

Protecting Organizational Information Assets: Exploring the Influence of Regulatory Focus on Rational Choices

A. J. Burns
Baylor University
aj_burns@baylor.edu

Abstract

Protecting organizational information assets is an essential objective for most organizations. More than ever, information security relies on insiders with access to information in their work. This research integrates regulatory focus theory with rational choice theory to help shed light on these insiders' motivations to protect organizational information. The result of these exploratory analyses indicates that promotion and prevention foci each distinctly relate to perceived costs and benefits of protecting organizational information assets. Additionally, the findings show that the overall benefit of protecting mediates an expanded set of costs and benefits. Ultimately, the model explains 57.1% of the variance in insiders' intentions to protect organizational information assets.

1. Introduction

Protecting sensitive information and information systems (IS) is a crucial task for many organizations. Today, organizational insiders (or simply insiders) have new responsibilities to ensure the security of organizational information and IS [5]. These insiders are all agents of the firm with access to information and IS [38]. Because insiders are entrusted with organizational information to complete any of a number of job roles and work-related tasks, their behaviors with this information are of paramount importance for information security [37, 12, 16]. Therefore, understanding how insiders make security-related decisions becomes an essential goal of IS security researchers [32].

Many theoretical perspectives have been examined to help understand insider security-related behavior. Underlying many of these prior studies [e.g., 43, 4, 47, 10] are the mechanisms by which individuals weigh the consequences of their decisions. One theory that helps explain human decision-making is rational choice theory (RCT) [13]. RCT's core philosophy is somewhat simple: people are utility seeking agents that make decisions based on their evaluation of the benefits and costs of their choices [4]. Essentially, this

means that individuals weigh the benefits and the costs associated with behavior when forming their intentions [39].

As exhibited by the large body of literature, based, at least in part, on rational choice theory, calculating costs and benefits of security-related behavior can be influenced by many factors. For example, several studies have considered the influence of organizational sanctions [e.g., 25, 15], security threat severity [e.g., 26, 6, 42], and both negative and positive emotional reactions to confronting security threats [e.g., 8, 14, 21].

Despite these significant advances in our understanding of insiders' security-related behaviors, researchers continue to call for broader theoretical consideration of these issues [48, 32, 27, 36]. Additionally, much of the prior research has examined RCT in the context of policy compliance [e.g., 4]. While this is an important area or investigation for IS security, research indicates that the motives to comply and protect are distinct [7]. Thus, we contend that a candidate for further theoretical extension of rational choices and security-related behavior is integration with regulatory focus theory (RFT) [19] to examine motivations to protect organizational information assets.

Although RFT has been examined by behavioral and organizational theorists across many contexts, it has not been widely studied in the context of information security [30]. RFT posits that individuals' motivations can be explained by their promotion or prevention focus [19]. The lack of security research investigating RFT is somewhat surprising given that a significant body of literature deals with both preventing [15, 13, 44] and promoting [37, 6, 3] various security-related behaviors and organizational outcomes.

Given this opportunity, we set out to perform an initial exploration of the relationship of regulatory focus, rational choices (i.e., perceptions of the costs and benefits), and intentions to protect organizational information assets. Distinct from the compliance intentions in prior RCT research [e.g., 4], intentions to protect go beyond "explicitly defined responsibilities incorporating extra-role behaviors that are not

associated with rewards for performance or punishments for inaction” [7, p. 1192].

2. Theoretical Background

As noted, this research seeks to integrate two well-established theories of rational choices (i.e., RCT [4]) and regulatory focus (i.e., RFT [19]). RCT explains that individuals consider the benefits and costs of a course of action to determine their behavior [4]. RFT posits that individuals’ motivations can further be explained by their promotion or prevention focus [19]. We contend that these theories are complementary because the emphasis on promotion or prevention likely influences the perceptions of costs and benefits associated with a behavior. For example, prior research distinguishes motivations to protect from motivations to comply [7]. Similarly, the drive to proactively protect the firm from security threats may be distinct from that to prevent a lapse in security. Thus, a prevention-oriented focus might influence perceptions of costs, while a promotion-oriented focus might influence perceptions of benefits.

Next, we provide a more detailed background into our focal theories. Figure 2 exhibits our research model and the theoretical integration of RCT and RFT.

2.1 Rational Choice Theory

RCT reflects an individual’s perceptions of the balance between the costs and benefits of a course of action [4]. At its core, RCT seeks to explain decision making of so-called “rational” actors that choose a utility-maximizing course of action [1]. Indeed, because it accounts for benefits and costs, RCT has been widely applied in economics and provides the underlying mechanism for many models of consumption [17]. As a behavioral choice model, RCT has been commonly used in criminology to help explain the criminal decision-making process [32].

