# The Application of Rhetorical Theory in Designing Effective Information Security Messages for Different Leadership Styles

Sumin Kim
Mississippi State University
sk2013@msstate.edu

Minsek Ko
Iowa State University
minsekk@iastate.edu

Chinju Paul
Mississippi State University
cpaul@business.msstate.edu

## Abstract

*Fear appeal has been widely explored in designing information security messages. However, our understanding of how to design an effective one has yet to be fully explored. This study aims to enhance the effectiveness of fear appeal messages by drawing upon Aristotle's rhetorical theory (pathos, logos, ethos appeals). Furthermore, we employ the elaboration likelihood model (ELM) as a bridging framework to integrate the fear appeal literature with leadership literature, explaining which messaging styles are more effective under different leadership styles (transformational vs. transactional leadership). Therefore, this paper provides a significant theoretical contribution to the fear appeal literature. We anticipate that our planned experiment will yield substantial managerial implications, enabling security managers to strategically craft security compliance messages tailored to the leadership style within their organization.*

**Keywords:** Information security, fear appeal, rhetorical theory, leadership style, elaboration likelihood model

## 1. Introduction

The escalating risk of cyberattacks and security breaches targeting organizations necessitates the implementation of comprehensive security measures to effectively mitigate the frequency of successful intrusions. Hackers employ a range of methods to breach computer information systems (Nieles et al., 2017), which include exploiting compromised Wi-Fi networks or servers, utilizing stolen credentials, deploying phishing attacks through emails, and distributing malware through downloaded files. To safeguard their computer information systems, organizations often prioritize the implementation of robust technical security measures, such as strict access controls, file and hard drive encryption, and security systems like Intrusion Detection and Prevention Systems (IDPS) and Firewalls (Swanson et al., 2006). However, technical measures alone are insufficient to effectively mitigate the security risk without the implementation of organizational measures such as security policies, security trainings, and audits, because insiders (e.g., employees and managers) can be the most vulnerable point or "weakest link" for hackers to exploit when attempting to break into the system (Furnell & Clarke, 2012).

Not surprisingly, understanding insiders' security behaviors and developing methods to increase their security compliance have become important research topics among information security researchers (Crossler et al., 2013). One of their key concerns has been understanding how users perceive and respond to security messages. This understanding is crucial for organizations to design persuasive messages that can effectively influence individuals' attitudes toward security policies and promote security compliance. (Brinton Anderson et al., 2016).

One widely recognized method of creating persuasive messages is leveraging fear appeal, which involves instilling fear in employees to encourage them to follow recommended actions corresponding to security policies (Boss et al., 2015). According to the literature on fear appeal messaging (Johnston & Warkentin, 2010a; Witte, 1992), fear appeal messages must articulate the severity of the threat and the probability of the threat occurring. Numerous studies have shown the effectiveness of fear appeal in changing individuals' attitudes to adhere to security policies and procedures and their security compliance intention (Johnston et al., 2015). However, there is a lack of focus on understanding how to improve these fear appeal messages. In this study, we aim to address this gap in the fear appeal messaging literature.

*RQ1: How can we design effective fear appeal security compliance messages?*

URI: https://hdl.handle.net/10125/106959
978-0-9981331-7-1

To address our first research question, we draw on Aristotle's rhetorical theory (Murphy, 1981), which proposes three rhetorical appeals of persuasion: *pathos* (e.g., emotional responses), *logos* (e.g., logical judgment), and *ethos* (e.g., credibility belief). We examine how fear appeal security compliance messages can be designed more effectively to change individuals' attitudes toward security policies through these rhetorical appeals.

Furthermore, we investigate the effectiveness of different styles of security compliance messages (*logos-based, pathos-based, and ethos-based fear appeal messages*) in changing employees' attitudes toward information security policy compliance, specifically considering different leadership styles. While Torres & Crossler (2019) proposed an experiment that manipulates the elements of rhetoric appeals, no prior studies have examined their relationship with leadership styles.

*RQ2: Does leadership style moderate the effectiveness of rhetorical fear appeal security messages? If so, which rhetorical fear appeal message is more effective in which leadership style?*

We focus on the potential contingency of leadership in relation to the effect of fear appeal security compliance messages for two reasons. First, the leadership literature suggests that leadership can shape the attitudes, intention, and behavior of individuals within an organization. Leadership may set the tone for information security and influence how individuals perceive its importance (relevance) (Jung et al., 1995; Schein, 2004). For example, leadership's resource allocations (e.g., budget and employees) can signal the organization's emphasis on information security and motivates employees in distinct ways (Feng et al., 2019; Schein, 2004).

