validated using multigroup analysis of factorial invariance with baseline data from scenarios 1 to 4. The results are provided in Table C1.1, and Table C1.2 provides item loads and fit indexes for the invariant solution. The test of configural invariance, which involves a comparison of elements within the matrix of variances and covariances underlying the measurement model, resulted in an acceptable model fit, chi-square ($\chi 2$) = 759.156, df = 620, $p < 0.001$, CFI = 0.979, RMSEA = 0.037 (90% CI = 0.027 – 0.046), SRMR = 0.049. Although the chi-square ($\chi 2$) was statistically significant, the CFI exceeded 0.95, RMSEA was below 0.06, and the SRMR was below 0.08. Thus, the measurement model was configural invariant across scenarios. The test of metric invariance, which involves a comparison of indicators – latent variables loads, resulted in an acceptable fit, chi-square ($\chi 2$) = 809.262, df = 662, $p < 0.001$, CFI = 0.978, RMSEA = 0.037 (90% CI = 0.027 – 0.045), SRMR = 0.055. Although the chi-square ($\chi 2$) was statistically significant, CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08. There was no difference between models constraining the factor structure (configural invariant) and factor loadings (metric invariant); the difference test was non-significant, chi-square ($\chi 2$) diff = 50.105, df = 42, p-value = 0.1828 and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was metrically invariant across scenarios. The test of scalar invariance, which involves a comparison of intercepts, resulted in an acceptable fit, chi-square ($\chi 2$) = 847.627, df = 704, $p < 0.001$, CFI = 0.979, RMSEA = 0.035 (90% CI = 0.025 – 0.044), SRMR = 0.056. Although the chi-square ($\chi 2$) was statistically significant, the CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08. There was no difference between models constraining the factor loadings (metric invariant) and intercepts (scalar invariant); the difference test was non-significant, chi-square ($\chi 2$) diff = 38.365, df = 42, p-value = 0.6313 and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was scalar invariant across scenarios.

Table C1.1

Model Parameters and Factorial Invariance Across Scenarios

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
Sc01 (n=170)	191.904 P = 0.023	155	0.977	0.037 [0.015-0.054]	0.045
Sc02 (n=153)	178.318 P=0.097	155	0.985	0.031 [0.000-0.051]	0.053
Sc03 (n=159)	197.436 P=0.012	155	0.973	0.041 [0.021-0.058]	0.051
Sc04 (n=179)	191.498 P=0.025	155	0.982	0.036 [0.014-0.052]	0.048
Configural invariant	759.156 (p<0.001)	620	0.979	0.037 [0.027-0.046]	0.049
Metric invariant	809.262 (p<0.001)	662	0.978	0.037 [0.027-0.045]	0.055
Scalar invariant	847.627 (p<0.001)	704	0.979	0.035 [0.025-0.044]	0.056

Note. N=661. Sc: Scenario. df: degrees of freedom. . chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	50.105	42	0.1828	0.001
Metric invariance vs. Scalar invariant	38.365	42	0.6313	0.001

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C1.2

Items Loads and Fit Indexes Across Scenarios for the Invariant Modified Six-Factors Solution

		Scenario 1 (n=170)		Scenario 2 (n=153)		Scenario 3 (n=159)		Scenario 4 (n=179)	
Factor	Indicator	Ustd	Std	Ustd	Std	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.714	1.000	0.749	1.000	0.776	1.000	0.785
	At02	0.897	0.632	0.897	0.769	0.897	0.748	0.897	0.789
	At03	1.007	0.738	1.007	0.806	1.007	0.784	1.007	0.797
	At04	0.971	0.727	0.971	0.704	0.971	0.794	0.971	0.828
ATC	At05	1.000	0.802	1.000	0.816	1.000	0.776	1.000	0.825
	At06	0.913	0.773	0.913	0.779	0.913	0.697	0.913	0.807
	At07	1.045	0.821	1.045	0.809	1.045	0.759	1.045	0.812
MSR	At09	1.000	0.717	1.000	0.863	1.000	0.750	1.000	0.795
	At11	0.708	0.568	0.708	0.649	0.708	0.609	0.708	0.660
	At12	0.854	0.615	0.854	0.763	0.854	0.647	0.854	0.696
DN	Sn13	1.000	0.711	1.000	0.807	1.000	0.756	1.000	0.769
	Sn14	1.111	0.797	1.111	0.831	1.111	0.784	1.111	0.929
	Sn15	1.022	0.812	1.022	0.833	1.022	0.739	1.022	0.857
Inj	Sn16	1.000	0.801	1.000	0.851	1.000	0.866	1.000	0.867
	Sn17	0.919	0.714	0.919	0.789	0.919	0.818	0.919	0.744
	Sn18	0.988	0.853	0.988	0.835	0.988	0.859	0.988	0.793
IN	In22	1.000	0.749	1.000	0.750	1.000	0.873	1.000	0.838
	In23	0.872	0.805	0.872	0.709	0.872	0.708	0.872	0.685
	In24	0.934	0.761	0.934	0.746	0.934	0.627	0.934	0.797
	In25	0.978	0.788	0.978	0.818	0.978	0.829	0.978	0.845

Note. Null model: chi-square ($\chi2$) = 7511.854, df = 760, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi2$) =847.627, df = 704, $p < 0.001$, CFI = 0.979, RMSEA = 0.035 (90% CI = 0.025 – 0.044), SRMR = 0.056.

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C2 Factorial Invariance for yes/no Answers to Ad01 (have systems?)

Factorial invariance of the modified six-factors solution was examined among those who answered yes/no to whether their organizations have systems in place to help employees share information securely (Ad01). The analysis was made with baseline data from 661 valid responses separated into two groups; 476 participants answered yes, and 185 answered no. The results are provided in Table C2.1, and Table C2.2 provides item loads and fit indexes for the invariant solution. Model fit was good in the sample "yes", chi-square ($\chi 2$) = 212.055, df = 155, p = 0.002, CFI = 0.987, RMSEA = 0.028 (90% CI = 0.018 – 0.037), SRMR = 0.037. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Model fit was good in the sample "no", chi-square ($\chi 2$) = 204.326, df = 155, p = 0.005, CFI = 0.975, RMSEA = 0.041 (90% CI = 0.024 – 0.056), SRMR = 0.038. The chi-square ($\chi 2$) was statistically significant, the RMSEA was below the limit of 0.06, the SRMR was below 0.08, and the CFI slightly exceeded the limit of 0.95.

The results of the invariance routine are shown in Table C2.1. The test of configural invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 416.381, df = 310, p < 0.000, CFI = 0.983, RMSEA = 0.032 (90% CI = 0.024 – 0.040), SRMR = 0.037. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Thus, the measurement model was configural invariant for Ad01 responses. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 433.310, df = 324, p < 0.001, CFI = 0.983, RMSEA = 0.032 (90% CI = 0.023 – 0.040), SRMR = 0.041. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below the limit 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the difference was not significant, chi-square ($\chi 2$) diff = 16.929, df = 14, p value = 0.26), and the CFI was overlapping (Delta CFI < 0.01). Thus, the measurement model was metric invariant for Ad02 responses. The test of scalar invariance resulted in a good model fit, chi-square ($\chi 2$) = 445.743, df = 338, p < 0.001, CFI = 0.983, RMSEA = 0.031 (90% CI = 0.023 – 0.039), SRMR = 0.041. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining factor loadings (metric invariant) and intercepts (scalar invariant) were invariant; the difference was not significant (chi-square ($\chi 2$) diff = 12.433, df = 14, p value = 0.5715), the CFI was overlapping (Delta CFI < 0.01). Thus, the measurement model was scalar invariant for Ad02 between respondents that answer yes/no to the inquiry of whether their organizations have systems in place to help them share information securely.

Table C2.1

Factorial Invariance for Ad01 (Does Your Organization Have Secure Systems for Data Sharing?)

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
"yes" (n=476)	212.055 p=0.002	155	0.987	0.028 [0.018-0.037]	0.037
"no" (n=185)	204.326 p=0.005	155	0.975	0.041 [0.024-0.056]	0.038
Configural invariant	416.381 p<0.001	310	0.983	0.032 [0.024-0.040]	0.037
Metric invariant	433.310 (p<0.001)	324	0.983	0.032 [0.023-0.040]	0.041
Scalar invariant	445.743 (p<0.001)	338	0.983	0.031 [0.023-0.039]	0.041

Note. N=661. df: degrees of freedom. . chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Configural invariant vs Metric invariance	16.929	14	0.26	0.000
Metric invariant vs Scalar invariant	12.433	14	0.5715	0.000

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C2.2

Items Loads and Fit Indexes Between Yes/No Respondents to Ad01 for the Invariant Modified Six-Factors Solution

		"yes" (n=476)		"no" (n=185)	
Factor	Indicator	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.701	1.000	0.855
	At02	0.898	0.711	0.898	0.758
	At03	0.994	0.737	0.994	0.827
	At04	0.947	0.716	0.947	0.804
ATC	At05	1.000	0.787	1.000	0.807
	At06	0.928	0.754	0.928	0.780
	At07	1.058	0.795	1.058	0.803
MSR	At09	1.000	0.762	1.000	0.741
	At11	0.740	0.643	0.740	0.559
	At12	0.862	0.672	0.862	0.617
DN	Sn13	1.000	0.751	1.000	0.751
	Sn14	1.102	0.819	1.102	0.845
	Sn15	1.023	0.798	1.023	0.817
Inj	Sn16	1.000	0.843	1.000	0.900
	Sn17	0.927	0.759	0.927	0.824
	Sn18	0.965	0.831	0.965	0.797
IN	In22	1.000	0.839	1.000	0.714
	In23	0.865	0.702	0.865	0.747
	In24	0.924	0.746	0.924	0.671
	In25	0.982	0.812	0.982	0.846

Note. Null model: chi-square ($\chi2$) = 6797.444, df = 380, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi2$) = 445.743, df = 338, $p < 0.001$, CFI = 0.983, RMSEA = 0.031 (90% CI = 0.023 – 0.039), SRMR = 0.041.

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C3 Factorial Invariance for yes/no Answers for Ad02 (email monitor?)

Factorial invariance of the six-factors solution was examined among those that answered yes/no to the inquiry of whether their organizations monitor their email accounts. The analysis was made with baseline data being the 661 valid responses distributed in 447 that answered yes and 214 that answered no. The results are provided in Table C3.1, and Table C3.2 provides item loads and fit indexes for the invariant solution. Model fit was acceptable in the sample "yes", chi-square ($\chi 2$) = 212.762, df = 155, p < 0.001, CFI = 0.986, RMSEA = 0.029 (90% CI = 0.018 – 0.028), SRMR = 0.036. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Model fit was good in the sample "no", chi-square ($\chi 2$) = 175.323, df = 155, p = 0.126, CFI = 0.991, RMSEA = 0.025 (90% CI = 0.000 – 0.041), SRMR = 0.038. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below the limit of 0.06, the SRMR was below 0.08, and the CFI slightly exceeded the limit of 0.95.

The results of the invariance routine are shown in Table C3.1. The test of configural invariance, resulted in a good model fit, chi-square ($\chi 2$) = 388.085, df = 310, p = 0.002, CFI = 0.988, RMSEA = 0.028 (90% CI = 0.018 – 0.036), SRMR = 0.037. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Thus, the measurement model was configural invariant for Ad03 responses. The test of metric invariance resulted in a good fit, chi-square ($\chi 2$) = 401.538, df = 324, p = 0.002, CFI = 0.988, RMSEA = 0.028 (90% CI = 0.018 – 0.036), SRMR = 0.037. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below the limit 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the difference was not significant (chi-square ($\chi 2$) diff = 13.453, df = 14, p value = 0.4912), the CFI was overlapping (Delta CFI < 0.01). Thus, the measurement model was metric invariant for Ad03 responses. The test of scalar invariance, resulted in a good fit, chi-square ($\chi 2$) = 419.855, df = 338, p = 0.002, CFI = 0.987, RMSEA = 0.027 (90% CI = 0.017 – 0.035), SRMR = 0.041. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The models constraining the factor loadings (metric invariant) and intercepts (scalar invariant) were invariant; the difference test was no significant (chi-square ($\chi 2$) diff = 18.317, df = 14, p-value = 0.1927) the CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was scalar invariant between respondents that answer yes/no to the inquiry of whether their organizations have systems in place to help them share information securely.

Table C3.1

Factorial Invariance for Ad02 (Does Your Organization Monitor Your Email Account?)

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
"yes" (n=447)	212.762 (p<0.001)	155	0.986	0.029 [0.018-0.028]	0.036
"no" (n=214)	175.323 P=0.126	155	0.991	0.025 [0.000-0.041]	0.038
Configural invariant	388.085 p=0.002	310	0.988	0.028 [0.018-0.036]	0.037
Metric invariant	401.538 p=0.002	324	0.988	0.027 [0.017-0.035]	0.040
Scalar invariant	419.855 p=0.002	338	0.987	0.027 [0.017-0.035]	0.041

Note. N=661. df: degrees of freedom. . chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	13.453	14	0.4912	0.000
Metric invariant vs. Scalar invariant	18.317	14	0.1927	0.001

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C3.2

Items Loads and Fit Indexes Between Yes/No Respondents to Ad02 for the Invariant Modified Six-Factors Solution

		"yes" (n=447)		"no" (n=214)	
Factor	Indicator	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.734	1.000	0.785
	At02	0.908	0.722	0.908	0.756
	At03	1.006	0.760	1.006	0.805
	At04	0.945	0.734	0.945	0.763
ATC	At05	1.000	0.808	1.000	0.782
	At06	0.923	0.785	0.923	0.734
	At07	1.046	0.794	1.046	0.796
MSR	At09	1.000	0.787	1.000	0.684
	At11	0.732	0.638	0.732	0.571
	At12	0.868	0.680	0.868	0.633
DN	Sn13	1.000	0.748	1.000	0.747
	Sn14	1.108	0.793	1.108	0.870
	Sn15	1.033	0.788	1.033	0.822
Inj	Sn16	1.000	0.850	1.000	0.845
	Sn17	0.919	0.745	0.919	0.826
	Sn18	0.985	0.827	0.985	0.835
IN	In22	1.000	0.795	1.000	0.771
	In23	0.881	0.697	0.881	0.738
	In24	0.927	0.690	0.927	0.746
	In25	1.002	0.804	1.002	0.848

Note. Null model: chi-square ($\chi 2$) = 6702.113, df = 380, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi 2$) = 419.855, df = 338, p = 0.002, CFI = 0.987, RMSEA = 0.027 (90% CI = 0.017 – 0.035), SRMR = 0.041.

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C4 Factorial Invariance Across Age Groups

Factorial invariance of the modified six-factors solution was examined across age groups with baseline data from four groups (661 valid responses). The results are provided in Table C4.1 and Table C4.2 provides item loads and fit indexes for the invariant solution. The ages were combined to have similar and acceptable sample size. The groups were, age1 (18-34 years old, n=166), age3 (35-44 years old, n=167), age4 (45-54 years old, n=131) and age5 (55 years old and over, n=197). Model fit was good in the sample age1, chi-square ($\chi 2$) = 151.088, df = 155, p = 0.574, CFI = 1, RMSEA = 0.000 (90% CI = 0.000 – 0.033), SRMR = 0.046. The chi-square ($\chi 2$) was not statistically significant, CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08. Model fit was acceptable in the sample age3, chi-square ($\chi 2$) = 208.530, df = 155, p = 0.003, CFI = 0.968, RMSEA = 0.045 (90% CI = 0.028 – 0.061), SRMR = 0.050.Although the chi-square ($\chi 2$) was statistically significant at p < 0.01, the CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08. Model fit was acceptable in the sample age4, chi-square ($\chi 2$) = 213.265, df = 155, p = 0.001, CFI = 0.953, RMSEA = 0.054 (90% CI = 0.034 – 0.70), SRMR = 0.057. Although the chi-square ($\chi 2$) was statistically significant, the CFI was above to the minimum acceptable (0.95), the RMSEA was below 0.06, and the SRMR was below 0.08. Model fit was acceptable in the sample age5, chi-square ($\chi 2$) = 199.555, df = 155, p = 0.009, CFI = 0.982, RMSEA = 0.038 (90% CI = 0.020 – 0.053), SRMR = 0.042. The chi-square ($\chi 2$) was statistically significant at p-value < 0.01, but CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08.