Drawing mainly on its criminology roots, IS security researchers have also employed RCT to understand security policy compliance [4, 10]. For example, Bulgurcu et al. [4] examined the *benefit of compliance*, *cost of compliance*, and *cost of non-compliance* with IS security policies to explain policy compliance. Others have used a general measure of cost-benefit to explain compliance decisions [e.g., 36].

2.2. Regulatory Focus Theory

Regulatory focus theory posits that individuals’ motivations can be explained by their promotion or prevention focus [19]. *Promotion focus* relates to

gains, ideals, and accomplishment, and *prevention focus* refers to duties, obligations, and security [22]. Thus, promotion focus reflects achievement-oriented motivation, while prevention focus reflects an avoidance-oriented basis [22]. Depending on the organizational or personal objective, promotion or prevention focus might provide a more effective motivational stimulus [28, 41]. For example, a prevention focus often leads to conservative choices, while promotion focus is linked to riskier options [2].

Interestingly, regulatory focus is at once a lingering personality characteristic and a temporary state [22]. Despite the clear relevance for IS security stemming from the two regulatory approaches, relatively little research has examined RFT and IS security-related behavior. A notable exception is research showing regulatory focus moderates the role of punishments (prevention focus) and rewards (promotion focus) on insiders’ ISP compliance [30]. Given that both RFT and RCT distinguish between benefits (achievement orientation) and costs (avoidance orientation), we contend that a natural extension of these seminal theories is to consider them together.

3. Hypotheses

Next, we briefly discuss our hypotheses. Adapting and extending the prior work of Bulgurcu et al. [4], we conceptualize four distinct benefits and costs to protecting the information assets: (1) cost of protecting, (2) benefit of protecting, (3) cost of not protecting, and finally (4) benefit of not protecting. While the first of these were adapted directly from the prior work, the fourth, the benefit of not protecting, is novel to this study. Because this is an exploratory work, we are interested in distinguishing the influence of promotion and prevention foci on the various costs and benefits of protecting information assets. We are also the first to formally examine how individual costs and benefits of protecting organizational assets influence the overall benefit of protecting organizational information.

3.1. Promotion Focus on Benefits and Costs

Promotion focus is oriented toward achievement. Promotion-focused individuals typically employ an eagerness strategy framed around the potential for gains [41]. However, this reality is complicated because some perceived costs result in a security benefit. For example, the *cost of not protecting* works counter to *not protecting* (i.e., it is a motivational force that counteracts harmful security behaviors), whereas the *cost of protecting* works as a disincentive to

protecting (i.e., it is a motivational force that enhances harmful security behaviors). Figure 1 exhibits the relationship between the various costs/benefits, and their association with an increase/decrease in organizational security.



Figure 1. Costs, Benefits, and Organizational Security

At issue is that both regulatory foci are motivational frames. Thus, a benefit or a cost can depend on the salience of a higher- or lower-order outcome or goal. This is similar to the distinction among higher- and lower-order effects in other theories used in IS research [7, 9]. We hypothesize that a promotion focus will be positively related to security-enhancing behaviors and negatively associated with harmful information security behaviors.

H1a: Promotion focus will be positively related to the benefit of protecting.

H1b: Promotion focus will be negatively related to the benefit of not protecting.

H1c: Promotion focus will be negatively related to the cost of protecting.

H1d: Promotion focus will be positively related to the cost of not protecting.

H1d: Promotion focus will be positively related to the cost of not protecting.

3.2. Prevention Focus on Benefits and Costs

Prevention focus reflects a motivational tendency framed around avoidance of losses. These individuals typically employ a vigilance strategy to preserve status and avoid losses [41]. As noted above, this is complicated by costs and benefits that can influence organizational security differently, depending on the salience of the goal or outcome. As such, we hypothesize that prevention focus will also positively relate to security-enhancing behaviors and negatively associate with harmful information security behaviors.

H2a: Prevention focus will be positively related to the benefit of protecting.

H2b: Prevention focus will be negatively related to the benefit of not protecting.

H2c: Prevention focus will be negatively related to the cost of protecting.

H2d: Prevention focus will be positively related to cost of not protecting.

3.3. Individual Costs and Benefits on Overall Benefit of Protecting

Previous researchers have examined the costs and benefits of RCT in different ways. For example, Bulgurcu et al. [4] examined individual costs and benefits, while Moody et al. [36] looked at the overall benefit or cost. Interestingly, researchers have not yet clarified the relationship between individual costs and benefits and the overall cost-benefit balance. Additionally, when prior researchers examined costs and benefits separately, the benefit of *not* performing the action was excluded [4]. This research gap is significant because researchers have found that