Second, different leadership styles can motivate individuals differently and influence their tendencies in processing information (Lyons & Schneider, 2009; Sarros & Santora, 2001). This implies that organizations may be able to tailor their persuasion strategies in designing effective rhetorical fear appeal security compliance messages. Although there are research investigating how leadership style can influence employees' security-related intentions in distinct ways (Guhr et al., 2019; Humaidi & Balakrishnan, 2015), the role of rhetoric appeal under different leadership style has yet to be studied in the information security discipline. Understanding the contingency of leadership style on the effects of these messages can bring immediate benefits to organizations, while changing leadership style is often not practical. Thus, investigating the contingency effect of leadership on security compliance messages provides significant practicality (research relevance), justifying the importance of our research. Therefore, this research investigates how leadership style moderates the effectiveness of fear appeal messages.

To address our second research question, we examine how managers could optimize rhetorical fear appeal security compliance messages for their organizations using the Elaboration Likelihood Model (ELM) as our theoretical framework. We take into consideration of two major leadership styles, namely transformational leadership (i.e., appeal to higher-order needs) and transactional leadership (i.e., focus on cost-benefit) (Jensen et al., 2019; Sarros & Santora, 2001), and theorize which rhetorical fear appeal messages (e.g., pathos-based fear appeal) would be more effective in changing individuals' attitude toward the security policies.

The rest of the paper is as follows. First, we present the literature review on the relevant topics. Second, the research model and hypotheses are presented. Next, the method for this study is discussed. Finally, we conclude with a discussion and future study.

## 2. Theoretical Background and Hypotheses

### 2.1 Fear Appeal

Fear appeal has been a predominant approach in the current body of information security literature, employed to design persuasive messages that encourage employees to comply with information security policies and procedures (Boss et al., 2015; Johnston et al., 2019). These fear appeal messages aim to motivate individuals to adopt recommended actions as a means of protecting themselves against security threats by 'scaring' them (Johnston & Warkentin, 2010a; Witte, 1992). Fear appeal message "initiates cognitive appraisal processes concerning (1) the noxiousness or severity of the threatened event, (2) the probability of the occurrence of the event, and (3) the efficacy of a recommended coping response" (Maddux & Rogers, 1983, p. 470).

To effectively promote the desired response, fear-appeal messages must contain threat and efficacy components (Johnston & Warkentin, 2010a; Witte, 1992). Threat components in the security compliance message instill fear in individuals (Witte, 1992), driving them to comply as a coping mechanism to mitigate the perceived threat so that they can protect themselves (Johnston & Warkentin, 2010a). The degree of perceived threat in terms of its severity and susceptibility can vary depending on how individuals perceive and judge it (Johnston et al., 2015).

The efficacy component of a fear-appeal message assures recipients that they are capable of performing the recommended actions and that doing so will lead to desirable consequences (Rogers, 1975; Witte, 1992). In

other words, if the recipients perceive the suggested security measures as difficult for them to implement or ineffective, they are less likely to take the necessary actions. Therefore, understanding individuals' emotional responses (pathos), judgment (logos), and beliefs (ethos) is crucial in designing persuasive information security messages to promote compliance and mitigate security risks.

Furthermore, security researchers in the field of Information Systems (IS) have highlighted the importance of making individuals perceive the relevance of the security threats mentioned in messages (Johnston et al., 2010). For example, Schuetz et al. (2020) found that concrete fear-appeal messages, which enhance the perceived relevance of security threats, are more effective than abstract messages. Also, Johnston et al. (2019) found that employees are more likely to respond to messages that align with their organizational identification, as opposed to messages that lack alignment. When the language used in the message resonates with recipients' rhetoric preferences, employees perceive the messages as personally relevant and take action to protect themselves and the organization. An important implication of these studies is the significant impact of personal relevance introduced by organizations, such as leadership style, on the effectiveness of fear appeal messages.

In the following sections, we will delve into how the three rhetorical appeals –logos, pathos, and ethos– can influence the performance of security compliance messages, and how these appeals may have varying effects in organizations led by different leadership styles, using the ELM framework.

## 2.2 Rhetorical Theory

Rhetorical theory is a device of persuasion, and it investigates how language and symbols can influence the cognitive, emotional, and behavioral responses of message recipients (Higgins & Walker, 2012). Rhetoric can be viewed as an inherent component of our everyday communication and a purposeful and intentional form of communication that aim to persuade the message recipient (Burke, 1969; Hartelius & Browning, 2008; Higgins & Walker, 2012). There are three types of rhetorical appeals—logos, pathos, and ethos—for persuading audiences. Logos appeals to reason, logic, and evidence; pathos appeals to emotions and ideals; ethos appeals to credibility and trustworthiness.

The use of different rhetoric in persuading message recipients (e.g., consumers or employees) is well established in marketing and management literature (Green Jr, 2004; Hartelius & Browning, 2008). For example, Ge and Gretzel (2018) examined, using a rhetorical framework, how a social media influencer employs Emoji as a persuasive strategy to engage their followers. They found that influencers utilize Emoji not only to amplify emotion (pathos), but to enhance argument– (logos) and credibility-based (ethos) appeals. Chu et al. (2014) investigated a web page design of product pages and found that rhetorical devices like logos, pathos, and ethos showed different persuasive power depending on the product type.