The results of the invariance routine are shown in Table C4.1. The test of configural invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 772.438, df = 620, p < 0.001, CFI = 0.977, RMSEA = 0.039 (90% CI = 0.029 – 0.047), SRMR = 0.048. Although the chi-square ($\chi 2$) was statistically significant, CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08. Thus, the measurement model was configural invariant across age groups. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 824.088, df = 662, p < 0.001, CFI = 0.976, RMSEA = 0.038 (90% CI = 0.029 – 0.047), SRMR = 0.056. Although the chi-square ($\chi 2$) was statistically significant, CFI exceeded 0.95, the RMSEA was below 0.06, and the SRMR was below 0.08. Models constraining the factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the difference test was not significant, chi-square ($\chi 2$) diff (df=42) = 51.65, p value = 0.1462. Thus, the measurement model was metric invariant across age groups. The test of scalar invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 877.860, df = 704, p < 0.001, CFI = 0.974, RMSEA = 0.039 (90% CI = 0.030 – 0.047), SRMR = 0.057. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. There was no difference between models constraining the loadings (metric invariant) and intercepts (scalar invariant); the difference test was non-

significant, chi-square ($\chi 2$)diff (df=42) = 53.772, p value = 0.1053 and CFI was overlapping (Delta CFI < 0.01). Thus, the measurement model was scalarly invariant across age groups.

Table C4.1

Factorial Invariance Across Age Groups

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
Age1 18 – 34 years old (n=166)	151.088 P=0.574	155	1.000	0.000 [0.000-0.033]	0.046
Age3 35 – 44 years old (n=167)	208.530 p=0.003	155	0.968	0.045 [0.028-0.061]	0.050
Age4 45 – 54 years old (n=131)	213.265 p=0.001	155	0.953	0.054 [0.034-0.070]	0.057
Age5 55 years old and over (n=197)	199.555 p=0.009	155	0.982	0.038 [0.020-0.053]	0.042
Configural invariant	772.438 p<0.001	620	0.977	0.039 [0.029-0.047]	0.048
Metric invariant	824.088 p<0.001	662	0.976	0.038 [0.029-0.047]	0.056
Scalar invariant	877.860 p<0.001	704	0.974	0.039 [0.030-0.047]	0.057

Note. N=661. df: degrees of freedom. . chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	51.65	42	0.1462	0.001
Metric invariant vs. Scalar invariant	53.772	42	0.1053	0.002

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014)

Table C4.2

Items Loads and Fit Indexes Across Age Groups for the Invariant Modified Six-Factors Solution

		Age1 (18-24 years old) (n=166)		Age3 (35-44 years old) (n=167)		Age4 (45-54 years old) (n=131)		Age5 (55 years old and over) (n=197)	
Factor	Indicator	Ustd	Std	Ustd	Std	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.742	1.000	0.726	1.000	0.742	1.000	0.804
	At02	0.901	0.724	0.901	0.693	0.901	0.743	0.901	0.776
	At03	1.012	0.783	1.012	0.764	1.012	0.753	1.012	0.827
	At04	0.943	0.730	0.943	0.717	0.943	0.804	0.943	0.761
ATC	At05	1.000	0.731	1.000	0.803	1.000	0.829	1.000	0.828
	At06	0.930	0.739	0.930	0.792	0.930	0.706	0.930	0.811
	At07	1.052	0.768	1.052	0.791	1.052	0.796	1.052	0.833
MSR	At09	1.000	0.754	1.000	0.790	1.000	0.682	1.000	0.754
	At11	0.747	0.621	0.747	0.711	0.747	0.613	0.747	0.553
	At12	0.890	0.673	0.890	0.707	0.890	0.623	0.890	0.679
DN	Sn13	1.000	0.688	1.000	0.723	1.000	0.784	1.000	0.801
	Sn14	1.117	0.736	1.117	0.872	1.117	0.815	1.117	0.899
	Sn15	1.028	0.687	1.028	0.868	1.028	0.795	1.028	0.871
Inj	Sn16	1.000	0.867	1.000	0.823	1.000	0.793	1.000	0.887
	Sn17	0.926	0.768	0.926	0.753	0.926	0.689	0.926	0.832
	Sn18	0.987	0.849	0.987	0.772	0.987	0.834	0.987	0.877
IN	In22	1.000	0.775	1.000	0.837	1.000	0.728	1.000	0.843
	In23	0.867	0.658	0.867	0.691	0.867	0.786	0.867	0.769
	In24	0.920	0.716	0.920	0.776	0.920	0.679	0.920	0.699
	In25	0.963	0.793	0.963	0.808	0.963	0.753	0.963	0.874

Note. Null model: chi-square ($\chi2$) = 7511.854, df = 760, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi2$) =877.860, df = 704, $p < 0.001$, CFI = 0.974, RMSEA = 0.039 (90% CI = 0.030 – 0.047), SRMR = 0.057.

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C5 Factorial Invariance Across Gender

Factorial invariance of the modified six-factors solution was examined between males (n=301) and females (n=360) with baseline data from two groups (661 valid responses). The results are provided in Table C5.1 and Table C5.2 provides item loads and fit indexes for the invariant solution. Model fit was good for males, chi-square ($\chi 2$) = 173.248, df = 155, p = 0.150, CFI = 0.993, RMSEA = 0.020 (90% CI = 0.000 – 0.034), SRMR = 0.036. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Model fit was acceptable for females, chi-square ($\chi 2$) = 207.391, df = 155, p = 0.003, CFI = 0.987, RMSEA = 0.031 (90% CI = 0.018 – 0.041), SRMR = 0.037. The chi-square ($\chi 2$) was statistically significant at a p value < 0.01, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95.

The results of the invariance routine are shown in Table C5.1. The test of configural invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 380.640, df = 310, p = 0.004, CFI = 0.989, RMSEA = 0.026 (90% CI = 0.016 – 0.035), SRMR = 0.036. Although the chi-square ($\chi 2$) was statistically significant at a p value 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Thus, the measurement model was configural invariant across gender. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 392.382, df = 324, p = 0.005, CFI = 0.990, RMSEA = 0.025 (90% CI = 0.015 – 0.034), SRMR = 0.038. Although the chi-square ($\chi 2$) was statistically significant at a p value < 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining the factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the difference test was not significant, chi-square ($\chi 2$) diff = 11.742, df = 14, p value = 0.627 and the CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was metric invariant across gender. The test of scalar invariance, resulted in a good fit, chi-square ($\chi 2$) = 409.996, df = 338, p = 0.004, CFI = 0.989, RMSEA = 0.025 (90% CI = 0.015 – 0.034), SRMR = 0.039. Although the chi-square ($\chi 2$) was statistically significant at a p value < 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. There was no difference between models constraining the factor loadings (metric invariant) and intercepts (scalar invariant); the difference test was non-significant, and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was scalarly invariant across gender.

Table C5.1

Factorial Invariance Across Gender

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Male (n=301)	173.248 p=0.150	155	0.993	0.020 [0.000-0.034]	0.036
Female (n=360)	207.391 p=0.003	155	0.987	0.031 [0.018-0.041]	0.037
Configural invariant	380.640 p=0.004	310	0.989	0.026 [0.016-0.035]	0.036
Metric invariant	392.382 p=0.005	324	0.990	0.025 [0.015-0.034]	0.038
Scalar invariant	409.996 p=0.004	338	0.989	0.025 [0.015-0.034]	0.039

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	11.742	14	0.627	0.001
Metric invariant vs. Scalar invariant	17.614	14	0.2249	0.001

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C5.2

Items Loads And Fit Indexes for the Invariant Modified Six-Factors Solution Across Gender

		Male (n=301)		Female (n=360)	
Factor	Indicator	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.748	1.000	0.762
	At02	0.911	0.736	0.911	0.743
	At03	1.007	0.785	1.007	0.779
	At04	0.950	0.736	0.950	0.766
ATC	At05	1.000	0.787	1.000	0.814
	At06	0.929	0.776	0.929	0.769
	At07	1.050	0.823	1.050	0.785
MSR	At09	1.000	0.800	1.000	0.749
	At11	0.727	0.653	0.727	0.610
	At12	0.858	0.734	0.858	0.621
DN	Sn13	1.000	0.726	1.000	0.790
	Sn14	1.091	0.801	1.091	0.852
	Sn15	1.016	0.807	1.016	0.812
Inj	Sn16	1.000	0.825	1.000	0.882
	Sn17	0.911	0.738	0.911	0.786
	Sn18	0.973	0.790	0.973	0.866
IN	In22	1.000	0.721	1.000	0.840
	In23	0.884	0.666	0.884	0.753
	In24	0.933	0.673	0.933	0.748
	In25	1.005	0.810	1.005	0.832

Note. Null model: chi-square ($\chi 2$) = 6975.193, df = 380, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi 2$) = 409.996, df = 338, p = 0.004, CFI = 0.989, RMSEA = 0.025 (90% CI = 0.015 – 0.034), SRMR = 0.039.
ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C6 Factorial Invariance Across Groups with Different Levels of Education

Factorial invariance of the modified six-factors solution was examined across groups of different levels of education with baseline data from four groups of different education level (661 valid responses). The results are provided in Table C6.1 and Table C6.2 provides item loads and fit indexes for the invariant solution. The groups were combined to have similar and acceptable sample sizes. The groups were, edu1 (high school graduate, no college, and less than high school diploma, n=124), edu3 (some college, no degree and associate degree, n=192), ed5 (bachelor's degree, n=217), and edu6 (advance degree, n=128). Model fit was good in the sample edu1, chi-square ($\chi 2$) = 162.651, df = 155, p = 0.321, CFI = 0.992, RMSEA = 0.020 (90% CI = 0.000 – 0.047), SRMR = 0.053. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Model fit was acceptable in the sample edu3, chi-square ($\chi 2$) = 248.975, df = 155, p < 0.001, CFI = 0.954, RMSEA = 0.056 (90% CI = 0.043 – 0.069), SRMR = 0.051. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded the limit 0.95. Model fit was good in the sample edu5, chi-square ($\chi 2$) = 184.974, df = 155, p = 0.050, CFI = 0.988, RMSEA = 0.030 (90% CI = 0.000 – 0.045), SRMR = 0.039. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Model fit was good in the sample edu6, chi-square ($\chi 2$) = 143.269, df = 155, p = 0.741, CFI = 1.000, RMSEA = 0.000 (90% CI = 0.000 – 0.031), SRMR = 0.050. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95.

The results of the invariance routine are shown in Table C6.1. The test of configural invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 739.869, df = 620, p = 0.001, CFI = 0.982, RMSEA = 0.034 (90% CI = 0.023 – 0.043), SRMR = 0.047. Although the chi-square ($\chi 2$) was statistically significant at p value 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Thus, the measurement model was configural invariant across groups of education. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 792.986, df = 662, p < 0.001, CFI = 0.981, RMSEA = 0.035 (90% CI = 0.024 – 0.043), SRMR = 0.054. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining the factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the difference test was not significant, chi-square ($\chi 2$) diff = 53.117, df = 42, p value = 0.1168 and CFI was overlapping (Delta CFI < 0.01). Thus, the measurement model was metric invariant across groups of education. The test of scalar invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 830.900, df = 704, p = 0.001, CFI = 0.981, RMSEA = 0.033 (90% CI = 0.023 – 0.046), SRMR = 0.055. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. There was no difference between models constraining the factor

loadings (metric invariant) and intercepts (scalar invariant); the difference test was non-significant, chi-square ($\chi 2$) diff = 37.914, df = 42, p value = 0.6509, and CFI was overlapping (Delta CFI < 0.01). Thus, the measurement model was scalar invariant across groups of education.

Table C6.1

Factorial Invariance Across Groups of Different Levels of Education

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
Edu1 (n=124)	162.651 p=0.321	155	0.992	0.020 [0.000-0.047]	0.053
Edu3 (n=192)	248.975 (p<0.000)	155	0.954	0.056 [0.043-0.069]	0.051
Edu5 (n=217)	184.974 p=0.050	155	0.988	0.030 [0.000-0.045]	0.039
Edu6 (n=128)	143.269 p=0.741	155	1.000	0.000 [0.000-0.031]	0.050
Configural invariant	739.869 p=0.001	620	0.982	0.034 [0.023-0.043]	0.047
Metric invariant	792.986 p<0.001	662	0.981	0.035 [0.024-0.043]	0.054
Scalar invariant	830.900 p=0.001	704	0.981	0.033 [0.023-0.046]	0.055

Note. N=661. Edu1: High school graduate, no college, and less than high school diploma, Edu3: Some college, no degree, and associate degree, Edu5: Bachelor's degree, Edu6: Advance degree. df: degrees of freedom. chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	53.117	42	0.1168	0.001
Metric invariant vs Scalar invariant	37.914	42	0.6509	0.000

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C6.2

Items Loads and Fit Indexes Across Groups Separated by Level of Education for the Invariant Modified Six-Factors Solution

		Edu1 (n=124)		Edu3 (n=192)		Edu5 (n=217)		Edu6 (n=128)	
Factor	Indicator	Ustd	Std	Ustd	Std	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.743	1.00	0.75	1.00	0.81	1.00	0.70
	At02	0.896	0.739	0.90	0.77	0.90	0.73	0.90	0.71
	At03	0.994	0.754	0.99	0.77	0.99	0.82	0.99	0.76
	At04	0.930	0.729	0.93	0.72	0.93	0.79	0.93	0.72
ATC	At05	1.000	0.779	1.00	0.79	1.00	0.81	1.00	0.84
	At06	0.918	0.726	0.92	0.75	0.92	0.77	0.92	0.84
	At07	1.042	0.757	1.04	0.81	1.04	0.80	1.04	0.82
MSR	At09	1.000	0.733	1.00	0.71	1.00	0.78	1.00	0.81
	At11	0.743	0.607	0.74	0.62	0.74	0.65	0.74	0.64
	At12	0.881	0.695	0.88	0.65	0.88	0.69	0.88	0.70
DN	Sn13	1.000	0.696	1.00	0.76	1.00	0.80	1.00	0.73
	Sn14	1.111	0.741	1.11	0.86	1.11	0.87	1.11	0.84
	Sn15	1.025	0.741	1.03	0.82	1.03	0.82	1.03	0.85
Inj	Sn16	1.000	0.842	1.00	0.84	1.00	0.86	1.00	0.83
	Sn17	0.940	0.729	0.94	0.70	0.94	0.85	0.94	0.79
	Sn18	0.992	0.838	0.99	0.81	0.99	0.89	0.99	0.77
IN	In22	1.000	0.721	1.00	0.85	1.00	0.86	1.00	0.72
	In23	0.859	0.687	0.86	0.77	0.86	0.70	0.86	0.68
	In24	0.950	0.609	0.95	0.86	0.95	0.70	0.95	0.80
	In25	0.963	0.721	0.96	0.79	0.96	0.88	0.96	0.83

Note. Null model: chi-square ($\chi2$) = 7502.311, df = 760, p < 0.001. Scalar invariant model (N=661): chi-square ($\chi2$) = 830.900, df = 704, p = 0.001, CFI = 0.981, RMSEA = 0.033 (90% CI = 0.023 – 0.042), SRMR = 0.055.