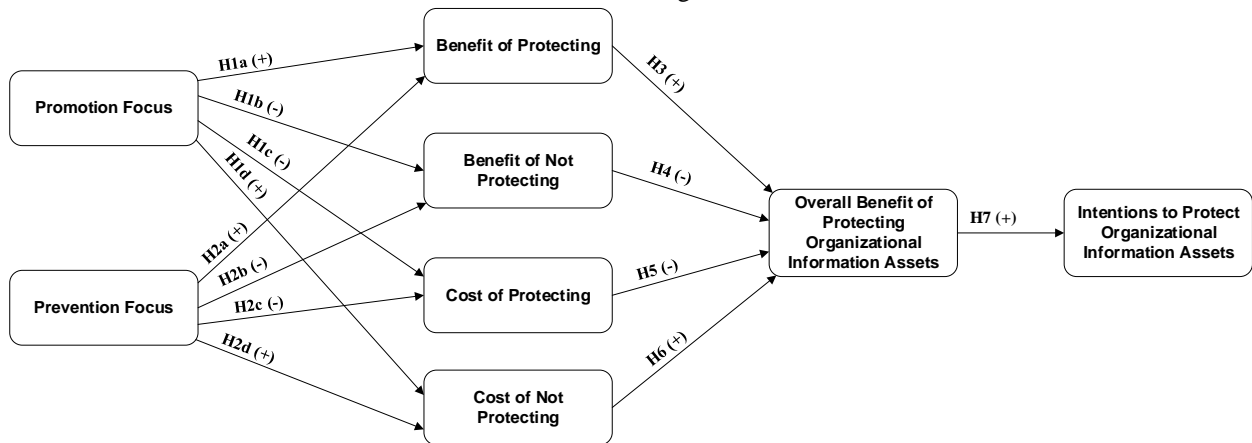


Figure 2. Research Model

motivations exist not to protect one's firm (often described as maladaptive rewards) [6, 37]. Thus, we hypothesize that the four unique costs and benefits will relate to the overall benefit of protecting the organization.

H3: The benefit of protecting will be positively related to the overall benefit of protecting organizational information assets.

H4: The benefit of not protecting will be negatively related to the overall benefit of protecting organizational information assets.

H5: The cost of protecting will be negatively related to the overall benefit of protecting organizational information assets.

H6: Cost of not protecting will be positively related to the overall benefit of protecting organizational information assets.

3.4. Overall Benefit of Protecting Organizational Information Assets on Intentions to Protect Organizational Information Assets

As explained by RCT, the balance between costs and benefits helps explain decision making [4]. Thus, we hypothesize that the overall benefit of protecting organizational information assets will be positively related to insiders' intentions to protect these assets.

H7: Overall benefit of protecting organizational information assets will be positively related to intentions to protect organizational information assets

4. Study

To examine the integrated model of RCT and RFT, we surveyed 295 insiders using an online marketing research firm. Our sample represents organizational insiders working in a variety of roles across many

different companies and industries. As recommended by researchers, we adapted our measures from previous studies whenever possible [45].

Table 1. Sample Statistics

Female	53.2%
Age	45.25
Tenure	10.21
IT position	14.2%
Management	41.0%
Bachelor's degree	61%
Org Size	
Very large (10,000 or more computers)	25.1%
Large (1,000 to 10,000 computers)	28.1%
Medium (100 to 1,000 computers)	21.0%
Small (1 to 100 computers)	25.8%

4.1. Study Measures

Promotion and prevention were measured using scales from Higgins et al. [20]. An item for promotion is "I feel like I have made progress toward being successful in my life," and an item for prevention is "How often did you obey rules and regulations that were established by your parents?"

The benefits and costs of protecting were measured using scales adapted from Bulgurcu et al. [4]. In the original scales, these measures captured the benefits and costs of compliance. Therefore, we adapted these measures to our context of protecting organizational information assets. We also extended this prior work to include the benefit of not protecting. An example item of the benefit of protecting is "My protecting the firm from security threats would be favorable to me."

Table 2. Construct Statistics

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	CR
Benefit Protecting (1)	0.836								0.939
Benefit Not Protecting (2)	-0.195	0.887							0.959
Cost Not Protecting (3)	0.541	-0.299	0.890						0.961
Cost Protecting (4)	-0.048	0.345	-0.143	0.777					0.912
Overall Benefit Protecting (5)	0.468	-0.473	0.497	-0.254	0.629				0.834
Prevention (6)	0.142	-0.195	0.125	-0.183	0.245	0.573			0.869
Promotion (7)	0.122	-0.212	0.191	-0.114	0.215	0.095	0.518		0.809
Protection Intention (8)	0.485	-0.409	0.492	-0.172	0.679	0.206	0.216	0.796	0.921