Furthermore, management discipline has emphasized the effect of rhetoric, recognizing its significance within organizations. Leadership, in particular, dedicates a substantial amount of time "talking with other people, negotiating, selling, discussing, sharing, questioning, organizing, reporting, motivating, encouraging, challenging, and – in essence – persuading" (Flory & Iglesias, 2010, p. 113). Especially, Heracleous and Klaering (2014) showed how different rhetoric can be strategically employed by leadership depending on the situation, yielding different effects to enhance persuasiveness. Heracleous and his colleague particularly examined the relationship between charismatic leadership and rhetorical competence and how charismatic leaders change their rhetoric (e.g., logos, pathos, and ethos) based on the circumstances, conducting a case study of the rhetoric of Steve Jobs.

In this vein, we investigate the potential of using rhetoric to enhance the persuasiveness of fear appeal messages concerned with information security. In the following section, we explain how fear appeal messages that employ the rhetorical appeals (logos, pathos, ethos) can influence employees' attitudes towards information security policy compliance, which is a direct antecedent of their behavioral intention (Ajzen, 1991; Johnston & Warkentin, 2010b; Johnston et al., 2015). Additionally, it is common practice in the field of information security research to examine the antecedents of employees' security related intention (Bulgurcu et al., 2010; Guo et al., 2011).

**2.2.1 Logos**. Logos appeal emphasizes the argument and references to the shared reality of the author and audience (Killingsworth, 2005). Logos appeals, which are rooted in formal reasoning and logical calculation, can play an important role in changing attitudes (Crano & Prislin, 2008; Green Jr, 2004). Petty and Cacioppo (1986) suggest that strong arguments that contain compelling, logical points can elicit favorable reactions in individuals and lead to attitude change. When presented with a strong argument that is logically sound and aligned with their goals, individuals tend to adopt a positive attitude toward the issue or behavior being discussed (Crano & Prislin, 2008; Petty & Cacioppo, 1986). Overall, the use of logos appeals can be an effective way to persuade individuals to change their attitudes and behaviors.

We argue that the effectiveness of fear appeal messages can be improved by emphasizing the severity and susceptibility of threats through logical statements.

Logos-based fear appeal message, for example, can be "*According to a recent cybersecurity report, in the past 5 years the number of data breach has increased substantially by 25% due to employees' negligence…our company has very high risk of being hacked*" (adapted from Ng et al., 2021). The perception of threat severity can be enhanced by mentioning possible outcome (e.g., "very high risk of being hacked"), and the susceptibility of threat can be highlighted by providing factual information and figures to support the argument (Bronstein, 2013). As we discussed earlier, when the severity and susceptibility of a threat are emphasized using formal reasoning and logical calculations, it arouses fear and has the potential to influence employees' attitudes toward complying with information security policies. This is because they are logically persuaded by the compelling arguments presented in the information security messages. Therefore, we hypothesize:

*H1: Logos-based fear appeal message is positively associated with attitude toward information security policy compliance.*

**2.2.2 Pathos**. Pathos appeal is an approach to persuade message recipients by eliciting an emotional response through the message (Varpio, 2018). The impact of pathos lies in its ability to appeal to individuals' emotions and justify a particular action, often by evoking feelings of greed or fear in the message recipient (Green Jr, 2004). The effect of emotion is well-explored in the Management discipline as an important tool for motivating employees, creating a positive workplace culture, or predicting work-related behaviors (Ashkanasy & Dorris, 2017). The emotional state of the message recipient can be strongly reflected in their attitude and behavior (Petty et al., 2003; Van Kleef et al., 2015). By appealing to emotions for a particular course of action, pathos appeal can serve as a powerful tool for influencing individuals to change their attitudes and behaviors.

This study argues that the effectiveness of fear appeal messages can be improved by emphasizing the severity and susceptibility of threats through pathos-based statements. For example, pathos-based fear appeal message can be "*In recent times, a data breach in our client's company had catastrophic consequences, which led to a significant decline in market share and the termination of the employment for those directly responsible for the breach. Considering that our company employs a similar security system, we are genuinely concerned about the potential occurrence of a similar data breach impacting us."* The threat severity can be enhanced by emphasizing its disastrous outcomes (e.g., a significant decline in market share and the termination of employment). The threat susceptibility, on the other hand, can be strengthened by highlighting genuine concern about its potential occurrence (e.g., "we are genuinely concerned…"). In the end, these message components, which intend to evoke emotion, are intend to instill a sense of fear in employees so that they may change their attitude toward information security policy compliance. This is because their emotional state evoked by security messages is reflected in their attitude. Hence, we hypothesize:

*H2: Pathos-based fear appeal message is positively associated with attitude toward information security policy compliance.*