Ed1: High school graduate, no college, and less than high school diploma, Ed3: Some college, no degree, and associate degree, Ed5: Bachelor's degree, Ed6: Advance degree

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). .chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C7 Factorial Invariance Across Groups with Different Work Experience

Factorial invariance of the modified six-factor solution was examined between two groups divided by work experience with baseline data from two work experience groups (661 valid responses). The results are provided in Table C7.1, and Table C7.2 provides item loads and fit indexes for the invariant solution. The groups were combined with acceptable sample sizes. The groups were exp1 (less than ten years of work experience, n=184) and exp4 (more than ten years of work experience, n=477). Model fit was good in the sample exp1, chi-square ($\chi 2$) = 174.351, df = 155, p = 0.137, CFI = 0.986, RMSEA = 0.026 (90% CI = 0.000 – 0.044), SRMR = 0.049. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Model fit was good in the sample exp4, chi-square ($\chi 2$) = 197.304, df = 155, p = 0.012, CFI = 0.992, RMSEA = 0.024 (90% CI = 0.012 – 0.033), SRMR = 0.032. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95.

The results of the invariance routine are shown in Table C7.1. The test of configural invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 371.655, df = 310, p = 0.009, CFI = 0.991, RMSEA = 0.025 (90% CI = 0.013 – 0.033), SRMR = 0.037. Although the chi-square ($\chi 2$) was statistically significant at p value 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Thus, the measurement model was configural invariant across groups of work experience. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 388.529, df = 324, p = 0.008, CFI = 0.990, RMSEA = 0.025 (90% CI = 0.013 – 0.033), SRMR = 0.040. Although the chi-square ($\chi 2$) was statistically significant at p value < 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining the factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the difference test was not significant, chi-square ($\chi 2$) diff = 16.874, df = 14, p value = 0.263 and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was metric invariant across groups of work experience. The test of scalar invariance, resulted in a good fit, chi-square ($\chi 2$) = 407.756, df = 338, p = 0.005, CFI = 0.989, RMSEA = 0.025 (90% CI = 0.014 – 0.033), SRMR = 0.041. Although the chi-square ($\chi 2$) was statistically significant at p value < 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. There was no difference between models constraining the factor loadings (metric invariant) and intercepts (scalar invariant); the difference test was non-significant, chi-square ($\chi 2$) = 19.227, df = 14, p value = 0.1564 and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was scalar invariant across groups of work experience.

Table C7.1

Factorial Invariance Across Groups with Different Work Experience

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Exp1 (n=184)	174.351 p=0.137	155	0.986	0.026 [0.000-0.044]	0.049
Exp4 (n=477)	197.304 p=0.012	155	0.992	0.024 [0.012-0.033]	0.032
Configural invariant	371.655 p=0.009	310	0.991	0.025 [0.013-0.033]	0.037
Metric invariant	388.529 p=0.008	324	0.990	0.025 [0.013-0.033]	0.040
Scalar invariant	407.756 p=0.005	338	0.989	0.025 [0.014-0.033]	0.041

Note. N=661. Exp1: Less than ten years. Exp4 more than ten years. df: degrees of freedom. chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	16.874	14	0.263	0.001
Metric invariant vs. Scalar invariant	19.227	14	0.1564	0.001

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C7.2

Items Loads and Fit Indexes Across Groups Separated by Work Experience for the Invariant Modified Six-Factors Solution

		Exp1 (Less than 10 years) (n=184)		Exp4 (More than 10 years) (n=477)	
Factor	Indicator	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.689	1.000	0.786
	At02	0.889	0.647	0.889	0.771
	At03	1.005	0.760	1.005	0.795
	At04	0.934	0.694	0.934	0.771
ATC	At05	1.000	0.701	1.000	0.831
	At06	0.928	0.711	0.928	0.786
	At07	1.055	0.718	1.055	0.825
MSR	At09	1.000	0.764	1.000	0.740
	At11	0.727	0.621	0.727	0.594
	At12	0.877	0.684	0.877	0.652
DN	Sn13	1.000	0.675	1.000	0.776
	Sn14	1.106	0.717	1.106	0.866
	Sn15	1.032	0.701	1.032	0.844
Inj	Sn16	1.000	0.840	1.000	0.844
	Sn17	0.912	0.762	0.912	0.756
	Sn18	0.968	0.799	0.968	0.832
IN	In22	1.000	0.780	1.000	0.801
	In23	0.870	0.630	0.870	0.757
	In24	0.927	0.742	0.927	0.710
	In25	0.983	0.781	0.983	0.830

Note. Null model: chi-square ($\chi2$) = 6877.103, df = 380, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi2$) = 407.756, df = 338, p = 0.005, CFI = 0.989, RMSEA = 0.025 (90% CI = 0.014 – 0.033), SRMR = 0.041.

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C8 Factorial Invariance Across Job Level

Factorial invariance of the modified six-factor solution was examined between two groups divided by job level with baseline data from two groups of job level (661 valid responses). The results are provided in Table C8.1, and Table C8.2 provides item loads and fit indexes for the invariant solution. The job groups were combined with acceptable sample sizes. The groups were L1 (entry and mid-level, n=530) and L3 (executive level, n=131). Model fit was acceptable for the sample L1, chi-square ($\chi 2$) = 215.788, df = 155, p = 0.001, CFI = 0.988, RMSEA = 0.027 (90% CI = 0.018 – 0.036), SRMR = 0.033. Although the chi-square ($\chi 2$) was statistically significant at a p-value < 0.01, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Model fit was good for the sample L3, chi-square ($\chi 2$) = 195.661, df = 155, p = 0.015, CFI = 0.972, RMSEA = 0.045 (90% CI = 0.021 – 0.063), SRMR = 0.051. Although the chi-square ($\chi 2$) was statistically significant at p-value < 0.05, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI was very close to the limit 0.95.

The results of the invariance routine are shown in Table C8.1. The test of configural invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 411.448, df = 310, p < 0.001, CFI = 0.985, RMSEA = 0.031 (90% CI = 0.023 – 0.039), SRMR = 0.036. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Thus, the measurement model was configural invariant across groups of job level. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 430.121, df = 324, p < 0.001, CFI = 0.984, RMSEA = 0.031 (90% CI = 0.023 – 0.039), SRMR = 0.038. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining the factor structure (configural invariant) and factor loadings (metric invariant) were invariant; the chi-square ($\chi 2$) difference test was not significant, chi-square ($\chi 2$) = 18.672, df = 14, p value = 0.1779 and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was metric invariant across groups of job level. The test of scalar invariance, resulted in a good fit, chi-square ($\chi 2$) = 450.803, df = 338, p < 0.001, CFI = 0.983, RMSEA = 0.032 (90% CI = 0.023 – 0.039), SRMR = 0.039. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. Models constraining the factor loadings (metric invariant) and factor intersections (scaler invariant) were invariant; the difference test was not significant, chi-square ($\chi 2$) = 20.682, df = 14, p value = 0.1101 and CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was scalar invariant across groups of job level.

Table C8.1

Factorial Invariance Across Groups with Different Job Level

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
L1 (n=530)	215.788 p=0.001	155	0.988	0.027 [0.018-0.036]	0.033
L3 (n=131)	195.661 p=0.015	155	0.972	0.045 [0.021-0.063]	0.051
Configural invariant	411.448 p<0.001	310	0.985	0.031 [0.023-0.039]	0.036
Metric invariant	430.121 p<0.001	324	0.984	0.031 [0.023-0.039]	0.038
Scalar invariant	450.803 p<0.001	338	0.983	0.032 [0.023-0.039]	0.039

Note. N=661. L1: Entry and mid-level, L3: Executive level. df: degrees of freedom. chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	18.672	14	0.1779	0.001
Metric invariant vs. Scalar invariant	20.682	14	0.1101	0.001

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).

Table C8.2

Items Loads and Fit Indexes Across Groups Separated by Job Level for the Invariant Modified Six-Factors Solution

		L1 (Entry and mid-levels) (n=530)		L3 (executive) (n=131)	
Factor	Indicator	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.755	1.000	0.754
	At02	0.902	0.740	0.902	0.705
	At03	1.013	0.776	1.013	0.822
	At04	0.954	0.759	0.954	0.732
ATC	At05	1.000	0.804	1.000	0.820
	At06	0.922	0.761	0.922	0.816
	At07	1.038	0.799	1.038	0.790
MSR	At09	1.000	0.735	1.000	0.858
	At11	0.744	0.594	0.744	0.773
	At12	0.852	0.622	0.852	0.793
DN	Sn13	1.000	0.761	1.000	0.746
	Sn14	1.098	0.831	1.098	0.827
	Sn15	1.028	0.797	1.028	0.884
Inj	Sn16	1.000	0.847	1.000	0.853
	Sn17	0.938	0.800	0.938	0.711
	Sn18	0.967	0.834	0.967	0.789
IN	In22	1.000	0.819	1.000	0.730
	In23	0.873	0.716	0.873	0.724
	In24	0.922	0.690	0.922	0.842
	In25	0.988	0.824	0.988	0.811

Note. Null model: chi-square ($\chi 2$) = 6995.771, df = 380, $p < 0.001$. Scalar invariant model (N=661): chi-square ($\chi 2$) = 450.803, df = 338, $p < 0.001$, CFI = 0.983, RMSEA = 0.032 (90% CI = 0.023 – 0.039), SRMR = 0.039.

ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

C9 Factorial Invariance Across Organization Size

Factorial invariance of the modified six-factor solution was examined across groups divided by organization size with baseline data from three groups of organization size (661 valid responses). The results are provided in Table C9.1, and Table C9.2 provides item loads and fit indexes for the invariant solution. The groups were combined with acceptable sample sizes. The groups were size1 (between 2 and 100 members, n=202), size4 (between 101 and 500 members, n=138), and size5 (more than 500 members, n=321). Model fit was good in sample size1, chi-square ($\chi 2$) = 197.602, df = 155, p = 0.012, CFI = 0.978, RMSEA = 0.037 (90% CI = 0.018 – 0.051), SRMR = 0.044. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Model fit was minimally acceptable for sample size4, chi-square ($\chi 2$) = 239.278, df = 155, p < 0.001, CFI = 0.947, RMSEA = 0.063 (90% CI = 0.047 – 0.078), SRMR = 0.056. The chi-square ($\chi 2$) was statistically significant, the RMSEA slightly above the limit of 0.06, the SRMR was below 0.08, and the CFI was slightly lower than 0.95. The poor fit for sample size4 is likely due to the small sample size relative to the other two groups. The model was retained because the six-factor solution fits well for the other two groups, although invariance inspection revealed partial invariance, reported in the next paragraph. Model fit was good for sample size5, chi-square ($\chi 2$) = 178.600, df = 155, p = 0.094, CFI = 0.993, RMSEA = 0.022 (90% CI = 0.000 – 0.035), SRMR = 0.037. The chi-square ($\chi 2$) was not statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95.

The results of the invariance routine are shown in Table C9.1. The test of configural invariance, resulted in an acceptable fit, chi-square ($\chi 2$) = 615.480, df = 465, p < 0.001, CFI = 0.977, RMSEA = 0.038 (90% CI = 0.030 – 0.046), SRMR = 0.043. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Thus, the measurement model was configural invariant across groups of organization size. The test of metric invariance resulted in an acceptable fit, chi-square ($\chi 2$) = 664.729, df = 493, p < 0.001, CFI = 0.974, RMSEA = 0.040 (90% CI = 0.032 – 0.049), SRMR = 0.050. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Models constraining the factor structure (configural invariant) and factor loadings (metric invariant) were not invariant; the difference test was significant, chi-square ($\chi 2$) diff = 49.25, df = 28, p-value < 0.001, although the CFI was overlapping (Delta CFI less than 0.01). Twenty different models were examined to investigate the cause of invariance, freeing only one loading parameter corresponding to each indicator in the six-factor modified solution. It was found that freeing the loading parameter of At02 has the biggest impact on the fit indexes. However, the configural and metric invariant models freeing At02 load were still not invariant. The next contributor of invariance was found to be the Sn17 load. The

modified metric invariant freeing the At02 and Sn17 had good model fit, chi-square ($\chi 2$) = 643.673, df = 489, $p < 0.001$, CFI = 0.977, RMSEA = 0.038 (90% CI = 0.029 – 0.046), SRMR = 0.048. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Models constraining the factor structure (configural invariant) and loadings (scalar invariant) freeing the At02 and Sn17 loads were invariant; the difference test was not significant, chi-square ($\chi 2$) diff = 28.194, df = 24, p-value = 0.252, and the CFI was overlapping (Delta CFI less than 0.01). Thus, the measurement model was partially metric invariant across organization size freeing At02 and Sn17 loads. The test of scalar invariance, resulted in a good fit, chi-square ($\chi 2$) = 684.805, df = 517, $p < 0.001$, CFI = 0.975, RMSEA = 0.038 (90% CI = 0.030 – 0.049), SRMR = 0.050. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Models constraining the factor loadings (metric invariant) except for At02 and Sn17 loadings and intercepts (scalar invariant) were not invariant; the difference test was significant, chi-square ($\chi 2$) diff = 48.858, df = 26, p-value = 0.00841, although the CFI was overlapping (Delta CFI less than 0.01). Twenty different models freeing only one intersection parameter corresponding to each indicator were examined to investigate the cause of this invariance. It was found that freeing the intersection parameter of At02 has the biggest impact on the fit indexes. The modified scalar invariant model freeing the intersection coefficient At02 had good model fit, chi-square ($\chi 2$) = 670.531, df = 515, $p < 0.001$, CFI = 0.977, RMSEA = 0.037 (90% CI = 0.029 – 0.045), SRMR = 0.049. Although the chi-square ($\chi 2$) was statistically significant, the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. Models constraining the loadings (metric invariant) except At02 and Sn17 and intersections (scalar invariant) except At02 intersection were invariant; the difference test was not significant, chi-square ($\chi 2$) diff = 26.858, df = 26, p-value = 0.4168, and the CFI was overlapping (Delta CFI less than 0.01).Thus, the measurement model was scalar invariant across groups of job levels, allowing to freely estimate the load and intersection of At02 and the load of Sn17.