CR = Composite Reliability; AVEs on diagonal

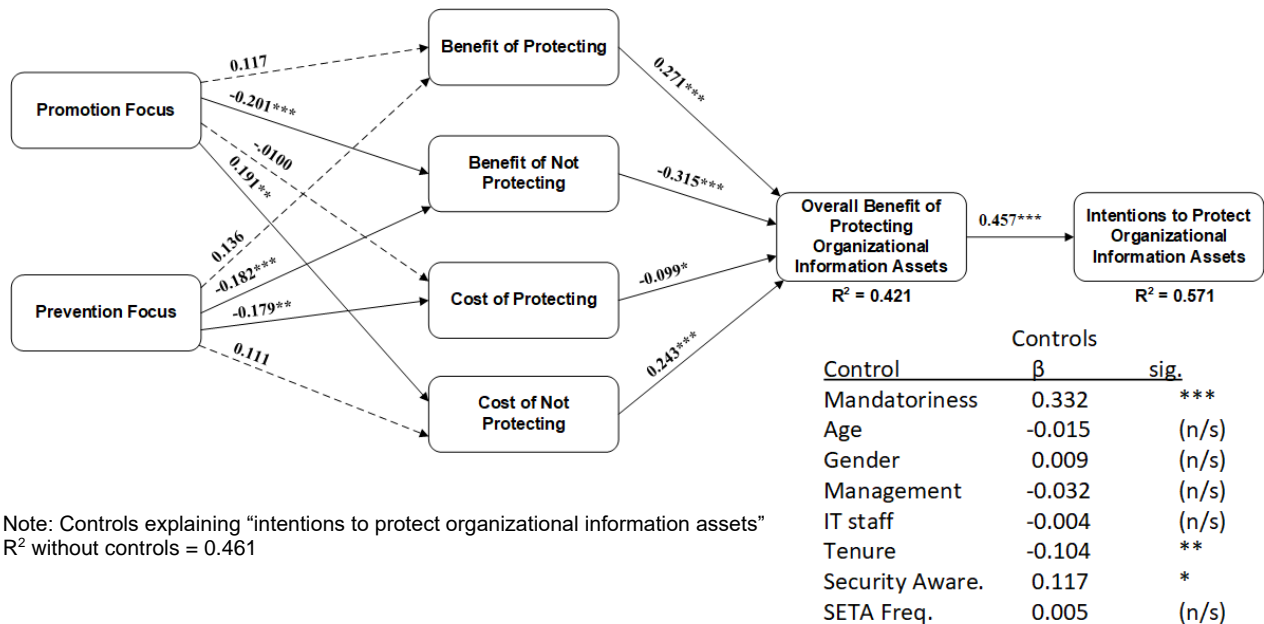


Figure 3. Structural Results

An example item for the cost of protection is “Protecting my firm from information security threats is burdensome for me.” An item for the cost of not protecting is “My failure to protect my firm from information security threats would impact me negatively.” Finally, our adapted measure for the benefit of not protecting is “My failure to protect my firm from information security threats would be favorable for me.”

The overall benefit of protecting construct was adapted from Moody et al. [36]. An example item is “Overall, my benefits from helping to protect my organization from its information security threats outweigh the costs.” Finally, the intention to protect information assets was taken from Posey et al. [37]. An example item is “I intend to protect my organization from its information security threats.”

5. Analysis and Results

We chose the partial least squares-based structural equation modeling platform, SmartPLS 3.0 [40] to perform our analyses. PLS is appropriate for our study because of the exploratory nature of our work [33]. We first evaluated the validity of the measures and subsequently examined our research model.

5.1. Construct Validity

The first criterion we evaluated was the composite reliabilities of each of the measures in our model. The composite reliabilities were all above 0.70. Additionally, all AVEs were above 0.50. Finally, each

pair of constructs met the Fornell-Larker criterion with AVEs greater than squared correlations for every construct pair. Table 2 exhibits the construct statistics.

5.2. Structural Results

Next, we evaluated the results of the structural model. As recommended, we ran the bootstrapping algorithm with 5,000 samples to achieve our results [18]. Figure 3 exhibits the structural results. Overall, 9 of the 13 hypothesized relationships were significant and in the predicted direction. Moreover, the model explains 57.1% of the variance of intentions to protect organizational information assets.

The relationships were all in the direction that increases organizational security (see Figure 1). Thus, for promotion focus, a positive relationship was found with the cost of not protecting, while for prevention focus, a negative association with the cost of protecting was found. Finally, for both foci, a negative relationship was found with the benefit of not protecting.

5.3. Post Hoc Mediation & CMV Analyses

Beyond merely exploring the direct relationships in the research model, we were also interested in measuring the indirect and mediated effects present in the results. For example, it is instructive to see whether the four distinct costs and benefits relate to intentions to protect information assets through the overall benefit of protecting. Second, we also wanted to examine the significance of the relational path from

regulatory focus to protection intentions working through RCT's costs and benefits.

To formally test these indirect effects, the bias-controlled confidence intervals from a bootstrapped analysis of 5,000 samples were examined [35, 46]. To formally evaluate mediation, we examined the 95% confidence interval for each specific indirect effect as calculated in SmartPLS 3.0. Where the upper and lower bounds of the 95% confidence interval for the indirect paths do not contain zero, there is mediation [34]. Table 3 exhibits significant indirect/mediated relationships.