**2.2.3 Ethos**. Ethos appeal persuades the message recipient by emphasizing characteristics such as credibility, trust, and expertise of the message sender (Varpio, 2018), and emphasizing the credibility of the message itself (Rosenthal, 1971). Ethos appeal influences moral or ethical sensibilities, and it is often evoked by the credibility and moral character of the message sender (Green Jr, 2004; Portolano & Evans, 2005). According to Higgins and Walker (2012), a message may specifically appeal to ethos by including elements such as:

(a) similitude: it appeals to establishing cohesion, harmony, and a sense of community between the message sender and recipient

(b) deference: it involves signaling respect toward the message recipient

(c) expertise: it relies on the qualifications, judgment, or experience of the message sender, appealing to both ethos and logos

(d) self-criticism: it implies the honesty of the message sender in the message

(e) inclination to succeed: it involves highlighting past accomplishments or future success

An implication is that ethos-based fear appeal message can be designed by appealing to the importance of morality and credibility of information security. This standpoint is also highlighted by Donalds and Barclay (2022), which identified objectives of information security compliance such as enhancing customer trust and confidence, and increasing business reputation. Ethos-based fear appeal message can be "*Our company can establish trust and credibility in our business by protecting information security asset. The challenges we faced during last year's data breach were significant for our company. We want to emerge as one of the most secure companies in the nation and another security breach will damage our trust and credibility.*" Particularly, this message appeals to ethos by fostering a sense of community through the use of pronouns (e.g., "we," "our"). It further strengthens the ethos appeal by highlighting that another security breach will damage

the company's reputation. It signals threat severity that failing to protect security would lead to unfavorable consequences, such as the loss of trust and credibility, and threat susceptibility by honestly mentioning the data breach that happened last year. By emphasizing the severity and susceptibility of threat through ethos appeal (e.g., the value of trust and credibility regarding information security within the organization), this statement evokes fear and aim to change employees' attitude toward information security policy compliance. Therefore, we hypothesize:

*H3: Ethos-based fear appeal message is positively associated with attitude toward information security policy compliance.*

## 2.3. Leadership Style

In this study, we focus on two distinct leadership styles (Jensen et al., 2019): transformational and transactional leadership. Transformational leadership pursues collective goals by motivating followers to achieve higher ideals and values through following (Sarros & Santora, 2001):

(a) individualized consideration: "treating individuals as important contributors" (p. 385) and demonstrating consideration for their needs.
(b) inspirational motivation: encouraging the awareness of the organization's vision and encouraging them to committing to it.
(c) intellectual stimulation: encouraging and stimulating creativity and challenges.
(d) idealized influence: being a role model of their employees and inspiring employees with charisma.

To motivate employees to transcend their self-interest and achieve organizational goals, leaders clarify the organization's vision, share it with employees who will execute it, and sustain it in the long run (Jensen et al., 2019). As leadership shares vision, which is a core element of transformational leadership, the message establishes a shared understanding of the work among employees, which encourages and motivates employees to devote their effort toward the vision (Carton et al., 2014; Jensen et al., 2019).

Transactional leadership, on the other hand, is known for its reward and punishment approach in pursuing the organization's goal (Jensen et al., 2019). While transformational leadership expects employees to achieve beyond expected outcomes by motivating group interest, transactional leadership expects them "to finish the job to a satisfactory standard" by motivating self-interest (Sarros & Santora, 2001, p. 389). Rather than motivating employees to use their creative and innovative ideas to achieve organizational goals as transformational leadership does, transactional leadership expects employees to behave based on rules and policies, and to follow its direction "so the job gets done," and it controls them with rewards and sanctions (Sarros & Santora, 2001, p. 388).

In the following section, we discuss the impact of different leadership styles on the effectiveness of security compliance messages (logos-based, pathos-based, ethos-based fear appeal messages) in changing employees' attitudes toward information security policy compliance. Specifically, we employ ELM to explain why individuals may respond differently to the rhetorical elements of the message contingent on the leadership style.

## 2.4 Leadership Style and Elaboration Likelihood Model

ELM is a dual-process approach that explains how the message recipient process information using the central and peripheral route. (Petty & Cacioppo, 1986). It proposes that people use two different routes to process information: the central route and the peripheral route. The central route is used when people are highly motivated to process information and, in this case, they carefully consider the message and its arguments, and they are more likely to be persuaded by strong /logical arguments and issue-relevant arguments (Petty & Cacioppo, 1986). The peripheral route is used when people are less motivated to process information. They may not pay close attention to the message itself, and they are more likely to be persuaded by peripheral cues, such as affect, attractiveness, source credibility, and number of arguments, among others, as per the ELM.