Table C9.1

Factorial Invariance Across Groups From Organizations With Different Size

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Size1 (n=202)	197.602 p=0.012	155	0.978	0.037 [0.018-0.051]	0.044
Size4 (n=138)	239.278 p<0.001	155	0.947	0.063 [0.047-0.078]	0.056
Size5 (n=321)	178.600 p=0.094	155	0.993	0.022 [0.000-0.035]	0.037
Configural invariant	615.480 p<0.001	465	0.977	0.038 [0.030-0.046]	0.043
Metric invariant	664.729 p<0.001	493	0.974	0.040 [0.032-0.049]	0.050
Metric invariant freeing loads ATI=~At02 and Inj=~Sn17	643.673 p<0.001	489	0.977	0.038 [0.029-0.046]	0.048
Scalar invariant freeing loads ATI=~At02 and Inj=~Sn17	684.805 p<0.001	517	0.975	0.038 [0.030-0.046]	0.050
Scalar Invariant freeing loads ATI=~At02 and Inj=~Sn17 and intersection At02~1	670.531 p<0.001	515	0.977	0.037 [0.029-0.045]	0.049

Note. N=661. Size1: Between 2 and 100, Size4: Between 101 and 500, Size 5: More than 500. df: degrees of freedom. chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Configural invariant vs. Metric invariant	49.25	28	0.007833	0.003
Configural invariant vs. Metric invariant freeing ATI=~At02 and Inj =~Sn17	28.194	24	0.252	0.000
Metric invariant freeing ATI=~At02 and Inj =~Sn17 vs. Scalar invariance	48.858	26	0.00841	0.002
Metric invariant freeing ATI=~At02 and Inj =~Sn17 vs Scalar invariant freeing At02~1	26.858	26	0.4168	0.000

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
ATI: Attitudes toward the importance of security recommendations. Inj Injunctive norms. At02, Sn17 are indicators. =~ indicator-factor load, ~1 indicator intersection

Table C9.2

Items Loads and Fit Indexes Across Groups Separated by Organization Size for the Invariant Modified Six-Factors Solution

		Size1 (2-100 members) (n=202)		Size4 (101-500 members) (n=138)		Size5 (more than 500) (n=321)	
Factor	Indicator	Ustd	Std	Ustd	Std	Ustd	Std
ATI	At01	1.000	0.725	1.000	0.713	1.000	0.791
	(At02*)	1.049	0.736	1.034	0.758	0.777	0.744
	At03	1.012	0.765	1.012	0.745	1.012	0.815
	At04	0.955	0.724	0.955	0.731	0.955	0.783
ATC	At05	1.000	0.799	1.000	0.837	1.000	0.801
	At06	0.916	0.750	0.916	0.792	0.916	0.772
	At07	1.040	0.763	1.040	0.856	1.040	0.797
MSR	At09	1.000	0.794	1.000	0.867	1.000	0.719
	At11	0.702	0.646	0.702	0.663	0.702	0.560
	At12	0.863	0.718	0.863	0.814	0.863	0.595
DN	Sn13	1.000	0.731	1.000	0.705	1.000	0.799
	Sn14	1.097	0.810	1.097	0.835	1.097	0.835
	Sn15	1.022	0.786	1.022	0.841	1.022	0.809
Inj	Sn16	1.000	0.904	1.000	0.846	1.000	0.819
	Sn17*	0.807	0.703	1.084	0.912	0.871	0.710
	Sn18	0.969	0.850	0.969	0.835	0.969	0.803
IN	In22	1.000	0.691	1.000	0.849	1.000	0.845
	In23	0.875	0.677	0.875	0.675	0.875	0.757
	In24	0.919	0.733	0.919	0.788	0.919	0.685
	In25	0.993	0.829	0.993	0.802	0.993	0.832

Note. Null model: chi-square ($\chi 2$) = 7255.767, df = 570, p < 0.001. Scalar invariant model (N=661): chi-square ($\chi 2$) = 670.531, df = 515, p < 0.001, CFI = 0.977, RMSEA = 0.037 (90% CI = 0.029 – 0.045), SRMR = 0.059.
ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR. Ustd: Unstandardized load. Std: Standardized load (cutoff > 0.6). . chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).
*At02 and Sn17 Load parameters freely estimated across groups
(At02) Intersection parameter freely estimated across groups

D. STRUCTURAL INVARIANCE ANALYSES ACROSS SAMPLES

(From Chapter 3 / 3.4.10 Structural Invariance Analyses)

D1 Structural Invariance Analysis Across Scenarios

The results of the structural invariance test routine are shown in Table D1.1. The scalar invariant model freeing all regression coefficient to be estimated (unconstrained model) with baseline data from scenarios 1 – 4 (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 847.627, df = 707, $p < 0.001$, CFI = 0.979, RMSEA = 0.035 (90% CI = 0.025 – 0.043), SRMR = 0.059. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficients to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 864.284, df = 719, $p < 0.001$, CFI = 0.979, RMSEA = 0.035 (90% CI = 0.025 – 0.043), SRMR = 0.059. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the constrained model were not different, the difference test was not significant, chi-square ($\chi 2$) diff = 16.657, df = 15, p-value = 0.3398 and the CFI was overlapping (Delta CFI < 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the following regression coefficients does not produce a difference in terms of fit indexes, ATI->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 2.0581, df = 3, p value = 0.5604 and the CFI was overlapping (Delta CFI less than 0.01)), ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 2.6223, df = 3, p value = 0.4536 and the CFI was overlapping (Delta CFI less than 0.01)), DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 2.2187, df = 3, p value = 0.5283 and the CFI was overlapping (Delta CFI less than 0.01)), and Inj->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.6012, df = 3, p value = 0.6591 and the CFI was overlapping (Delta CFI less than 0.01)). Thus, ATI->IN, ATC->IN, DN->IN, and Inj->IN regression coefficients were not significantly different across scenarios. In contrast, comparing the unconstrained model with the model constraining the regression coefficient MSR-> IN significantly changed the fit index chi-square ($\chi 2$) diff = 6.5498, df = 3, p value = 0.08772, although the CFI was overlapping (Delta CFI less than 0.01). Thus,, MSR->IN parameter was significantly different across scenarios. The model constraining all regression coefficients except the MSR->IN (structural invariant) resulted in a good model fit, chi-square ($\chi 2$) = 857.109, df = 716, $p<0.001$, CFI = 0.979, RMSEA 0.035 (90% CI [0.025 – 0.043]), SRMR = 0.057. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and structural invariant model were invariant, chi-square ($\chi 2$) diff = 9.4825, df = 12, p value = 0.6613, although the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining the regression coefficient except MSR->IN was invariant across scenarios. The regression coefficients across groups are shown in Table D1.2.

Table D1.1

Structural Invariance Results Across Scenarios

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	847.627 (p<0.001)	707	0.979	0.035 [0.025-0.043]	0.059
Constrained model	864.284 (p<0.001)	719	0.979	0.035 [0.025-0.043]	0.059
Partially constrained model constraining ATI->IN	849.685 (p<0.001)	707	0.979	0.035 [0.025-0.043]	0.056
Partially constrained model constraining ATC->IN	850.249 (p<0.001)	707	0.979	0.035 [0.025-0.043]	0.056
Partially constrained model constraining MSR->IN	854.176 (p<0.001)	707	0.978	0.035 [0.025-0.044]	0.057
Partially constrained model constraining DN->IN	849.845 (p<0.001)	707	0.979	0.035 [0.025-0.043]	0.056
Partially constrained model constraining Inj->IN	849.228 (p<0.001)	707	0.979	0.035 [0.025-0.043]	0.056
Structural invariant Constrained model freeing MSR->IN	857.109 (p<0.001)	716	0.979	0.035 [0.025-0.043]	0.057

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Unconstrained model vs. Constrained model	16.657	15	0.3398	0.000
Unconstrained model vs. Partially constrained model constraining ATI->IN	2.0581	3	0.5604	0.000
Unconstrained model vs. Partially constrained model constraining ATC->IN	2.6223	3	0.4536	0.000
Unconstrained model vs. Partially constrained model constraining MSR->IN	6.5498	3	0.08772	0.001
Unconstrained model vs. Partially constrained model constraining DN->IN	2.2187	3	0.5283	0.000
Unconstrained model vs. Partially constrained model constraining Inj->IN	1.6012	3	0.6591	0.000
Unconstrained model vs. structural invariant	9.4825	12	0.6613	0.000

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D1.2

Regression Coefficients Across Scenarios From The Structural Invariant Model (H7)

	Sc1				Sc2				Sc3				Sc4			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI >IN	0.748	0.870	0.127	0.000	0.706	0.870	0.127	0.000	0.724	0.870	0.127	0.000	0.763	0.870	0.127	0.000
ATC>IN	-0.449	-0.369	0.107	0.001	-0.356	-0.369	0.107	0.001	-0.330	-0.369	0.107	0.001	-0.390	-0.369	0.107	0.001
*MSR ->IN	-0.052	-0.038	0.058	0.512	0.091	0.062	0.055	0.262	0.095	0.076	0.063	0.228	0.229	0.176	0.058	0.003
DN->IN	0.080	0.080	0.076	0.293	0.071	0.080	0.076	0.293	0.067	0.080	0.076	0.293	0.079	0.080	0.076	0.293
Inj->IN	0.431	0.323	0.035	0.000	0.418	0.323	0.035	0.000	0.413	0.323	0.035	0.000	0.407	0.323	0.035	0.000

Note. Structural invariant model: chi-square (χ2) (df=716, N=661)=857.109, p value < 0.001. Null: chi-square (χ2) (df=760, N=661)=7519.549. CFI = 0.979 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.035; 90%CI [0.025 – 0.043])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.057 (cutoff < 0.8) (Bentler & Wu, 2005). $\mathbf{R(sc1)^2 = 0.681}$, $\mathbf{R(sc2)^2 = 0.568}$, $\mathbf{R(sc3)^2 = 0.594}$, $\mathbf{R(sc4)^2 = 0.575}$.

Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups.

D2 Structural Invariance for yes/no Answers to Ad01 (H8)

The results of the invariance test routine are shown in Table D2.1. The scalar invariant model was examined, freeing all regression coefficients estimated (unconstrained model) with baseline data from respondents to the Ad01question (661 valid responses). Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 445.743, df = 338, p < 0.001, CFI = 0.983, RMSEA = 0.031 (90% CI = 0.023 – 0.039), SRMR = 0.041. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The constrained model fixing all regression coefficients equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 458.832, df = 343, p < 0.001, CFI = 0.982, RMSEA = 0.032 (90% CI = 0.024 – 0.039), SRMR = 0.045. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The unconstrained model and the constrained model were different, the difference test was significant, chi-square ($\chi 2$) diff = 13.089, df = 5, p-value = 0.02256 although the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models was examined, each constraining one regression coefficient only (partially constrained models). It was found that constraining the regression coefficients individually for ATI->IN and Inj->IN produced a difference in terms of fit indexes (the difference test was significant, p-value <0.05) and for the other three ATC->IN and MSR->IN the difference is significative at p<0.1. This is evidence that the mentioned regression coefficients are different across groups. The partially constrained model constraining only DN->IN had a good model fit, chi-square ($\chi 2$) = 448.569, df = 339, p < 0.001, CFI = 0.983, RMSEA = 0.031 (90% CI = 0.023 – 0.039), SRMR = 0.042. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The unconstrained model and the partially constrained model constraining DN->IN to be equal across groups were invariant (p<0.05), the difference test was not significant, chi-square ($\chi 2$) diff =2.8257, df = 4, p-value = 0.09277 and the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining DN->IN to be equal across groups was invariant for respondents to Ad02 questions. The regression coefficients across groups are shown in Table D2.2.

Table D2.1

Structural Invariance Results Between Respondents to Ad01 (H8)

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	445.743 (p<0.001)	338	0.983	0.031 [0.023-0.039]	0.041
Constrained model	458.832 (p<0.001)	343	0.982	0.032 [0.024-0.039]	0.045
Partially constrained model constraining ATI->IN	450.027 (p<0.001)	339	0.983	0.031 [0.023-0.039]	0.042
Partially constrained model constraining ATC->IN	448.839 (p<0.001)	339	0.983	0.031 [0.023-0.039]	0.041
Partially constrained model constraining MSR->IN	448.663 (p<0.001)	339	0.983	0.031 [0.023-0.039]	0.042
Partially constrained model constraining DN->IN (Structural invariant)	448.569 (p<0.001)	339	0.983	0.031 [0.023-0.039]	0.042
Partially constrained model constraining Inj->IN	450.067 (p<0.001)	339	0.983	0.031 [0.023-0.039]	0.042

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Unconstrained model vs. Constrained model	13.089	5	0.02256	0.001
Unconstrained model vs. Partially constrained model constraining ATI->IN	4.2837	1	0.03848	0.000
Unconstrained model vs. Partially constrained model constraining ATC->IN	3.0966	1	0.07846	0.000
Unconstrained model vs. Partially constrained model constraining MSR->IN	2.9197	1	0.08751	0.000
Unconstrained model vs. Partially constrained model constraining DN->IN (Structural invariant)	2.8257	1	0.09277	0.000
Unconstrained model vs. Partially constrained model constraining Inj->IN	4.3243	1	0.03757	0.000

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D2.2

Regression Coefficients Per Yes/No Respondents to Ad01 for the Structural Invariant Model (H8)

	Yes				No			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
*ATI ->IN	0.797	1.054	0.180	0.000	0.404	0.401	0.221	0.069
*ATC->IN	-0.410	-0.425	0.149	0.004	-0.176	-0.160	0.172	0.352
*MSR ->IN	0.148	0.108	0.041	0.009	-0.039	-0.038	0.076	0.620
DN ->IN	0.076	0.084	0.081	0.300	0.080	0.084	0.081	0.300
*Inj ->IN	0.406	0.297	0.039	0.000	0.536	0.479	0.090	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=339, N=661)=448.569, p value < 0.001. Null: chi-square ($\chi 2$) (df=380, N=661)=6797.444. CFI = 0.983 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.031; 90%CI [0.023 – 0.039])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.042 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Indicate parameter significantly different across groups

$\mathbf{R(yes)^2 = 0.606.R(no)^2 = 0.630}$.

D3 Structural Invariance for yes/no Answers to Ad02 (H9)

The results of the invariance test routine are shown in Table D3.1. The scalar invariant model freeing all regression coefficients to be estimated (unconstrained model) with baseline data from respondents to the Ad03 question (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 419.855, df = 338, p = 0.002, CFI = 0.987, RMSEA = 0.027 (90% CI = 0.017 – 0.035), SRMR = 0.041. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The constrained model fixing all regression coefficients equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 441.069, df = 343, p < 0.001, CFI = 0.984, RMSEA = 0.029 (90% CI = 0.021 – 0.037), SRMR = 0.044. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The unconstrained model and the constrained model were different, the difference test was significant, chi-square ($\chi 2$) diff = 21.214, df = 5, p-value <0.001 although the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained and five different models was examined, each one constraining one regression coefficient only (partially constrained models). It was found that constraining the regression coefficients individually for Inj->IN across groups significantly changed the model fit indexes (the difference test was significant, chi-square ($\chi 2$) diff = 12.493, df = 1, p-value <0.001, although the CFI was overlapping (Delta CFI less than 0.01)). The unconstrained model and the constrained model freeing Inj->IN was different (the difference test was significant, chi-square ($\chi 2$) diff = 11.9074, df = 4, p-value =0.01806 although the CFI was overlapping (Delta CFI less than 0.01)). It was found that freeing ATC->IN additional to Inj->IN. The constrained model freeing Inj->IN and ATC->IN had good model fit, chi-square ($\chi 2$) = 420.949, df = 341, p = 0.002, CFI = 0.987, RMSEA = 0.027 (90% CI = 0.017 – 0.035), SRMR = 0.041. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08, and the CFI exceeded 0.95. The unconstrained model and the constrained model freeing Inj-IN and ATC->IN to be equal across groups were invariant, the difference test was not significant, chi-square ($\chi 2$) diff =1.0939, df = 3, p-value = 0.7785 and the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining ATI->IN, MSR->IN, and DN->IN to be equal across groups was invariant for respondents to Ad03 questions. The regression coefficients across groups are shown in Table D3.2.

Table D3.1

Structural Invariance Results Between Respondents to Ad02 (H9)

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	419.855 (p=0.002)	338	0.987	0.027 [0.017-0.035]	0.041
Constrained model	441.069 (p<0.001)	343	0.984	0.029 [0.021-0.037]	0.044
Partially constrained model constraining ATI->IN	420.217 (p=0.002)	339	0.987	0.027 [0.017-0.035]	0.041
Partially constrained model constraining ATC->IN	420.511 (p=0.002)	339	0.987	0.027 [0.017-0.035]	0.041
Partially constrained model constraining MSR->IN	420.066 (p=0.002)	339	0.987	0.027 [0.017-0.035]	0.041
Partially constrained model constraining DN->IN	420.309 (p=0.002)	339	0.987	0.027 [0.017-0.035]	0.041
Partially constrained model constraining Inj->IN	432.348 (p<0.001)	339	0.985	0.029 [0.020-0.037]	0.041
Constrained model freeing Inj->IN	431.762 (p=0.001)	342	0.986	0.028 [0.019-0.036]	0.044
Constrained model freeing Inj->IN, and ATC->IN (Structural invariant)	420.949 (p=0.002)	341	0.987	0.027 [0.017-0.035]	0.041

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Unconstrained model vs. Constrained model	21.214	5	<0.001	0.003
Unconstrained model vs. Partially constrained model constraining ATI->IN	0.36144	1	0.5477	0.000
Unconstrained model vs. Partially constrained model constraining ATC->IN	0.65526	1	0.4182	0.000
Unconstrained model vs. Partially constrained model constraining MSR->IN	0.2104	1	0.6465	0.000
Unconstrained model vs. Partially constrained model constraining DN->IN	0.45401	1	0.5004	0.000
Unconstrained model vs. Partially constrained model constraining Inj->IN	12.493	1	<0.001	0.002
Unconstrained model vs. constrained model freeing Inj->IN	11.907	4	0.01806	0.001
Unconstrained model vs. constrained model freeing Inj->IN and ATC->IN (Structural invariant)	1.0939	3	0.7785	0.000

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D3.2

Regression Coefficients Per Yes/No Respondents to Ad02 for the Structural Invariant Model (H9)

	Yes				No			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.746	0.868	0.135	0.000	0.749	0.868	0.135	0.000
*ATC->IN	-0.345	-0.321	0.118	0.006	-0.625	-0.623	0.153	0.000
MSR ->IN	0.073	0.049	0.033	0.144	0.049	0.049	0.033	0.144
DN ->IN	0.087	0.097	0.082	0.236	0.093	0.097	0.082	0.236
*Inj ->IN	0.356	0.244	0.038	0.000	0.659	0.610	0.081	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=341, N=661)=420.949, p value = 0.002. Null: chi-square ($\chi 2$) (df=380, N=661)=6702.113. CFI = 0.987 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.027; 90%CI [0.017 – 0.035])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.041 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Indicate parameter significantly different across groups

$\mathbf{R(yes)^2 = 0.579}.\mathbf{R(no)^2 = 0.680}$.