Finally, we examined common method variance (CMV) using the unmeasured latent variable analysis [11]. The average variance explained by the method unmeasured latent variable was only 0.54%, providing evidence that the sample does not suffer from harmful CMV.

6. Discussion

The overriding goal of this research is to explore the relationship of RFT and RCT in motivating insiders' protection of organizational information assets. Prior studies have examined both; however, these previous works did not examine RFT and RCT in concert. Because of RFT's consideration of promotion and prevention foci, it is worth investigating how these orientations influence the perceptions of the relative costs and benefits of protecting information assets. This is true because while promotion and prevention are both motivational paradigms, they each disparately reflect insiders' focus on achievement (promotion) or security (prevention) [31, 41]. Thus, RCT's delineation of costs and benefits is especially relevant for RFT.

The exploratory study results show that promotion focus and prevention focus distinctly influence the

perceptions of benefits and costs. Interestingly, we expected that a promotion focus would be more oriented toward benefits and a prevention focus more oriented toward costs. However, as we detail next, our results tell a more nuanced story.

In terms of the relationship between the facets of RFT and RCT, two important differences emerge. First, promotion focus was positively related to the cost of not protecting and negatively associated with the benefit of not protecting. This finding was intriguing because both RCT components relate to *not protecting* rather than protecting. Intuitively, we might have expected promotion focus, with its orientation around achievement rather than security, to be related to benefits rather than costs.

Second, prevention focus is negatively associated with the benefit of not protecting and the cost of protecting. Again, this is an interesting finding because we might have expected prevention focus to be more oriented toward the costs of not protecting. Instead, we found that prevention focus was most impactful at *reducing the disincentives* to protect. In retrospect, this makes sense because a prevention focus is oriented toward reducing negatives more than increasing positives. Interestingly, neither promotion nor prevention focus showed a significant relationship with the *benefit of protecting*. In fact, the benefit of protecting was the only RCT component that was not impacted by either regulatory focus orientation.

Additionally, the analyses show that the four costs and benefits examined were each related to the overall benefit of protecting information assets. Further, the mediation test results show that overall benefit can act as a mediator of specific individual costs and benefits.

The mediation analyses also indicate that both prevention and promotion have positive indirect effects on insiders' intentions to protect information assets. Interestingly, they worked through one benefit

Table 3. Significant Mediation Relationships

Mediation Relationship	Mediation Test		
	2.5% lower bound ¹	97.5% upper bound	Mediation?
Individual Costs/Benefits on Protection Intention through Overall Benefit			
Benefit of Protecting → Overall Benefit → Protection Intention	0.067	0.189	yes
Benefits of Not Protecting → Overall Benefit → Protection Intention	-0.204	-0.095	yes
Cost of Not Protecting → Overall Benefit → Protection Intention	0.047	0.188	yes
Cost of Protecting → Overall Benefit → Protection Intention	-0.092	-0.002	yes
Regulatory Focus on Protection Intention through Individual Costs/Benefits and Overall Benefit			
Prevention → Benefit of Not Protecting → Overall Benefit → Protection Intention	0.008	0.045	yes
Promotion → Benefit of Not Protecting → Overall Benefit → Protection Intention	0.01	0.051	yes
Promotion → Cost of Not Protecting → Overall Benefit → Protection Intention	0.003	0.047	yes

¹Bias-corrected confidence intervals

and one cost: the benefit of not protecting and the cost of not protecting. Finally, the model explains a substantial portion of both the overall benefit of protecting and the intention to protect information assets.

These results are robust to several demographic and theoretical controls. As shown in figure 3, we included eight control variables in the model to validate our findings. Three controls were significant: mandatoriness of security behavior, security threat awareness, and organizational tenure. We included mandatoriness and security threat awareness because we focused on protection intention beyond formally prescribed organizational actions [7]. The measures for mandatoriness were adapted from Boss et al. [3], and an example item is “My organization requires its employees to take measures to help protect the organization's information security.” The measures for security threat awareness were adapted from Bulgurcu et al. [4], and an example item is “Thinking about your current job, to what extent are you aware of the threats to your organization's information security?” Therefore, we controlled for insiders' awareness of security threats and whether they felt participation in security was mandatory in their organization since these might influence protection intentions.

6.1. Implications and Contributions

This research makes several significant contributions to IS security practice and research. First, our study answers the call for more research into rational choices [32], and our findings show that regulatory focus significantly relates to perceptions of rational choices. The overall perception of benefits (i.e., benefits vs. costs) subsequently relates to insiders' intentions to protect organizational information assets. Next, we consider the specific implications this research has for IS security practice and research.