There is a substantial body of research, which used ELM. For their research, they manipulated the degree of motivation or elaboration to process information by using privacy concerns (Angst & Agarwal, 2009; Bansal et al., 2015), job relevance and user expertise (Bhattacherjee & Sanford, 2006), expertise and involvement (Cheung et al., 2012), and need for cognition (Tam & Ho, 2005). If the message respondents are highly motivated, then they use the central route of information processing, which is strongly responded by argument framing (Angst & Agarwal, 2009), argument adequacy (Bansal et al., 2015), argument quality (Bhattacherjee & Sanford, 2006; Cheung et al., 2012), and level of preference matching (Tam & Ho, 2005). If the message respondents are less motivated, then they use the peripheral route of information processing, and are strongly responded by source credibility (Bhattacherjee & Sanford, 2006; Cheung et al., 2012), availability of company information, website information quality, design appeal, and reputation (Bansal et al., 2015),

review consistency and review sidedness (Cheung et al., 2012), and sorting cue and size of recommendation set (Tam & Ho, 2005).

Aforementioned, transformational leadership inspires individual efforts by intrinsically motivating employees and 'transforming' them to achieve organizational goals through higher ideas and values (Jensen et al., 2019; Odumeru & Ogbonna, 2013; Sarros & Santora, 2001). On the other hand, transactional leadership focuses on using external motivation factors, such as rewards and punishments (Odumeru & Ogbonna, 2013). As a result, employees under transformational leadership generally demonstrate greater ownership and commitment to the organization's tasks and missions, while those under transactional leadership are mainly passive and merely comply with rules and policies (Barbuto, 2005; Odumeru & Ogbonna, 2013). Hence, compared to employees under transactional employees, those under transformational leadership may also be more likely to recognize the importance of accomplishing the company's objective of securing valuable information.

An implication is that employees under transformational leadership are more likely to engage in the central route of information processing when receiving security compliance messages. Therefore, we expect that logos-based fear appeal is more effective for employees under transformational leadership compared to transactional leadership. Therefore, we hypothesize:

*H4a: Transformational leadership style has a stronger positive moderating effect on the relationship between logos-based fear appeal and attitude than transactional leadership style.*

ELM suggests that when employees are less motivated in the subject, they are more likely to rely on peripheral cues rather than processing the message arguments themselves (Petty & Cacioppo, 1986; Weizman & Dascal, 1991). Peripheral cues encompass any elements other than the message's argument or its intrinsic meaning (Petty & Cacioppo, 1986; Weizman & Dascal, 1991). Messages associated with pathos (e.g., emotional appeal) and ethos (e.g., credibility appeal) are considered peripheral cues.

As mentioned earlier, transactional leadership leverages extrinsic motivating factors (e.g., rewards and sanctions) to ensure that "the job gets done" without necessarily sharing the organization's vision (Jensen et al., 2019; Odumeru & Ogbonna, 2013; Sarros & Santora, 2001), while transformational leadership relies on intrinsic motivating factors (e.g., higher ideas and values) and establishes a shared understanding of the organization's goals with their employees. Consequently, employees under transactional leadership tend to prioritize their self-interest and have a lower sense of ownership compared to those under transformational leadership (Barling, 2014). Additionally, employees under transactional leadership are likely to have a limited understanding of the organization's goals and their importance, in contrast to those under transformational leadership. Therefore, for employees under transactional leadership, the organization's goal of securing valuable information may be perceived as less important than for those under transformational leadership.

Therefore, instead of concentrating on the argument within the security compliance message, employees under transactional leadership are more likely to focus on peripheral cues, such as pathos and ethos appeal, in the security compliance message compared to those under transformational leadership. Therefore, we hypothesize:

*H4b: Transactional leadership style has a stronger positive moderating effect on the relationship between pathos-based fear appeal and attitude than transformational leadership style.*

*H4c: Transactional leadership style has a stronger positive moderating effect on the relationship between ethos-based fear appeal and attitude than transformational leadership style.*

Employee's attitude toward information security compliance leads to their intention to comply with information security policy (Siponen et al., 2014). Therefore, we hypothesize:

*H5: Attitude towards information security policy compliance is positively associated with intention to comply with information security policy.*

See Figure 1 for the hypothesized model.

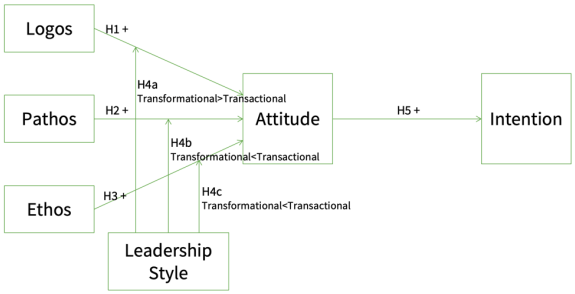


**Figure 1. Hypothesized model.**

## 3. Proposed Methodology

We plan to conduct a controlled experiments to test our hypotheses using a between-subject design. We plan to recruit 600 participants who are working full time (at least 35 hours per week) through Qualtrics subject pool.

Participants will be compensated appropriately for their participation.