D4 Structural Invariance Across Age Groups

The results of the invariance test routine are shown in Table D4.1. The scalar invariant model freeing all regression coefficients to be estimated (unconstrained model) with baseline data four groups separated by age (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 877.860, df = 704, $p < 0.001$, CFI = 0.974, RMSEA = 0.039 (90% CI = 0.030 – 0.047), SRMR = 0.057. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficient to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 900.463, df = 719, $p < 0.001$, CFI = 0.973, RMSEA = 0.039 (90% CI = 0.030 – 0.047), SRMR = 0.061. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the constrained model were different, the difference test was significant ($p<0.1$), chi-square ($\chi 2$) diff = 22.603, df = 15, p-value = 0.09029 and the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the following regression coefficients does not produce a difference in terms of fit indexes, ATI->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.095174, df = 3, p value = 0.9924 and the CFI was overlapping (Delta CFI less than 0.01)), ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.1007, df = 3, p value = 0.7769 and the CFI was overlapping (Delta CFI less than 0.01)), MSR->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.1829, df = 3, p value = 0.7571 and the CFI was overlapping (Delta CFI less than 0.01)), DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.080623, df = 3, p value = 0.9941 and the CFI was overlapping (Delta CFI less than 0.01)). Thus, ATI->IN, ATC->IN, MSR->IN and DN->IN regression coefficients are not significantly different across scenarios. In contrast, comparing the unconstrained model with the model constraining the regression coefficient Inj-> IN significantly changed the fit indexes chi-square ($\chi 2$) diff = 6.8892, df = 3, p value = 0.07522, although the CFI was overlapping (Delta CFI less than 0.01). Hence Inj->IN parameter is significantly different across groups. The model constraining all regression coefficients except the Inj->IN (structural invariant) resulted in a good model fit, chi-square ($\chi 2$) = 894.970, df = 716, $p<0.001$, CFI = 0.973, RMSEA 0.039 (90% CI [0.030 – 0.047]), SRMR = 0.060. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and structural invariant model were invariant, chi-square ($\chi 2$) diff = 17.11, df = 12, p value = 0.1455, although the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining the regression coefficient except Inj->IN is invariant across scenarios. The regression coefficients across groups are shown in Table D4.2.

Table D4.1

Structural Invariance Results Across Age Groups

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	877.860 (p<0.001)	704	0.974	0.039 [0.030-0.047]	0.057
Constrained model	900.463 (p<0.001)	719	0.973	0.039 [0.030-0.047]	0.061
Partially constrained model constraining ATI->IN	877.955 (p<0.001)	707	0.975	0.038 [0.029-0.046]	0.057
Partially constrained model Constraining ATC->IN	878.960 (p<0.001)	707	0.975	0.038 [0.029-0.046]	0.057
Partially constrained model Constraining MSR->IN	879.043 (p<0.001)	707	0.975	0.038 [0.029-0.046]	0.057
Partially constrained model Constraining DN->IN	877.940 (p<0.001)	707	0.975	0.038 [0.029-0.046]	0.057
Partially constrained model Constraining Inj->IN	884.749 (p<0.001)	707	0.974	0.039 [0.030-0.047]	0.058
Structural invariant Constrained model freeing Inj->IN	894.970 (p<0.001)	716	0.973	0.039 [0.030-0.047]	0.060

Note. N=661. df: degrees of freedom. chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Unconstrained model vs. constraining model	22.603	15	0.090293	0.001
Unconstrained model vs. Partially constrained model Constraining ATI->IN	0.095174	3	0.9924	0.001
Unconstrained model vs. Constraining ATC->IN	1.1007	3	0.7769	0.001
Unconstrained model vs. Constraining MSR->IN	1.1829	3	0.7571	0.001
Unconstrained model vs. Constraining DN->IN	0.080623	3	0.9941	0.001
Unconstrained model vs. Constraining Inj->IN	6.8892	3	**0.07552**	0.000
Unconstrained model vs. structural invariant	17.11	12	0.1455	0.001

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D4.2

Regression Coefficients Per Age Group for the Structural Invariant Model

	Age1				Age3				Age4				Age5			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI->IN	0.835	0.979	0.138	0.000	0.776	0.979	0.138	0.000	0.841	0.979	0.138	0.000	0.887	0.979	0.138	0.000
ATC->IN	-0.415	-0.489	0.121	0.000	-0.519	-0.489	0.121	0.000	-0.501	-0.489	0.121	0.000	-0.574	-0.489	0.121	0.000
MSR->IN	0.134	0.104	0.035	0.003	0.150	0.104	0.035	0.003	0.119	0.104	0.035	0.003	0.121	0.104	0.035	0.003
DN->IN	0.094	0.121	0.076	0.111	0.111	0.121	0.076	0.111	0.117	0.121	0.076	0.111	0.128	0.121	0.076	0.111
Inj->IN*	0.300	0.214	0.059	0.000	0.517	0.378	0.059	0.000	0.463	0.386	0.071	0.000	0.365	0.317	0.062	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=716, N=661)=894.970, p value < 0.001. Null: chi-square ($\chi 2$) (df=760, N=661)=7511.854. CFI = 0.973 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.039; 90%CI [0.030 – 0.047])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.060 (cutoff < 0.8 (Bentler & Wu, 2005)) Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups

$\mathbf{R(age1)^2 = 0.527, R(age3)^2 = 0.597., R(age4)^2 = 0.768, R(age5)^2 = 0.647}$.

D5 Structural Invariance Across Gender

The results of the invariance test routine are shown in Table D5.1. The scalar invariant model freeing all regression coefficient to be estimated (unconstrained model) with baseline data from two groups of gender (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 409.996, df = 338, p = 0.004, CFI = 0.989, RMSEA = 0.025 (90% CI = 0.015 – 0.034), SRMR = 0.039. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficient to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 430.085, df = 343, p = 0.001, CFI = 0.987, RMSEA = 0.028 (90% CI = 0.018 – 0.036), SRMR = 0.043. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the constrained model were different, the difference test was significant, chi-square ($\chi 2$) diff = 20.089, df = 5, p-value = 0.001202 and the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the following regression coefficients does not produce a difference in terms of fit indexes, ATI->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.869, df = 1, p-value = 0.1716 and the CFI was overlapping (Delta CFI less than 0.01)), ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.86884, df = 1, p value = 0.3513 and the CFI was overlapping (Delta CFI less than 0.01)), MSR->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.1385, df = 1, p value = 0.286 and the CFI was overlapping (Delta CFI less than 0.01)), DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.24439, df = 1, p value = 0.6211 and the CFI was overlapping (Delta CFI less than 0.01)). Hence ATI->IN, ATC->IN, MSR->IN and DN->IN regression coefficients are not significantly different across scenarios. In contrast, comparing the unconstrained model with the model constraining the regression coefficient Inj-> IN significantly changed the fit indexes, chi-square ($\chi 2$) diff = 17.253, df = 1, p-value >0.001, although the CFI was overlapping (Delta CFI less than 0.01). Hence Inj->IN parameter is significantly different across groups. The model constraining all regression coefficients except the Inj->IN (structural invariant) resulted in a good model fit, chi-square ($\chi 2$) = 415.033, df = 342, p=0.004, CFI = 0.989, RMSEA 0.025 (90% CI [0.015 – 0.034]), SRMR = 0.040. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and structural invariant model were invariant, chi-square ($\chi 2$) diff = 5.0373, df = 4, p-value = 0.2835, although the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining the regression coefficient except Inj->IN is invariant across scenarios. The regression coefficients across groups are shown in Table D5.2.

Table D5.1

Structural Invariance Results Across Groups of Gender

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	409.996 (p=0.004)	338	0.989	0.025 [0.015-0.034]	0.039
Constrained model	430.085 (p=0.001)	343	0.987	0.028 [0.018-0.036]	0.043
Partially constrained model Constraining ATI->IN	411.865 (p=0.004)	339	0.989	0.026 [0.015-0.034]	0.039
Partially constrained model Constraining ATC->IN	410.864 (p=0.004)	339	0.989	0.025 [0.015-0.034]	0.039
Partially constrained model Constraining MSR->IN	411.134 (p=0.004)	339	0.989	0.025 [0.015-0.034]	0.039
Partially constrained model Constraining DN->IN	410.240 (p=0.005)	339	0.989	0.025 [0.015-0.034]	0.039
Partially constrained model Constraining Inj->IN	427.249 (p=0.001)	339	0.987	0.028 [0.019-0.036]	0.042
Structural invariant (Constrained model freeing Inj->IN)	415.033 (p=0.004)	342	0.989	0.025 [0.015-0.034]	0.040

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Unconstrained model vs. Constraining constrained	20.089	5	0.001202	0.002
Unconstrained model vs. Partially constrained model Constraining ATI->IN	1.869	1	0.1716	0.000
Unconstrained model vs. Partially constrained model Constraining ATC->IN	0.86884	1	0.3513	0.000
Unconstrained model vs. Partially constrained model Constraining MSR->IN	1.1385	1	0.286	0.000
Unconstrained model vs. Partially constrained model Constraining DN->IN	0.24439	1	0.6211	0.000
Unconstrained model vs. Partially constrained model Constraining Inj->IN	17.253	1	<0.001	0.002
Unconstrained model vs. Structural invariant (Constrained model freeing Inj->IN)	5.0373	4	0.2835	0.000

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D5.2

Regression Coefficients Per Gender for the Structural Invariant Model

	Female				Male			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.680	0.839	0.133	0.000	0.800	0.839	0.133	0.000
ATC->IN	-0.379	-0.383	0.118	0.001	-0.444	-0.383	0.118	0.001
MSR ->IN	0.069	0.059	0.032	0.069	0.097	0.059	0.032	0.069
DN ->IN	0.082	0.089	0.078	0.253	0.090	0.089	0.078	0.253
*Inj ->IN	0.505	0.434	0.046	0.000	0.330	0.211	0.043	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=339, N=661)=411.865, p value = 0.004. Null: chi-square ($\chi 2$) (df=380, N=661)=6975.193. CFI = 0.989 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.026; 90%CI [0.015 – 0.034])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.039 (cutoff < 0.8 (Bentler & Wu, 2005)) Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups

$\mathbf{R(female)^2 = 0.690. R(age3)^2 = 0.510}$.

D6 Structural Invariance Across Levels of Education

The results of the invariance test routine are shown in Table D6.1. The scalar invariant model freeing all regression coefficient to be estimated (unconstrained model) with baseline data from four groups of educations (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 830.900, df = 704, p = 0.001, CFI = 0.981, RMSEA = 0.033 (90% CI = 0.023 – 0.042), SRMR = 0.055. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficient to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 856.788, df = 719, p < 0.001, CFI = 0.980, RMSEA = 0.034 (90% CI = 0.024 – 0.043), SRMR = 0.060. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the constrained model were different, the difference test was significant, chi-square ($\chi 2$) diff = 25.888, df = 15, p-value = 0.03922 although the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the following regression coefficients does not produce a difference in terms of fit indexes: ATI->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.4217, df = 3, p value = 0.7004 and the CFI was overlapping (Delta CFI less than 0.01)), ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.5176, df = 3, p value = 0.0.6782 and the CFI was overlapping (Delta CFI less than 0.01)), MSR->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.4204, df = 3, p value = 0.7007 and the CFI was overlapping (Delta CFI less than 0.01)), DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 3.1169, df = 3, p value = 0.3739 and the CFI was overlapping (Delta CFI less than 0.01)), and Inj->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 3.4398, df = 3, p value = 0.0.3287 and the CFI was overlapping (Delta CFI less than 0.01)). To investigate the parameter that causes the difference in fit indexes between the constrained and unconstrained models, other five models were tested, where all regression coefficients were constrained to be equal except one of the five possible. It was found that the partial constrained model freeing the regression parameters ATC->IN and MSR->IN (structural invariant) have a good model fit, chi-square ($\chi 2$) = 838.824, df = 713, p=0.001, CFI = 0.981, RMSEA 0.033 (90% CI [0.022 – 0.041]), SRMR = 0.056. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the structural invariant model were invariant, chi-square ($\chi 2$) diff = 7.9241, df = 9, p value = 0.5418, although the CFI was overlapping (Delta CFI < 0.01). Thus, the model constraining the regression coefficient except MSR->IN and ATC->IN is invariant across scenarios. The regression coefficients across groups are shown in Table D6.2.

Table D6.1

Structural Invariance Results Across Groups of Education

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	830.900 (p=0.001)	704	0.981	0.033 [0.023-0.042]	0.055
Constrained model	856.788 (p<0.001)	719	0.980	0.034 [0.024-0.043]	0.060
Partially constrained model Constraining ATI->IN	832.322 (p=0.001)	707	0.981	0.033 [0.022-0.042]	0.055
Partially constrained model Constraining ATC->IN	832.418 (p=0.001)	707	0.981	0.033 [0.022-0.042]	0.055
Partially constrained model Constraining MSR->IN	832.320 (p=0.001)	707	0.981	0.033 [0.022-0.042]	0.055
Partially constrained model Constraining DN->IN	834.017 (p=0.001)	707	0.981	0.033 [0.022-0.042]	0.055
Partially constrained model Constraining Inj->IN	834.340 (p=0.001)	707	0.981	0.033 [0.022-0.042]	0.055
Structural invariant constrained model freeing ATC->IN and MSR->IN	838.824 (p=0.001)	713	0.981	0.033 [0.022-0.041]	0.056

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Unconstrained model vs. constrained model	25.888	15	0.03922	0.001
Unconstrained model vs. Partially constrained model Constraining ATI->IN	1.4217	3	0.7004	0.000
Unconstrained model vs. Partially constrained model Constraining ATC->IN	1.5176	3	0.6782	0.000
Unconstrained model vs. Partially constrained model Constraining MSR->IN	1.4204	3	0.7007	0.000
Unconstrained model vs. Partially constrained model Constraining DN->IN	3.1169	3	0.3739	0.000
Unconstrained model vs. Partially constrained model Constraining Inj->IN	3.4398	3	0.3287	0.000
Unconstrained model vs. constrained model freeing ATI->IN	18.988	12	0.08882	0.000
Unconstrained model vs. constrained model freeing ATC->IN	16.523	12	0.1684	0.000
Unconstrained model vs. constrained model freeing MSR->IN	15.104	12	0.2358	0.000

Table D6.1 (continue)

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Unconstrained model vs. constrained model freeing DN->IN	20.839	12	0.0579	0.000
Unconstrained model vs. constrained model freeing Inj->IN	20.35	12	0.06075	0.000
Unconstrained model vs. constrained model freeing ATC->IN and MSR->IN (Structural invariant)	7.9241	9	0.5418	0.000

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D6.2

Regression Coefficients Per Level of Education for the Structural Invariant Model

	Edu1				Edu3				Edu5				Edu6			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.821	0.924	0.146	0.000	0.764	0.924	0.146	0.000	0.815	0.924	0.146	0.000	0.725	0.924	0.146	0.000
*ATC->IN	-0.489	-0.506	0.165	0.002	-0.409	-0.404	0.141	0.004	-0.551	-0.541	0.145	0.000	-0.334	-0.286	0.124	0.021
*MSR->IN	0.241	0.200	0.086	0.020	-0.003	-0.002	0.061	0.972	0.081	0.061	0.050	0.228	0.325	0.233	0.071	0.001
DN->IN	0.077	0.092	0.081	0.260	0.087	0.092	0.081	0.260	0.090	0.092	0.081	0.260	0.082	0.092	0.081	0.260
Inj->IN	0.447	0.360	0.038	0.000	0.397	0.360	0.038	0.000	0.461	0.360	0.038	0.000	0.523	0.360	0.038	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=713, N=661)=838.824, p-value = 0.001. Null: chi-square ($\chi 2$) (df=760, N=661)=7502.311. CFI = 0.981 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.033; 90%CI [0.022 – 0.041])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.056 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups

$\mathbf{R(edu1)^2 = 0.698, R(edu3)^2 = 0.588, R(edu5)^2 = 0.620, R(edu6)^2 = 0.599}$.