6.1.1. Implications for Practice

These results have implications for information security practice. This research indicates that regulatory focus influences choice rationality through individual costs and benefits. This reality explains how rational focus can influence information security outcomes in organizations. A primary focus of much IS security research is understanding the attractiveness of beneficial and harmful security behaviors. These results show that regulatory focus influences the cost-benefit calculations of protecting organizational information assets

In the present study, promotion focus was related *negatively* to the perceived benefit of not protecting and *positively* to the perceived cost of not protecting. Thus, insiders with a higher promotion focus calculate higher costs of not protecting information assets and lower benefits to not protecting these assets. While both of these results are positive for information security, they constitute an interesting finding because promotion focus is typically expected to be associated with achievement and gains rather than security and preventing losses.

On the other hand, prevention focus is related negatively to the benefit of not protecting and the cost of protecting. These negative relationships with disincentives to protect show that a prevention-focus leads to minimizing losses in security. Thus, as a motivational frame, these results indicate that prevention focus reduces the perceptions of protection-inhibiting costs and benefits (i.e., the benefit of not protecting and cost of not protecting) but does not impact the perceptions of protection-enhancing costs and benefits (i.e., the cost of protecting and benefit of protecting).

Finally, the research shows that while all four costs and benefits are significantly related to the overall perception of benefits from protecting information assets, some have a more substantial influence than others. For example, the benefit of protecting and the benefit of not protecting exhibited the strongest relationship with the overall benefit of protecting according to the beta coefficient's absolute value. In contrast, the weakest relationship involving the overall benefit of protecting was with the cost of protecting. This finding is intriguing because security professionals tend to think a major inhibitor of positive security-related behaviors stems from their perceived costs in terms of insiders' time and effort. Based on these findings, security practitioners can focus their efforts on amplifying the benefits of protecting and the costs of not protecting, rather than minimizing the perceived costs of protecting organizational assets.

In summary, taking insiders' regulatory focus into consideration can have beneficial impacts on information security. As motivational frames, both foci were related to costs and benefits to protecting organizational information assets in ways that enhance security. However, they worked through distinct costs and benefits. Additionally, we show how distinct costs and benefits relate to the overall perception of the benefit of protecting organizational assets, providing practitioners with a framework for increasing the protection of organizational information assets.

6.1.2. Implications for Research

Beyond the practical implications of the research, our findings also help inform IS security research. For example, we are among the first to integrate RCT with RFT to understand how insiders' regulatory focus influences protective behaviors' rationality. We show that regulatory focus influences distinct costs and benefits. Additionally, the findings indicate that each cost and benefit is uniquely associated with the overall benefit of protecting. In fact, the mediation results indicate that the overall benefit mediates the relationship between distinct costs/benefits and protection intention.

These found relationships between regulatory focus and costs/benefits also underscore another important theoretical contribution of our study: the expansion of previous works [e.g., 4] to include the benefit of not protecting.

Finally, the model explains a substantial portion of the variance in both the overall benefit of protecting and intentions to protect organizational information assets. The model's robust performance indicates that our research provides a compelling theoretical extension of RFT and RCT. Notably, previous research has examined rational choices on compliance with security policies; however, compliance and protection are not the same [7]. Thus, these findings are an important extension of the prior RCT research beyond policy compliance to the more inclusive goal of protecting organizational information assets.

6.2. Limitations and Future Research

It should be noted that this research relies on self-reported perceptions and intentions. However, survey instruments are an accepted medium for ascertaining insiders' security-related perceptions and intentions [3, 24]. To help counter any weaknesses from self-reported measures, we took recommended precautions to ensure that individual anonymity was preserved, and responses were reliable. Future research can address this shortcoming through experimental methods or by measuring actual behavior.

Our findings indicate that the overall benefit mediates distinct costs and benefits. However, regulatory focus worked distinctly through individual costs and benefits. Researchers have been mixed on their use of distinct costs and benefits [e.g., 4] or the overall balance of cost/benefit [e.g., 36]. Therefore, future research should continue to investigate both the overall benefit as well as distinct costs and benefits. When an overall measure is appropriate, our findings provide a new overall measure that mediates individual costs and benefits.

Regulatory focus can be a lingering characteristic or a temporary state [22]. Prior research indicates that regulatory focus can be also be influenced [29]. Additionally, researchers have found that regulatory fit between an individual and a task or environment can also improve motivation [22]. Finally, research indicates that regulatory focus is shaped by environmental cues, including management behavior and communication [23]. Thus, this type of regulatory focus activation provides numerous opportunities for IS security researchers. For example, future research should employ experimental methods to examine the activation of regulatory focus and explore the role of regulatory cues in motivating both protective and harmful IS-related behaviors. Despite the clear relevance for IS security, few studies have investigated RFT in this context [30].