### 3.1. Experimental Design and Procedure

A 3 (Rhetorical appeal: logos, pathos, ethos) x 2 (Leadership: transformational leadership, transactional leadership) factorial design will be employed to examine how different rhetorical appeal and leadership influence the employees' intention to comply with information security policy. Participants will be randomly assigned into one of the six experimental conditions. Then, each participant will read a scenario where they are told that they are working at a company. The scenario will describe the leadership style (transformational or transactional) of the company, and they will be also asked to read an email from IT department which emphasizes the importance of information security with different rhetoric (logos, pathos, or ethos). The participants will be asked to answer a survey at the end of the experiment.

### 3.2. Experimental Stimuli

We create three security messages to elicit the three rhetoric appeals. We manipulate the rhetoric appeals of the security message by manipulating the threat component of the message. The efficacy component of the three messages is kept constant. We add logical statement to the fear part to increase the logos appeal of the message. For example, *"According to a recent cybersecurity report, in the past 5 years the number of data breach has increased substantially by 25% due to employees' negligence…our company has very high risk of being hacked"*. The pathos appeal of the message is increased by adding emotion evoking statements to generate fear. *"In recent times, a data breach in our client's company had catastrophic consequence, which led to a significant decline in market share and the termination of the employment for those directly responsible for the breach. Considering that our company employs a similar security system, we are genuinely concerned about the potential occurrence of a similar data breach impacting us*" evokes emotional response. By addition of statements involving trust and credibility, ethos appeal of the fear appeal message can be increased. The statement *"Our company can establish trust and credibility in our business by protecting information security asset. The challenges we faced during last year's data breach were significant for our company. We want to emerge as one of the most secure companies in the nation and another security breach will damage our trust and credibility."* evokes ethos appeal.

Efficacy is achieved by adding efficacy statements [coping mechanism] to improve security to the security fear appeal message. The statement *"You can effectively secure or company network. Most attacks can be prevented by just performing very simple and very easy tasks such as changing default usernames, passwords, and updating firmware. Taking these basic security precautions takes only seconds. No effort is needed. With a click or a tap, you can update firmware and software"* provides the reader with measures to improve network security. For each security fear appeal message, we measure the logos, pathos, and ethos appeals as a manipulation check. We expect that the logos measure is going to be statistically higher for the fear appeal message that uses logical statement. Similarly, pathos and ethos measures are expected to be statistically higher for fear appeal message with emotional statements and credibility statements respectively.

The two leadership styles are manipulated using scenarios using scripts adapted from the leadership training program developed by Bass and Avolio (1997). The transformational leadership scenario emphasizes on the importance of the vision of group decision process, working together, and importance of questioning assumptions, and being creative. Transactional leadership style scenario emphasizes the specific goals needed to be achieved, desirable outcomes, and the rewards and punishments associated with task completion status. As a manipulation check we measure idealized influence, intellectual stimulation, inspirational motivation, individual consideration, and contingent reward. Transformational leadership is expected to be rated higher for transformational leadership behaviors like idealized influence, intellectual stimulation, inspirational motivation, and individual consideration. Transactional leadership scenario is expected to be rated higher for contingent rewards (Hoyt & Blascovich, 2003). Finally, participants are asked to answer how realistic the scenario was (Barlow et al., 2018; Dabhokar, 1994)).

### 3.3. Pretest and Pilot test

We plan to conduct pretest to assess the experiment stimuli and survey. An expert panel will review the scenario-based survey to check realism, content validity, and face validity. As it is unfeasible to use only one rhetoric appeals, we create message with one dominant appeal but still including other appeals. Then, we will assess if the manipulations for the fear appeal messages yield the expected rhetoric appeals. We plan to recruit 60 participants to test the fear appeal messages. Twenty participants will randomly view fear appeal message with logical statements. Another 20 participants will view fear appeal message with

emotional statements, and the rest of the participants will view fear appeal message with credibility statements. After viewing the messages, we will measure the logos, pathos, and ethos appeals experienced by the participants. Next, we will provide the participants with the scenario for leadership. Transactional leadership scenario is assigned randomly to 30 participants. The rest of the participants will be assigned transformational leadership scenario. Participants are asked to provide their perceptions of transformational leadership behaviors and contingent rewards.

Once the experimental stimuli are validated through pretest, the experiment will be pilot tested by 100 participants to evaluate the item reliability and the experimental procedure.

### 3.4. Construct Measurement

Constructs measures will be adapted from information security literature and is measured on a seven-point Likert-type scale unless otherwise mentioned. Pathos, ethos, and logos of the email messages will be measured using the scales adapted from the persuasive disclosure inventory (Feltham, 1994). Attitude toward information security policy will be measured with a three-item scale by Bulgurcu et al. (2010). To assess intention to comply with the information security policy, the items are adapted from Bulgurcu et al. (2010).