D7 Structural Invariance Across Work Experience

The results of the invariance test routine are shown in Table D7.1. The scalar invariant model freeing all regression coefficients to be estimated (unconstrained model) with baseline data from two groups of work experience (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 407.756, df = 338, p = 0.005, CFI = 0.989, RMSEA = 0.025 (90% CI = 0.014 – 0.033), SRMR = 0.041. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficients to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 423.907, df = 343, p = 0.002, CFI = 0.988, RMSEA = 0.027 (90% CI = 0.017 – 0.035), SRMR = 0.043. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the constrained model were different, the difference test was significant, chi-square ($\chi 2$) diff = 16.151, df = 5, p-value = 0.006425 although the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the regression coefficients does not produce a difference in terms of fit indexes, ATI->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.011888, df = 1, p value = 0.9132 although the CFI was overlapping (Delta CFI less than 0.01)), ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.12174, df = 1, p value = 0.7272 although the CFI was overlapping (Delta CFI less than 0.01), MSR->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0, df = 1, p value = 0.998 although the CFI was overlapping (Delta CFI less than 0.01)), and DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 0.04915, df = 1, p value = 0.8245 although the CFI was overlapping (Delta CFI less than 0.01)). In contrast, model constraining Inj->IN to be equal across groups was different than the unconstrained model, the difference test was significant, chi-square ($\chi 2$) diff = 3.226, df = 1, p value = 0.07248 and the CFI was overlapping (Delta CFI less than 0.01). The constrained model freeing the one parameter that cause a difference in fit indexes (Inj->IN) resulted in a good model fit, chi-square ($\chi 2$) = 417.718, df = 342, p = 0.003, CFI = 0.988, RMSEA = 0.026 (90% CI = 0.016 – 0.034), SRMR = 0.044. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. However, the unconstrained model and the constrained model freeing Inj-> were different, chi-square ($\chi 2$) diff = 9.9618, df = 4, p-value = 0.04108 although the CFI was overlapping (Delta CFI less than 0.01). To investigate what parameter additional parameter, cause the difference in fit indexes between the constrained and unconstrained models, other four models were tested, where all regression coefficients were constrained to be equal except Inj->IN and one of the four possible parameters. It was found that the partial constrained model freeing the regression parameters Inj->IN and ATC->IN

(structural invariant) have a good model fit, chi-square ($\chi 2$) = 407.810, df = 341, p=0.007, CFI = 0.990, RMSEA 0.025 (90% CI [0.014 – 0.033]), SRMR = 0.041. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and the structural invariant model were invariant, chi-square ($\chi 2$) diff = 0.053993, df = 3, p-value = 0.9967, although the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining the regression coefficient except Inj->IN and ATC->IN is invariant across groups of work experience. The regression coefficients across groups are provided in Table D7.2.

Table D7.1

Structural Invariance Results Across Groups of Work Experience

Model	chi-square ($\chi 2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	407.756 (p=0.005)	338	0.989	0.025 [0.014-0.033]	0.041
Constrained model	423.907 (p=0.002)	343	0.988	0.027 [0.017-0.035]	0.043
Partially constrained model Constraining ATI->IN	407.768 (p=0.006)	339	0.989	0.025 [0.014-0.033]	0.041
Partially constrained model Constraining ATC->IN	407.878 (p=0.006)	339	0.989	0.025 [0.014-0.033]	0.041
Partially constrained model Constraining MSR->IN	407.756 (p=0.006)	339	0.989	0.025 [0.014-0.033]	0.041
Partially constrained model Constraining DN->IN	407.805 (p=0.006)	339	0.989	0.025 [0.014-0.033]	0.041
Partially constrained model Constraining Inj->IN	410.982 (p=0.004)	339	0.989	0.025 [0.015-0.034]	0.041
constrained model freeing Inj->IN	417.718 (p=0.003)	342	0.988	0.026 [0.016-0.034]	0.044
constrained model freeing Inj->IN and ATI->IN	408.675 (p=0.007)	341	0.990	0.025 [0.014-0.033]	0.041
constrained model freeing Inj->IN and ATC->IN (Structural invariant)	407.810 (p=0.007)	341	0.990	0.025 [0.014-0.033]	0.041
constrained model freeing Inj->IN and MSR->IN	417.339 (p=0.003)	341	0.988	0.026 [0.016-0.034]	0.044
constrained model freeing Inj->IN and DN->IN	408.326 (p=0.007)	341	0.990	0.024 [0.014-0.033]	0.041

Note. N=661. df: degrees of freedom. . chi-square ($\chi 2$), cutoff $\chi 2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Table D7.1 (continue)

Model comparison	chi-square ($\chi 2$) diff	df	p-value	Delta CFI
Unconstrained model vs. constrained model	16.151	5	0.006425	0.001
Unconstrained model vs. Partially constrained model Constraining ATI->IN	0.011888	1	0.9132	0.000
Unconstrained model vs. Partially constrained model Constraining ATC->IN	0.12174	1	0.7272	0.000
Unconstrained model vs. Partially constrained model Constraining MSR->IN	0	1	0.998	0.000
Unconstrained model vs. Partially constrained model Constraining DN->IN	0.04915	1	0.8245	0.000
Unconstrained model vs. Partially constrained model Constraining Inj->IN	3.226	1	0.07248	0.000
Unconstrained model vs. constrained model freeing Inj->IN	9.9618	4	0.04108	0.001
Unconstrained model vs. constrained model freeing Inj->IN and ATI->IN	0.91929	3	0.8208	0.001
Unconstrained model vs. constrained model freeing Inj->IN and ATC->IN (Structural invariant)	0.053993	3	0.9967	0.001
Unconstrained model vs. constrained model freeing Inj->IN and MSR->IN	9.5834	3	0.02246	0.001
Unconstrained model vs. constrained model freeing Inj->IN and DN->IN	0.56963	3	0.9033	0.001

Note. Invariance test. Invariant if chi-square ($\chi 2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D7.2

Regression Coefficients Per Level of Work Experience for the Structural Invariant Model

	Exp1				Exp4			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.621	0.763	0.130	0.000	0.674	0.763	0.130	0.000
*ATC->IN	-0.038	-0.045	0.155	0.773	-0.414	-0.375	0.109	0.001
MSR ->IN	0.058	0.043	0.033	0.194	0.053	0.043	0.033	0.194
DN ->IN	0.039	0.052	0.074	0.479	0.052	0.052	0.074	0.479
*Inj ->IN	0.325	0.220	0.050	0.000	0.521	0.436	0.047	0.000

Note. Structural invariant model: chi-square (χ2) (df=341, N=661)=407.810, p value = 0.007. Null: chi-square (χ2) (df=380, N=661)=6877.103. CFI = 0.990 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.024; 90%CI [0.013 – 0.033])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.041 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.*Indicate parameter significantly different across groups

$\boldsymbol{R(exp1)^2 = 0.542}$. $\boldsymbol{R(exp4)^2 = 0.648}$.

D8 Structural Invariance Across Job Level

The results of the invariance test routine are shown in Table D8.1. The scalar invariant model freeing all regression coefficient to be estimated (unconstrained model) with baseline data from two groups of job level (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 450.803, df = 338, $p < 0.001$, CFI = 0.983, RMSEA = 0.032 (90% CI = 0.023 – 0.039), SRMR = 0.039. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficient to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 466.008, df = 343, $p < 0.001$, CFI = 0.981, RMSEA = 0.033 (90% CI = 0.025 – 0.040), SRMR = 0.041. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained and constrained models were different, the difference test was significant, chi-square ($\chi 2$) diff = 15.206, df = 5, p-value = 0.009519 although the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the following regression coefficients does not produce a difference in terms of fit indexes, ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 2.5321, df = 1, p-value = 0.1116 and the CFI was overlapping (Delta CFI less than 0.01)), MSR->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.1596, df = 1, p-value = 0.2815 and the CFI was overlapping (Delta CFI less than 0.01)), and DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.0084, df = 1, p-value = 0.3153 and the CFI was overlapping (Delta CFI less than 0.01)). Hence ATC->IN, MSR->IN, and DN->IN regression coefficients are not significantly different across groups. In contrast, comparing the unconstrained model with the model constraining the following regression coefficient were different, ATI->IN (the difference test was significant, chi-square ($\chi 2$) diff = 4.6936, df = 1, p-value = 0.03027 although the CFI was overlapping (Delta CFI less than 0.01)), and Inj->IN (the difference test was significant, chi-square ($\chi 2$) diff = 11.634, df = 1, p-value < 0.001 although the CFI was overlapping (Delta CFI less than 0.01)). Hence, ATI->IN and Inj->IN parameters are significantly different across groups. The model constraining all regression coefficients except the ATI->IN and Inj->IN (structural invariant) resulted in a good model fit, chi-square ($\chi 2$) = 455.135, df = 341, $p<0.001$, CFI = 0.983, RMSEA 0.032 (90% CI [0.024 – 0.039]), SRMR = 0.039. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and structural invariant model were invariant, chi-square ($\chi 2$) diff = 4.3329, df = 3, p-value = 0.2277, and the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining the regression coefficient except ATI->IN and Inj->IN is invariant across groups of job level. The regression coefficients across groups are shown in Table D8.2.

Table D8.1

Structural Invariance Results Across Groups of Different Job Level

Model	chi-square ($\chi2$)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	450.803 (p<0.001)	338	0.983	0.032 [0.023-0.039]	0.039
Constrained model	466.008 (p<0.001)	343	0.981	0.033 [0.025-0.040]	0.041
Partially constrained model constraining ATI->IN	455.496 (p<0.001)	339	0.982	0.032 [0.024-0.040]	0.039
Partially constrained model constraining ATC->IN	453.335 (p<0.001)	339	0.983	0.032 [0.024-0.039]	0.039
Partially constrained model constraining MSR->IN	451.962 (p<0.001)	339	0.983	0.032 [0.023-0.039]	0.039
Partially constrained model constraining DN->IN	451.811 (p<0.001)	339	0.983	0.032 [0.023-0.039]	0.039
Partially constrained model constraining Inj->IN	462.437 (p<0.001)	339	0.981	0.033 [0.025-0.041]	0.040
Structural invariant Constrained model freeing ATI->IN and Inj->IN	455.135 (p<0.001)	341	0.983	0.032 [0.024-0.039]	0.039

Note. N=661. df: degrees of freedom. . chi-square ($\chi2$), cutoff $\chi2$ non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square ($\chi2$) diff	df	p-value	Delta CFI
Unconstrained model vs. Constrained model	15.206	5	0.009519	0.002
Unconstrained model vs. Partially constrained model constraining ATI->IN	4.6936	1	0.03027	0.001
Unconstrained model vs. Partially constrained model constraining ATC->IN	2.5321	1	0.1116	0.000
Unconstrained model vs. Partially constrained model constraining MSR->IN	1.1596	1	0.2815	0.000
Unconstrained model vs. Partially constrained model constraining DN->IN	1.0084	1	0.3153	0.000
Unconstrained model vs. Partially constrained model constraining Inj->IN	11.634	1	<0.001	0.002
Unconstrained model vs. structural invariant	4.3329	3	0.2277	0.000

Note. Invariance test. Invariant if chi-square ($\chi2$) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D8.2

Regression Coefficients Per Job Level for the Structural Invariant Model

	Job1				Job3			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
*ATI ->IN	0.636	0.734	0.131	**0.000**	0.847	1.068	0.160	**0.000**
ATC->IN	-0.373	-0.351	0.114	**0.002**	-0.335	-0.351	0.114	**0.002**
MSR ->IN	0.059	0.048	0.034	0.151	0.077	0.048	0.034	0.151
DN ->IN	0.117	0.124	0.079	0.118	0.111	0.124	0.079	0.118
*Inj ->IN	0.466	0.382	0.041	**0.000**	0.273	0.183	0.060	**0.002**

Note. Structural invariant model: chi-square ($\chi 2$) (df=341, N=661)=455.135, p value < 0.001. Null: chi-square ($\chi 2$) (df=380, N=661)=6995.771. CFI = 0.983 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.032; 90%CI [0.024 – 0.039])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.039 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

*Parameter significantly different across groups

$\mathbf{R(job1)^2 = 0.598}$. $\mathbf{R(job3)^2 = 0.621}$.

D9 Structural Invariance Across Organization Size

The results of the invariance test routine are shown in Table D9.1. The scalar invariant model freeing all regression coefficients to be estimated (unconstrained model) with baseline data from three groups of organization size (661 valid responses) was examined. Model fit was good for the unconstrained model, chi-square ($\chi 2$) = 670.531, df = 515, $p < 0.001$, CFI = 0.977, RMSEA = 0.037 (90% CI = 0.029 – 0.045), SRMR = 0.049. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The constrained model fixing all regression coefficient to be equal across groups was examined. Model fit was good for the constrained model, chi-square ($\chi 2$) = 687.630, df = 525, $p < 0.001$, CFI = 0.976, RMSEA = 0.037 (90% CI = 0.029 – 0.045), SRMR = 0.051. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained and constrained models were different, the difference test was significant, chi-square ($\chi 2$) diff = 17.1, df = 10, p-value = 0.07219 although the CFI was overlapping (Delta CFI less than 0.01). The difference between the unconstrained model and five different models each one constraining one regression coefficient only (partially constrained models) was examined. It was found that constraining the following regression coefficients does not produce a difference in terms of fit indexes, ATI->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 2.8547, df = 2, p-value = 0.2399 and the CFI was overlapping (Delta CFI less than 0.01)), ATC->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.9123, df = 2, p-value = 0.3844 and the CFI was overlapping (Delta CFI less than 0.01)), MSR->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 2.8988, df = 2, p-value = 0.2347 and the CFI was overlapping (Delta CFI less than 0.01), and DN->IN (the difference test was not significant, chi-square ($\chi 2$) diff = 1.1289, df = 2, p-value = 0.5687 and the CFI was overlapping (Delta CFI less than 0.01)). Hence ATI->IN, ATC->IN, MSR->IN, and DN->IN regression coefficients are not significantly different across groups. In contrast, comparing the unconstrained model with the model constraining regression coefficient Inj->IN were different, the difference test was significant, chi-square ($\chi 2$) diff = 11.015, df = 2, p-value = 0.004056 although the CFI was overlapping (Delta CFI less than 0.01)). Hence, Inj->IN parameter are significantly different across groups. The model constraining all regression coefficients except the Inj->IN (structural invariant) resulted in a good model fit, chi-square ($\chi 2$) = 683.785, df = 523, $p<0.001$, CFI = 0.976, RMSEA 0.037 (90% CI [0.029 – 0.045]), SRMR = 0.051. The chi-square ($\chi 2$) was statistically significant, but the RMSEA was below 0.06, the SRMR was below 0.08 and the CFI exceeded 0.95. The unconstrained model and structural invariant model were invariant, chi-square ($\chi 2$) diff = 13.255, df = 8, p-value = 0.1034, and the CFI was overlapping (Delta CFI less than 0.01). Thus, the model constraining the regression coefficient except Inj->IN is invariant across groups of organization size. The regression coefficients across groups are shown in Table D9.2.