7. Conclusion

This study explored an integrated model of RCT and RFT. The results indicate that regulatory focus relates to distinct costs and benefits of protecting organizational information assets. Specifically, we found that promotion focus relates negatively to the benefit of not protecting and positively to the cost of not protecting, and prevention focus relates negatively to the benefit of not protecting and the cost of protecting.

Extending prior works in RCT [4], the model includes the benefit of not protecting and investigates intentions to protect organizational assets rather than intentions to comply with security policies. The results also show that distinct costs and benefits are mediated through the perceptions of the overall benefit of protecting information assets. However, because regulatory foci disparately impact the individual costs and benefits, the choice of measuring individual costs and benefits versus an overall measure depends largely on the goals of the research.

Finally, the research enumerates important opportunities for future researchers to expand on the role of RFT in IS security. Specifically, as a motivational theory based on prevention and promotion, future researchers should investigate the role of regulatory focus on conflicting organizational goals. For example, some organizational objectives are probably more likely to be framed through promotion cues ("make sales"), while other are probably more likely to be framed with prevention cues ("avoid security incidents"). This research indicates that promotion and prevention foci are both relevant to IS security motivation and intentions.

References

- [1] R. L. Akers, "Rational choice, deterrence, and social learning theory in criminology: The path not taken", *J. Crim. L. & Criminology*, 81, 1990, pp. 653.
- [2] J. M. Boldero and E. T. Higgins, "Regulatory focus and political decision making: When people favor reform over the status quo", *Political Psychology*, 32(3), 2011, pp. 399-418.
- [3] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss, "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security", *European Journal of Information Systems*, 18(2), 2009, pp. 151-164.
- [4] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, 34(4), 2010, pp. 523-548.
- [5] A. J. Burns, C. Posey and T. L. Roberts, "Insiders' Adaptations to Security-Based Demands in the Workplace: An Examination of Security Behavioral Complexity", *Information Systems Frontiers*, 2019.
- [6] A. J. Burns, C. Posey, T. L. Roberts and P. B. Lowry, "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals", *Computers in Human Behavior*(68), 2017, pp. 190-209.
- [7] A. J. Burns, T. L. Roberts, C. Posey, R. J. Bennett and J. F. Courtney, "Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts", *Decision Sciences*, 49(6), 2018, pp. 1187-1228.
- [8] A. J. Burns, T. L. Roberts, C. Posey and P. B. Lowry, "The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking", *Information Systems Research*, 30(4), 2019, pp. 1228-1247.
- [9] C. S. Carver and M. F. Scheier, "Control theory: A useful conceptual framework for personality-social, clinical, and health psychology", *Psychological Bulletin*, 92(1), 1982, pp. 111-135.
- [10] Y. Chen, K. Ramamurthy and K.-W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?", *Journal of Management Information Systems*, 29(3), 2012, pp. 157-188.
- [11] M. S. Choi and A. Durcikova, "Are Printed Documents Becoming Irrelevant? The Role of Perceived Usefulness of Knowledge Repositories in Selecting From Knowledge Sources", *Communications of the Association for Information Systems*, 34(1), 2014, pp. 751-773.
- [12] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin and R. Baskerville, "Future directions for behavioral information security research", *Computers & Security*, 32, 2013, pp. 90-101.
- [13] J. D'Arcy and T. Herath, "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, 20(6), 2011, pp. 643-658.
- [14] J. D'Arcy, T. Herath and M. Shoss, "Understanding employee responses to stressful information security requirements: A coping perspective", *Journal of Management Information Systems*, 31(2), 2014, pp. 285-318.
- [15] J. D'Arcy, A. Hovav and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, 20(1), 2009, pp. 79-98.
- [16] G. Dhillon and J. Backhouse, "Current directions in IS security research: Towards socio-organizational perspectives", *Information Systems Journal*, 11(2), 2001, pp. 127-153.
- [17] S. L. Green, "Rational Choice Theory: An Overview", *Baylor University Faculty Development Seminar on Rational Choice Theory*, 2002.
- [18] J. F. Hair, G. T. M. Hult, C. M. Ringle and M. Sarstedt, *A Primer on Partial Least Squares Structural Equations Modeling (PLS-SEM)*, Sage, Los Angeles, California, 2014.
- [19] E. T. Higgins, "Beyond pleasure and pain", *American psychologist*, 52(12), 1997, pp. 1280.
- [20] E. T. Higgins, R. S. Friedman, R. E. Harlow, L. C. Idson, O. N. Ayduk and A. Taylor, "Achievement orientations from subjective histories of success: Promotion pride versus prevention pride", *European Journal of Social Psychology*, 31(1), 2001, pp. 3-23.
- [21] Huigang Liang, Yajiong Xue, Alain Pinsonneault and Y. A. Wu, "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective", *MIS Quarterly*, 43(2), 2019, pp. 373-394.
- [22] R. E. Johnson, C.-H. Chang and L.-Q. Yang, "Commitment and motivation at work: The relevance of employee identity and regulatory focus", *Academy of management review*, 35(2), 2010, pp. 226-245.
- [23] R. E. Johnson, D. D. King, S.-H. Lin, B. A. Scott, E. M. Jackson Walker and M. Wang, "Regulatory focus trickle-down: How leader regulatory focus and behavior shape follower regulatory focus", *Organizational Behavior and Human Decision Processes*, 140, 2017, pp. 29-45.