To further explore the effects of rhetoric appeals and leadership on security compliance, we will also measure perceptions of threat susceptibility, threat severity, fear, response efficacy, self-efficacy, response cost, and maladaptive response (Posey et al., 2015). Perceptions of collectivism, power distance, and personal responsibility (Nehme & George, 2022) are also measured. We will also examine the influence of control variables on attitude towards information security policy compliance and intention to comply with information security policy. Gender, age, work experience, education, self-control (Burns et al., 2023; Li et al., 2018), whether the participant was a direct or indirect victim of cyberattacks, and participants level of media exposure to cyberattacks will be included as control variables to make sure there is no other influence than given manipulation. Finally, risk propensity, trust propensity, impulsivity, and psychological ownership is measured to control for individual differences (Nehme & George, 2022).

## 4. Conclusion

This study provides a comprehensive framework for analyzing rhetoric in message and designing effective fear appeal security compliance messages for different leadership styles. We integrate Aristotle's rhetorical theory with fear appeal literature to explain how the three rhetorical appeals (pathos, logos, and ethos) influence the persuading power of fear appeal in messages, specifically in terms of changing individuals' attitudes toward the security policy compliance. Our rhetorical approach allows us to investigate and formulate security messaging strategies for different leadership styles. In particular, we provide important insights into how individuals under different leadership styles respond differently to the three rhetorical appeals using ELM as our theoretical framework.

Our study has several theoretical contributions and managerial contributions. First, our study contributes to the theoretical understanding of the mechanism of security compliance messaging, in particular for the stream of fear appeal. Many researchers in IS view fear as an emotion and heavily focus on identifying its components associated with the notion of fear, such as threat and efficacy. While these studies help us to understand what fear appeal is and what affects it, they do not necessarily provide an in-depth explanation of the mechanism by which the message's rhetoric impacts the components (e.g., threat) of fear appeal. Our study explicates the link between the 'art' of rhetoric in the message and the components of fear appeal by theorizing and testing the influence of each rhetoric appeal (e.g., logos) and the observed effect of fear appeal (e.g., attitude change).

Second, we further extend the fear appeal literature by integrating it with the leadership literature using ELM as the connecting theory. Specifically, we explain how individuals may process the rhetoric in the security messages differently based on their leadership style. We propose that individuals under transactional leadership are more likely to rely on the peripheral cues (peripheral route) when processing security messages, whereas those under transformational leadership are more likely to engage in central route processing. Then, we theorize that fear appeal security compliance messaging based on pathos and ethos will be more effective for organizations led by transactional leadership, while messaging based on logos will be more effective for organizations led by transformational leadership.

Finally, this research adds value to practice by designing security messages based on leadership style within an organization. From an organizational perspective, it is more practical to employ rhetorical appeal that align with their existing leadership style rather than changing the leadership style. Our study provides significant implications for security managers seeking to enhance security compliance in their organizations through messaging.

As part of our future plan, we plan to conduct a controlled lab experiment to test our theorizing and hypotheses.

## References


Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*(2), 339-370.

Ashkanasy, N. M., & Dorris, A. D. (2017). Emotions in the workplace. *Annual Review of Organizational Psychology and Organizational Behavior*, *4*, 67-90.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*, 624-644.

Barbuto, J. E. J. (2005). Motivation and transactional, charismatic, and transformational leadership: A test of antecedents. *Journal of Leadership & Organizational Studies*, *11*(4), 26-40.

Barling, J. (2014). *The science of leadership: Lessons from research for organizational leaders*. Oxford University Press, USA.

Bass, B. M., & Avolio, B. J. (1997). Full range leadership development: Manual for the Multifactor Leadership Questionnaire.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly*, 805-825.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & 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), 837-864.

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of information systems*, *25*(4), 364-390.

Bronstein, J. (2013). Like me! Analyzing the 2012 presidential candidates' Facebook pages. *Online Information Review*, *37*(2), 173-192.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An emperical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*, 523-548.

Burke, K. (1969). *A rhetoric of motives*. Univ of California Press.

Burns, A., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: a middle-range theory of motives and controls for insider computer abuse. *Information Systems Research*, *34*(1), 342-362.

Carton, A. M., Murphy, C., & Clark, J. R. (2014). A (blurry) vision of the future: How leader rhetoric about ultimate goals influences performance. *Academy of Management Journal*, *57*(6), 1544-1570.

Cheung, C. M.-Y., Sia, C.-L., & Kuan, K. K. (2012). Is this review believable? A study of factors affecting the credibility of online consumer reviews from an ELM perspective. *Journal of the Association for Information Systems*, *13*(8), 2.

Chu, H.-L., Deng, Y.-S., & Chuang, M.-C. (2014). Investigating the persuasiveness of e-commerce product pages within a rhetorical perspective. *International Journal of Business and Management*, *9*(4), 31.

Crano, W. D., & Prislin, R. (2008). *Attitudes and attitude change*. Psychology Press.

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.