Table D9.1

Structural Invariance Results Across Groups of Different Organization Size

Model	chi-square (χ2)	df	CFI	RMSEA [90% CI]	SRMR
Unconstrained model	670.531 (p<0.001)	515	0.977	0.037 [0.029-0.045]	0.049
Constrained model	687.630 (p<0.001)	525	0.976	0.037 [0.029-0.045]	0.051
Partially constrained model constraining ATI->IN	673.385 (p<0.001)	517	0.977	0.037 [0.029-0.045]	0.049
Partially constrained model constraining ATC->IN	672.443 (p<0.001)	517	0.977	0.037 [0.029-0.045]	0.049
Partially constrained model constraining MSR->IN	673.429 (p<0.001)	517	0.977	0.037 [0.029-0.045]	0.049
Partially constrained model constraining DN->IN	671.660 (p<0.001)	517	0.977	0.037 [0.028-0.045]	0.049
Partially constrained model constraining Inj->IN	681.546 (p<0.001)	517	0.975	0.038 [0.030-0.046]	0.051
Structural invariant Constrained model freeing Inj->IN	683.785 (p<0.001)	523	0.976	0.037 [0.029-0.045]	0.051

Note. N=661. df: degrees of freedom. . chi-square (χ2), cutoff χ2 non-significant (Jöreskog, 1969)), CFI: comparative fit index, cutoff > 0.95 (Bentler, 1990), RMSEA: root mean square error of approximation, cutoff < 0.06 (Steiger & Lind, 1980), SRMR: Standardized Root Mean Squared Residual, cutoff < 0.08 (Bentler & Wu, 2005).

Model comparison	chi-square (χ2) diff	df	p-value	Delta CFI
Unconstrained model vs. Constrained model	17.1	10	0.07219	0.001
Unconstrained model vs. Partially constrained model constraining ATI->IN	2.8547	2	0.2399	0.000
Unconstrained model vs. Partially constrained model constraining ATC->IN	1.9123	2	0.3844	0.000
Unconstrained model vs. Partially constrained model constraining MSR->IN	2.8988	2	0.2347	0.000
Unconstrained model vs. Partially constrained model constraining DN->IN	1.1289	2	0.5687	0.000
Unconstrained model vs. Partially constrained model constraining Inj->IN	11.015	2	0.004056	0.002
Unconstrained model vs. structural invariant	13.255	8	0.1034	0.001

Note. Invariance test. Invariant if chi-square (χ2) difference non-significant and delta CFI < 0.01 (Hirschfeld & Von Brachel, 2014).
-> regression coefficient

Table D9.2

Regression Coefficients Per Organization Size for the Structural Invariant Model

	Size1				Size4				Size5			
Estimates	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)	Stand	Uns	SE	P(>|z|)
ATI ->IN	0.770	0.852	0.126	0.000	0.728	0.852	0.126	0.000	0.711	0.852	0.126	0.000
ATC->IN	-0.402	-0.370	0.115	0.001	-0.425	-0.370	0.115	0.001	-0.369	-0.370	0.115	0.001
MSR ->IN	0.105	0.065	0.031	0.037	0.103	0.065	0.031	0.037	0.074	0.065	0.031	0.037
DN ->IN	0.115	0.121	0.082	0.142	0.121	0.121	0.082	0.142	0.110	0.121	0.082	0.142
*Inj ->IN	0.398	0.268	0.048	0.000	0.355	0.237	0.058	0.000	0.415	0.367	0.051	0.000

Note. Structural invariant model: chi-square ($\chi 2$) (df=523, N=661)=683.785, p value < 0.001. Null: chi-square ($\chi 2$) (df=570, N=661)=7255.767. CFI = 0.976 (Cutoff > 0.95 (Bentler, 1990)), RMSEA (0.037; 90%CI [0.029 – 0.045])(cutoff < 0.06 (Steiger & Lind, 1980)), SRMR = 0.051 (cutoff < 0.8 (Bentler & Wu, 2005)). Stand: Standardized, Uns: Unstandardized, SE: Standard error. Sc: Scenario. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR.

$\mathbf{R(size1)^2 = 0.614. R(size4)^2 = 0.464. R(size5)^2 = 0.633}$.

E. ITEMS'S DESCRIPTIVE STATISTICS

(From Chapter 4 / 4.1 Item's Descriptive Statistics)

Table E1

Item's Descriptive Statistics Per Scenario

Measure	Indicator	Scenario 1				Scenario 2				Scenario 3				Scenario 4			
		M	SD	Skew	Kurt	M	SD	Skew	Kurt	M	SD	Skew	Kurt	M	SD	Skew	Kurt
ATI	At01	1.78	0.77	0.63	-0.33	1.75	0.78	0.71	-0.28	1.77	0.79	0.51	-1	1.8	0.79	0.71	-0.1
	At02	1.64	0.79	1.17	0.86	1.57	0.7	0.93	-0.02	1.57	0.69	0.92	0.05	1.54	0.71	1.1	0.49
	At03	1.79	0.75	0.7	0.14	1.73	0.77	0.66	-0.48	1.7	0.75	0.71	-0.31	1.75	0.78	0.74	-0.12
	At04	1.59	0.68	1.04	1.1	1.67	0.78	0.97	0.34	1.6	0.75	1.16	0.95	1.63	0.77	1.11	0.71
ATC	At05	2.03	0.95	0.56	-0.68	1.97	0.88	0.68	-0.21	1.98	0.81	0.38	-0.62	2.01	0.93	0.81	0.26
	At06	1.96	0.91	0.79	0.13	1.88	0.82	0.65	-0.2	1.92	0.88	0.64	-0.42	1.87	0.84	0.87	0.55
	At07	2.05	1	0.78	-0.14	2.02	0.91	0.53	-0.62	1.99	0.85	0.44	-0.62	2.08	0.99	0.61	-0.36
	At08	1.85	0.9	0.89	0.23	1.86	0.89	1	0.88	1.96	0.9	0.59	-0.53	1.89	0.95	0.95	0.35
MSR	At09	2.99	1.2	-0.04	-0.92	3.01	1.27	0.01	-1.04	3.07	1.18	-0.13	-0.88	3.06	1.16	-0.31	-0.85
	At10	2.72	1.15	0.19	-0.86	2.59	1.16	0.18	-0.83	2.62	1.11	0.3	-0.54	2.71	1.21	0.03	-1.07
	At11	2.76	1.12	0.01	-0.88	2.62	1.09	0.06	-0.71	2.72	1.04	0.07	-0.52	2.68	1.03	0.08	-0.49
	At12	2.93	1.17	-0.06	-1.06	2.95	1.21	0.05	-0.99	2.96	1.21	-0.08	-1.04	2.91	1.15	-0.22	-0.95
DN	Sn13	1.93	0.89	0.74	-0.17	1.89	0.84	0.61	-0.4	2.01	0.8	0.78	1.21	2.03	0.88	0.82	0.39
	Sn14	1.96	0.88	0.64	-0.29	1.81	0.83	0.7	-0.35	1.94	0.85	0.91	1.01	1.94	0.87	0.67	-0.21
	Sn15	1.9	0.8	0.72	0.18	1.93	0.81	0.64	-0.02	1.89	0.82	0.68	-0.03	2.04	0.84	0.6	-0.14
Inj	Sn16	2.18	1.05	0.74	0.05	2.29	1.12	0.59	-0.37	2.23	1.02	0.61	-0.17	2.16	1.07	0.87	0.28
	Sn17	2.18	1.05	0.84	0.15	2.17	1.09	0.67	-0.29	2.23	1.07	0.79	0.24	2.2	1.11	0.86	0.17
	Sn18	2.21	0.97	0.5	-0.37	2.25	1.11	0.64	-0.28	2.25	1.08	0.84	0.18	2.2	1.1	0.84	0.12
AR	Ar19	1.68	0.71	0.73	0.02	1.76	0.8	0.67	-0.48	1.62	0.71	0.68	-0.78	1.64	0.7	0.81	0.15
	Ar20	1.68	0.76	0.85	0.02	1.71	0.82	0.85	-0.24	1.67	0.77	0.89	0.04	1.6	0.75	1.35	2.23
	Ar21	1.71	0.73	0.77	0.21	1.73	0.78	0.91	0.45	1.6	0.73	0.97	0.2	1.61	0.67	1.09	2.3
IN	In22	1.76	0.87	0.97	0.41	1.76	0.91	1.15	1.03	1.61	0.82	1.23	1.11	1.67	0.87	1.41	1.92
	In23	1.62	0.74	0.98	0.4	1.63	0.84	1.44	2.2	1.6	0.86	1.51	2.21	1.69	0.92	1.37	1.45
	In24	1.68	0.82	1.33	2.12	1.75	0.91	1.03	0.38	1.69	0.97	1.42	1.44	1.61	0.85	1.37	1.42
	In25	1.71	0.8	0.84	-0.1	1.74	0.89	0.92	-0.18	1.63	0.85	1.22	0.64	1.63	0.81	1.2	1.19

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, AR: No anticipated regret. M: mean, SD: Standard deviation, Skew: Skewness (cut off: < 3 (Bentler & Wu, 2005)), Kurt: Kurtosis (cut off < 3 (Bentler & Wu, 2005)).

Table E2

Item's Descriptive Statistics Per Group of Age

Measure	Indicator	Age1 (18 – 34 years old)				Age3 (35 – 44 years old)				Age4 (45 – 54 years old)				Age5 (55 years old and over)			
		M	SD	Skew	Kurt	M	SD	Skew	Kurt	M	SD	Skew	Kurt	M	SD	Skew	Kurt
ATI	At01	1.73	0.79	0.8	-0.08	1.78	0.78	0.69	-0.2	1.79	0.73	0.47	-0.65	1.79	0.8	0.57	-0.73
	At02	1.58	0.77	1.11	0.33	1.6	0.73	1.05	0.62	1.59	0.67	0.84	0.21	1.55	0.72	1.14	0.69
	At03	1.73	0.73	0.65	-0.27	1.79	0.73	0.62	-0.06	1.72	0.78	0.72	-0.39	1.74	0.79	0.79	-0.1
	At04	1.63	0.81	1.23	0.95	1.6	0.69	0.92	0.49	1.63	0.67	0.6	-0.73	1.63	0.78	1.19	1
ATC	At05	1.86	0.86	0.84	0.08	2.05	0.88	0.74	0.24	1.99	0.84	0.41	-0.63	2.08	0.97	0.52	-0.6
	At06	1.8	0.81	0.72	-0.23	1.97	0.89	0.83	0.33	1.95	0.87	0.72	-0.08	1.91	0.88	0.7	-0.05
	At07	1.84	0.8	0.65	-0.18	2.02	0.98	0.88	0.32	2.15	0.92	0.39	-0.72	2.14	1.01	0.42	-0.84
	At08	1.67	0.76	0.94	0.43	1.92	0.95	0.95	0.4	1.98	0.89	0.56	-0.52	1.98	0.98	0.77	-0.02
MSR	At09	2.79	1.26	0.09	-1.13	2.95	1.26	-0.04	-1.08	3.03	1.14	-0.03	-0.79	3.31	1.08	-0.32	-0.45
	At10	2.33	1.13	0.45	-0.68	2.6	1.18	0.29	-0.89	2.64	1.1	0.05	-0.81	3.01	1.11	-0.05	-0.69
	At11	2.49	1.12	0.25	-0.8	2.74	1.1	-0.03	-0.82	2.65	0.93	-0.12	-0.38	2.87	1.06	0.05	-0.52
	At12	2.53	1.21	0.36	-0.99	2.81	1.22	0.03	-1.06	3.05	1.07	-0.13	-0.91	3.31	1.06	-0.36	-0.48
DN	Sn13	1.84	0.82	0.75	-0.03	1.93	0.82	0.65	-0.02	2.03	0.85	0.76	0.54	2.06	0.91	0.74	0.24
	Sn14	1.79	0.82	0.73	-0.23	1.87	0.84	0.78	0.03	2	0.86	0.72	0.36	2.01	0.89	0.67	-0.06
	Sn15	1.87	0.83	0.55	-0.58	1.92	0.75	0.8	0.84	2	0.8	0.71	0.29	1.98	0.87	0.63	-0.28
Inj	Sn16	2.35	1.16	0.67	-0.25	2.3	1.15	0.62	-0.5	2.23	1.03	0.68	-0.03	2.01	0.87	0.53	-0.27
	Sn17	2.31	1.15	0.8	0.05	2.34	1.2	0.66	-0.48	2.13	1.04	0.8	0.09	2.02	0.9	0.59	-0.23
	Sn18	2.35	1.21	0.69	-0.39	2.37	1.17	0.62	-0.49	2.15	0.93	0.63	0.1	2.06	0.89	0.5	-0.31
AR	Ar19	1.65	0.74	0.74	-0.51	1.71	0.7	0.67	0	1.73	0.75	0.69	-0.24	1.63	0.73	0.85	-0.09
	Ar20	1.68	0.87	1.16	0.79	1.73	0.8	0.8	-0.2	1.59	0.68	0.71	-0.64	1.63	0.73	0.99	0.65
	Ar21	1.67	0.77	1.2	1.82	1.75	0.74	0.7	-0.03	1.64	0.66	0.69	0.11	1.59	0.72	1.02	0.52
IN	In22	1.7	0.93	1.38	1.63	1.76	0.82	0.92	0.65	1.73	0.92	1.26	1.29	1.62	0.82	1.12	0.39
	In23	1.73	0.98	1.29	1.02	1.7	0.85	1.3	1.77	1.55	0.73	1.27	1.31	1.57	0.76	1.38	1.97
	In24	1.7	0.96	1.34	1.29	1.68	0.83	1.16	1.04	1.73	0.86	1.2	1.24	1.64	0.89	1.41	1.58
	In25	1.72	0.92	1.14	0.53	1.77	0.82	0.77	-0.22	1.73	0.88	1.03	0.2	1.53	0.71	1.03	0.00

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, AR: No anticipated regret. M: mean, SD: Standard deviation, Skew: Skewness (cut off: < 3 (Bentler & Wu, 2005)), Kurt: Kurtosis (cut off < 3 (Bentler & Wu, 2005)).

Table E3

Item's Descriptive Statistics Per Gender

Measure	Indicator	Male				Female			
		M	SD	Skew	Kurt	M	SD	Skew	Kurt
ATI	At01	1.72	0.75	0.74	-0.1	1.82	0.8	0.56	-0.61
	At02	1.57	0.73	1.11	0.7	1.58	0.73	1.04	0.41
	At03	1.71	0.72	0.59	-0.53	1.77	0.79	0.76	-0.03
	At04	1.59	0.74	1.2	1.16	1.64	0.75	1	0.54
ATC	At05	1.99	0.91	0.66	-0.39	2.01	0.88	0.63	-0.05
	At06	1.9	0.83	0.7	-0.07	1.91	0.89	0.79	0.14
	At07	2	0.9	0.63	-0.23	2.07	0.98	0.62	-0.39
	At08	1.84	0.89	0.88	0.29	1.93	0.93	0.85	0.18
MSR	At09	2.94	1.23	-0.04	-1.04	3.11	1.17	-0.17	-0.79
	At10	2.5	1.13	0.23	-0.91	2.79	1.16	0.11	-0.79
	At11	2.55	1.11	0.24	-0.68	2.82	1.02	-0.08	-0.51
	At12	2.92	1.19	-0.08	-1.05	2.95	1.17	-0.07	-0.94
DN	Sn13	1.92	0.83	0.74	0.31	2.01	0.88	0.73	0.2
	Sn14	1.87	0.85	0.77	0.14	1.95	0.87	0.7	-0.01
	Sn15	1.89	0.77	0.67	0.25	1.99	0.86	0.63	-0.2
Inj	Sn16	2.33	1.16	0.76	-0.16	2.11	0.97	0.51	-0.4
	Sn17	2.27	1.16	0.89	0.05	2.14	1	0.61	-0.19
	Sn18	2.34	1.16	0.74	-0.27	2.13	0.96	0.58	-0.12
AR	Ar19	1.62	0.7	0.91	0.43	1.73	0.75	0.61	-0.59
	Ar20	1.63	0.77	1.04	0.43	1.69	0.78	0.96	0.55
	Ar21	1.63	0.66	0.72	0.01	1.69	0.77	1.03	0.89
IN	In22	1.68	0.87	1.36	1.87	1.71	0.87	1.07	0.58
	In23	1.59	0.81	1.57	2.74	1.68	0.86	1.24	1.22
	In24	1.61	0.85	1.55	2.38	1.74	0.92	1.14	0.79
	In25	1.59	0.78	1.18	0.71	1.75	0.87	0.94	0.14

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, AR: No anticipated regret. M: mean, SD: Standard deviation, Skew: Skewness (cut off: < 3 (Bentler & Wu, 2005)), Kurt: Kurtosis (cut off < 3 (Bentler & Wu, 2005)).