- [24] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study", *MIS Quarterly*, 34(3), 2010, pp. 549-566.
- [25] A. C. Johnston, M. Warkentin and M. Siponen, "An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric", *MIS Quarterly*, 39(1), 2015, pp. 113-134.
- [26] A. C. Johnston and M. E. Warkentin, "Fear appeals and information security behaviors: An empirical study", *MIS Quarterly*, 34(2), 2010, pp. 549-566.
- [27] M. Karjalainen, S. Sarker and M. Siponen, "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective", *Information Systems Research*, 30(2), 2019, pp. 687-704.
- [28] K. Lanaj, C.-H. Chang and R. E. Johnson, "Regulatory focus and work-related outcomes: a review and meta-analysis", *American Psychological Association*, 2012.
- [29] D. Laufer and J. M. Jung, "Incorporating regulatory focus theory in product recall communications to increase compliance with a product recall", *Public Relations Review*, 36(2), 2010, pp. 147-151.
- [30] H. Liang, Y. Xue and L. Wu, "Ensuring employees' it compliance: Carrot or stick?", *Information Systems Research*, 24(2), 2013, pp. 279-294.
- [31] P. Lockwood, C. H. Jordan and Z. Kunda, "Motivation by positive or negative role models: regulatory focus determines who will best inspire us", *Journal of personality and social psychology*, 83(4), 2002, pp. 854.
- [32] P. B. Lowry, T. Dinev and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda", *European Journal of Information Systems*, 26(6), 2017, pp. 546-563.
- [33] P. B. Lowry and J. Gaskin, "Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it", *IEEE Transactions on Professional Communication*, 57(2), 2014, pp. 123-146.
- [34] D. P. MacKinnon, *Introduction to Statistical Mediation Analysis*, Erlbaum, New York, NY, 2008.
- [35] D. P. MacKinnon, C. M. Lockwood and J. Williams, "Confidence Limits for the Indirect Effect: Distribution of the Product and Resampling Methods", *Multivariate behavioral research*, 39(1), 2004, pp. 99-99.
- [36] G. D. Moody, M. Siponen and S. Pahlila, "Toward a unified model of information security policy compliance", *MIS Quarterly*, 42(1), 2018, pp. 285-311.
- [37] C. Posey, T. L. Roberts and P. B. Lowry, "The impact of organizational commitment on insiders' motivation to protect organizational information assets", *Journal of Management Information Systems*, 32(4), 2015, pp. 179-214.
- [38] C. Posey, T. L. Roberts, P. B. Lowry, R. J. Bennett and J. F. Courtney, "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors", *MIS Quarterly*, 37(4), 2013, pp. 1189-1210.
- [39] S. Ransbotham and S. Mitra, "Choice and chance: A conceptual model of paths to information security compromise", *Information Systems Research*, 20(1), 2009, pp. 121-139.
- [40] C. M. Ringle, S. Wende and J.-M. Becker, "SmartPLS3. Bönningstedt: SmartPLS", 2015.
- [41] A. A. Scholer, X. Zou, K. Fujita, S. J. Stroessner and E. T. Higgins, "When risk seeking becomes a motivational necessity", *Journal of personality and social psychology*, 99(2), 2010, pp. 215.
- [42] S. Schuetz, P. Lowry, D. Pienta and J. Thatcher, "The effectiveness of abstract versus concrete fear appeals in information security", *Journal of Management Information Systems*, 2020, 2020, pp. forthcoming.
- [43] M. Siponen and A. Vance, "Neutralization: New insights into the problem of employee information systems security policy violations", *MIS Quarterly*, 34(3), 2010, pp. 487-502.
- [44] D. W. Straub, "Effective IS security", *Information Systems Research*, 1(3), 1990, pp. 255-276.
- [45] D. W. Straub, M. C. Boudreau and D. Gefen, "Validation guidelines for IS positivist research", *Communications of the Association for Information Systems*, 13(1), 2004, pp. 380-427.
- [46] A. Vance, P. B. Lowry and D. Eggett, "A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface", *MIS Quarterly*, 39(2), 2015, pp. 345-366.
- [47] A. Vance and M. Siponen, "IS security policy violations: A rational choice perspective", *Journal of Organizational and End-User Computing*, 24(1), 2012, pp. 21-41.
- [48] R. Willison and M. Warkentin, "Beyond deterrence: An expanded view of employee computer abuse", *MIS Quarterly*, 37(1), 2013, pp. 1-20.