Table E4

Item's Descriptive Statistics Per Group with Different Levels of Education

Measure	Indicator	Edu1				Edu3				Edu5				Edu6			
		M	SD	Skew	Kurt	M	SD	Skew	Kurt	M	SD	Skew	Kurt	M	SD	Skew	Kurt
ATI	At01	1.87	0.74	0.33	-0.79	1.73	0.81	0.76	-0.41	1.76	0.78	0.74	-0.14	1.78	0.76	0.6	-0.41
	At02	1.73	0.79	0.7	-0.46	1.48	0.65	1.23	1.32	1.59	0.76	1.07	0.4	1.55	0.7	1.15	1
	At03	1.85	0.83	0.61	-0.48	1.69	0.73	0.78	0.05	1.74	0.76	0.78	0.09	1.73	0.72	0.45	-0.99
	At04	1.75	0.81	0.84	-0.01	1.58	0.75	1.21	1.09	1.6	0.72	1.04	0.73	1.59	0.7	1.17	1.41
ATC	At05	1.97	0.85	0.46	-0.6	1.96	0.88	0.72	0.09	2.01	0.89	0.59	-0.41	2.07	0.97	0.67	-0.29
	At06	2.01	0.87	0.43	-0.69	1.85	0.88	0.74	-0.1	1.86	0.84	0.87	0.32	1.96	0.87	0.92	0.72
	At07	2.01	0.9	0.52	-0.59	2.04	0.92	0.64	-0.03	2	0.93	0.68	-0.25	2.12	1.03	0.58	-0.66
	At08	1.83	0.82	0.84	0.64	1.85	0.87	0.85	0.24	1.91	0.97	0.91	0.14	1.96	0.95	0.73	-0.18
MSR	At09	2.83	1.12	0.13	-0.8	3.14	1.2	-0.23	-0.89	3.09	1.23	-0.14	-0.97	2.97	1.2	-0.16	-0.9
	At10	2.38	1.09	0.23	-0.83	2.67	1.17	0.23	-0.83	2.73	1.14	0.14	-0.78	2.8	1.2	0	-1.03
	At11	2.45	1.04	0.45	-0.11	2.81	1.02	-0.08	-0.58	2.8	1.07	-0.05	-0.63	2.61	1.13	0.09	-0.9
	At12	2.63	1.06	0.2	-0.75	2.99	1.18	-0.11	-1.01	3.02	1.21	-0.16	-0.95	3.01	1.22	-0.2	-1.1
DN	Sn13	2	0.87	0.51	-0.54	1.98	0.85	0.8	0.51	1.93	0.87	0.89	0.66	1.98	0.82	0.62	-0.06
	Sn14	1.87	0.82	0.5	-0.65	1.92	0.88	0.7	-0.25	1.91	0.88	0.9	0.62	1.96	0.84	0.63	-0.13
	Sn15	1.94	0.8	0.49	-0.41	1.96	0.83	0.66	-0.04	1.94	0.86	0.76	0.05	1.92	0.75	0.57	0.16
Inj	Sn16	2.27	1.08	0.62	-0.25	2.09	0.94	0.63	0.02	2.09	0.99	0.57	-0.49	2.54	1.25	0.65	-0.57
	Sn17	2.2	1.06	0.78	0.11	2.03	0.99	0.75	0.1	2.18	1.04	0.68	-0.11	2.46	1.24	0.75	-0.43
	Sn18	2.21	0.99	0.52	-0.34	2.09	0.97	0.75	0.24	2.19	1.02	0.63	-0.18	2.5	1.29	0.63	-0.68
AR	Ar19	1.72	0.76	0.62	-0.67	1.66	0.73	0.78	-0.21	1.67	0.71	0.64	-0.54	1.66	0.72	0.97	0.79
	Ar20	1.77	0.86	0.69	-0.7	1.64	0.72	0.9	0.31	1.61	0.77	1.22	1.41	1.68	0.77	1.02	0.63
	Ar21	1.7	0.73	0.64	-0.47	1.66	0.72	0.95	0.67	1.64	0.75	1.16	1.61	1.67	0.7	0.81	0.43
IN	In22	1.82	0.9	0.88	0.19	1.65	0.8	1.13	0.97	1.64	0.86	1.25	0.96	1.77	0.93	1.42	2.08
	In23	1.72	0.87	1.09	0.74	1.58	0.77	1.36	1.89	1.65	0.9	1.46	1.93	1.62	0.82	1.45	2.18
	In24	1.85	1.03	1.12	0.58	1.61	0.8	1.12	0.41	1.67	0.92	1.43	1.79	1.64	0.78	1.2	1.15
	In25	1.81	0.94	0.79	-0.58	1.66	0.84	1.14	0.53	1.61	0.77	1.14	1.04	1.69	0.8	0.98	0.29

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, AR: No anticipated regret. M: mean, SD: Standard deviation, Skew: Skewness (cut off: < 3 (Bentler & Wu, 2005)), Kurt: Kurtosis (cut off < 3 (Bentler & Wu, 2005)).
Edu1: High school graduate, no college, and less than high school diploma, Edu3: Some college, no degree, and associate degree, Edu5: Bachelor's degree, Edu6: Advance degree.

Table E5

Item's Descriptive Statistics Per Group of Work Experience

Measure	Indicator	Exp1				Exp4			
		M	SD	Skew	Kurt	M	SD	Skew	Kurt
ATI	At01	1.74	0.78	0.82	0.12	1.79	0.78	0.58	-0.59
	At02	1.65	0.81	1.07	0.43	1.55	0.69	1.01	0.36
	At03	1.75	0.73	0.67	0.02	1.74	0.77	0.72	-0.23
	At04	1.65	0.8	1.16	0.87	1.61	0.72	1.03	0.69
ATC	At05	1.86	0.86	0.88	0.2	2.05	0.9	0.56	-0.31
	At06	1.8	0.8	0.81	0.2	1.95	0.88	0.72	0
	At07	1.88	0.81	0.72	0.06	2.1	0.98	0.56	-0.48
	At08	1.76	0.82	1.12	1.24	1.94	0.94	0.77	-0.03
MSR	At09	2.53	1.21	0.39	-0.89	3.23	1.14	-0.27	-0.66
	At10	2.21	1.13	0.7	-0.32	2.83	1.12	0.01	-0.75
	At11	2.36	1.1	0.43	-0.63	2.83	1.03	-0.06	-0.46
	At12	2.43	1.18	0.48	-0.79	3.13	1.12	-0.25	-0.77
DN	Sn13	1.84	0.77	0.71	0.18	2.02	0.88	0.72	0.19
	Sn14	1.75	0.8	0.79	-0.08	1.98	0.87	0.7	0.06
	Sn15	1.9	0.76	0.47	-0.3	1.96	0.84	0.7	0.03
Inj	Sn16	2.49	1.21	0.56	-0.58	2.1	0.98	0.68	0
	Sn17	2.53	1.23	0.58	-0.59	2.07	0.98	0.78	0.2
	Sn18	2.56	1.26	0.51	-0.79	2.1	0.95	0.65	0.02
AR	Ar19	1.68	0.72	0.73	-0.11	1.68	0.73	0.75	-0.24
	Ar20	1.73	0.87	1.05	0.53	1.64	0.73	0.91	0.19
	Ar21	1.74	0.78	1.03	1.28	1.63	0.7	0.87	0.3
IN	In22	1.78	0.87	1.14	1.25	1.67	0.86	1.23	1.14
	In23	1.74	0.96	1.38	1.56	1.6	0.79	1.3	1.5
	In24	1.7	0.88	1.23	1.22	1.68	0.89	1.34	1.46
	In25	1.78	0.89	1.01	0.45	1.64	0.81	1.06	0.26

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, AR: No anticipated regret. M: mean, SD: Standard deviation, Skew: Skewness (cut off: < 3 (Bentler & Wu, 2005)), Kurt: Kurtosis (cut off < 3 (Bentler & Wu, 2005)).
Exp1: Less than ten years. Exp4 more than ten years.

Table E6

Item's Descriptive Statistics Per Group of Job Level

Measure	Indicator	Job1				Job3			
		M	SD	Skew	Kurt	M	SD	Skew	Kurt
ATI	At01	1.8	0.79	0.63	-0.39	1.68	0.75	0.7	-0.53
	At02	1.57	0.71	1.04	0.55	1.6	0.79	1.12	0.36
	At03	1.78	0.77	0.68	-0.2	1.63	0.71	0.79	-0.14
	At04	1.64	0.75	1.08	0.81	1.56	0.71	1.1	0.71
ATC	At05	2.04	0.9	0.63	-0.21	1.85	0.85	0.67	-0.38
	At06	1.94	0.88	0.75	0.07	1.79	0.8	0.75	-0.1
	At07	2.08	0.95	0.58	-0.34	1.86	0.89	0.85	-0.04
	At08	1.91	0.91	0.84	0.22	1.79	0.92	1.01	0.39
MSR	At09	3.12	1.15	-0.17	-0.81	2.69	1.32	0.21	-1.14
	At10	2.72	1.15	0.11	-0.83	2.4	1.16	0.42	-0.73
	At11	2.76	1.04	0.02	-0.54	2.47	1.17	0.28	-0.85
	At12	2.96	1.16	-0.12	-0.94	2.82	1.26	0.12	-1.13
DN	Sn13	2	0.86	0.73	0.32	1.83	0.83	0.79	0.02
	Sn14	1.94	0.85	0.67	-0.07	1.84	0.88	0.98	0.62
	Sn15	1.97	0.83	0.65	-0.02	1.84	0.77	0.68	0.06
Inj	Sn16	2.13	0.98	0.65	0.02	2.53	1.31	0.5	-0.91
	Sn17	2.13	0.99	0.71	0.11	2.46	1.35	0.63	-0.82
	Sn18	2.16	0.96	0.64	0.05	2.5	1.37	0.52	-1
AR	Ar19	1.69	0.72	0.69	-0.24	1.63	0.77	0.94	-0.02
	Ar20	1.68	0.77	0.94	0.44	1.6	0.79	1.21	0.78
	Ar21	1.66	0.71	0.95	0.94	1.68	0.78	0.91	0.13
IN	In22	1.68	0.84	1.12	0.85	1.79	0.98	1.32	1.37
	In23	1.63	0.83	1.4	1.99	1.66	0.88	1.32	1.24
	In24	1.7	0.9	1.32	1.45	1.63	0.82	1.19	0.73
	In25	1.66	0.82	1.04	0.39	1.73	0.89	1.07	0.24

Note. ATI: Negative attitudes toward the importance of security recommendations (SR), ATC negative attitudes toward the completeness of SR, MSR: Mildness of SR, DN: Negative descriptive norms, Inj: Negative injunctive norms, IN: Intentions of not following SR, AR: No anticipated regret. M: mean, SD: Standard deviation, Skew: Skewness (cut off: < 3 (Bentler & Wu, 2005)), Kurt: Kurtosis (cut off < 3 (Bentler & Wu, 2005)).
L1: Entry and mid-level, L3: Executive level.

F. VARIANCE – COVARIANCE MATRICES

(From Chapter 4 / 4.1 Item's Descriptive Statistics)

Table F1

Variance-Covariance Matrix Per Scenario for the Original Seven-Factor Solution

Factor	Scenario	ATI	ATC	MSR	DN	Inj	AR	IN	Factor labels
ATI	Sc1	0.301							Negative attitudes toward the importance of security recommendations
	Sc2	0.322							
	Sc3	0.387							
	Sc4	0.361							
ATC	Sc1	0.384	0.594						Negative attitudes toward the completeness of security recommendations.
	Sc2	0.301	0.494						
	Sc3	0.340	0.387						
	Sc4	0.417	0.601						
MSR	Sc1	0.025	0.114	0.738					Mildness of security recommendations.
	Sc2	-0.048	0.152	1.247					
	Sc3	0.036	0.126	0.656					
	Sc4	0.088	0.240	0.695					
DN	Sc1	0.275	0.395	0.078	0.393				Negative descriptive norms relative to security recommendations.
	Sc2	0.294	0.437	0.129	0.499				
	Sc3	0.292	0.324	0.067	0.387				
	Sc4	0.257	0.344	0.184	0.418				
Inj	Sc1	0.283	0.300	-0.060	0.278	0.697			Negative injunctive norms regarding following security recommendations.
	Sc2	0.194	0.209	-0.238	0.285	0.919			
	Sc3	0.204	0.136	-0.093	0.097	0.726			
	Sc4	0.198	0.202	-0.142	0.131	0.915			
AR	Sc1	0.147	0.158	-0.029	0.126	0.214	0.208		No anticipated regret relative to not following security recommendations.
	Sc2	0.231	0.211	0.017	0.234	0.295	0.364		
	Sc3	0.134	0.050	0.113	0.205	0.244	0.244		
	Sc4	0.179	0.194	0.108	0.125	0.202	0.243		
IN	Sc1	0.232	0.230	-0.036	0.202	0.430	0.251	0.403	Intention of not following security recommendations.
	Sc2	0.226	0.207	-0.081	0.225	0.336	0.365	0.402	
	Sc3	0.295	0.210	0.022	0.214	0.344	0.310	0.522	
	Sc4	0.274	0.271	0.120	0.199	0.362	0.295	0.518	

VITA

Miguel Angel Toro-Jarrín

Engineering Management and Systems Engineering Department

2101 Engineering Systems Building, Norfolk, VA 23529

e – mail: matoro81@hotmail.com

Awards

Fulbright Student Award (USD260,000)

Academic Excellence Award (USD 55,000)

Cybersecurity Initiative Award (USD25,000)

Education

August 2022: Ph.D. Engineering Management and Systems Engineering. Old Dominion University, Norfolk, Virginia.

May 2015: Maestro en Ciencias con Especialización en Calidad y Productividad (M.Sc. Quality & Productivity). Tecnológico de Monterrey (Monterrey Institute of Technology), Monterrey, México

August 2005: Ingeniero en Electrónica y Control (Bachelor of Science in Electronic Engineering). Escuela Politécnica Nacional (National Polytechnic School), Quito, Ecuador

Teaching Experience

2020 – Present: Engineering Economics Analysis and Project Management. Engineering Management and Systems Engineering Department. Old Dominion University, Norfolk, Virginia.

2007 – 2011: Automation Systems and Devices, Siemens Ecuador

Research Experience

Aug 2017 – 2022: Determinants of information security related actions in organizations. Old Dominion University, Norfolk, Virginia.

May 2014 – May 2015: Strategic Management. Tecnológico de Monterrey (Monterrey Institute of Technology), Monterrey, México

Professional affiliations

Academy of Management

Association for Information systems

American Society for Engineering Management

The word processor for this dissertation was Miguel Angel Toro-Jarrin.