Donalds, C., & Barclay, C. (2022). Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information Systems*, *31*(1), 58-73.

Feltham, T. S. (1994). Assessing viewer judgement of advertisements and vehicles: scale development and validation. *ACR North American Advances*.

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems*, *20*(11), 2.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44.

Flory, M., & Iglesias, O. (2010). Once upon a time: The role of rhetoric and narratives in management research and practice. *Journal of Organizational Change Management*.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983-988.

Ge, J., & Gretzel, U. (2018). Emoji rhetoric: a social media influencer perspective. *Journal of Marketing Management*, *34*(15-16), 1272-1295.

Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of Management Review*, *29*(4), 653-669.

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, *29*(2), 340-362.

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.

Hartelius, E. J., & Browning, L. D. (2008). The application of rhetorical theory in managerial research: A literature review. *Management Communication Quarterly*, *22*(1), 13-39.

Heracleous, L., & Klaering, L. A. (2014). Charismatic leadership and rhetorical competence: An analysis of Steve Jobs's rhetoric. *Group & Organization Management*, *39*(2), 131-161.

Higgins, C., & Walker, R. (2012). Ethos, logos, pathos: Strategies of persuasion in social/environmental reports. *Accounting Forum, 36*(3), 194-208.

Hoyt, C. L., & Blascovich, J. (2003). Transformational and transactional leadership in virtual and physical environments. *Small Group Research*, *34*(6), 678-715.

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Jensen, U. T., Andersen, L. B., Bro, L. L., Bøllingtoft, A., Eriksen, T. L. M., Holten, A.-L., Jacobsen, C. B., Ladenburg, J., Nielsen, P. A., & Salomonsen, H. H. (2019). Conceptualizing and measuring transformational and transactional leadership. *Administration & Society*, *51*(1), 3-33.

Johnston, A. C., & Warkentin, M. (2010a). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*, 549-566.

Johnston, A. C., & Warkentin, M. (2010b). The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational & End User Computing*, *22*(3), 1-21.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*(2), 245-284.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly*, *39*(1), 113-134.

Jung, D. I., Bass, B. M., & Sosik, J. J. (1995). Bridging leadership and culture: A theoretical consideration of transformational leadership and collectivistic cultures. *Journal of Leadership Studies*, *2*(4), 3-18.

Killingsworth, M. J. (2005). *Appeals in modern rhetoric: An ordinary language approach*. SIU Press.

Li, H., Luo, X. R., Zhang, J., & Sarathy, R. (2018). Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management*, *55*(3), 358-367.

Lyons, J. B., & Schneider, T. R. (2009). The effects of leadership style on stress outcomes. *The Leadership Quarterly*, *20*(5), 737-748.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479.

Murphy, J. J. (1981). *Rhetoric in the Middle Ages: A history of rhetorical theory from Saint Augustine to the Renaissance* (Vol. 277). Univ of California Press.

Nehme, A., & George, J. F. (2022). Approaching IT Security & Avoiding Threats in the Smart Home Context. *Journal of Management Information Systems*, *39*(4), 1184-1214.

Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, *38*(3), 732-764.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An Introduction to Information Security*.

Odumeru, J. A., & Ogbonna, I. G. (2013). Transformational vs. transactional leadership theories: Evidence in literature. *International Review of Management and Business Research*, *2*(2), 355.

Petty, R. E., & Cacioppo, J. T. (1986). *The elaboration likelihood model of persuasion*. Springer.

Petty, R. E., Fabrigar, L. R., & Wegener, D. T. (2003). Emotional factors in attitudes and persuasion. In R. J. Davidson, K. R. Scherer, & H. H. Goldsmith (Eds.), *Handbook of affective sciences* (pp. 752-772).

Portolano, M., & Evans, R. B. (2005). The experimental psychology of attitude change and the tradition of classical rhetoric. *The American Journal of Psychology*, *118*(1), 123-140.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*, 93-114.

Rosenthal, P. I. (1971). Specificity, verifiability, and message credibility. *Quarterly Journal of Speech*, *57*(4), 393-401.

Sarros, J. C., & Santora, J. C. (2001). The transformational-transactional leadership model in practice. *Leadership & Organization Development Journal*, *22*(8), 383-394.

Schein, E. H. (2004). *Organizational culture and leadership* (3 ed.). John Wiley & Sons.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.

Swanson, M., Hash, J., & Bowen, P. (2006). *Guide for Developing Security Plans for Federal Information Systems*. NIST.

Tam, K. Y., & Ho, S. Y. (2005). Web personalization as a persuasion strategy: An elaboration likelihood model perspective. *Information Systems Research*, *16*(3), 271-291.

Torres, C. I., & Crossler, R. E. (2019). Rhetorical appeals and legitimacy perceptions: How to induce information security policy compliance. *WISP 2019 Proceedings*. 8.

Van Kleef, G. A., Van den Berg, H., & Heerdink, M. W. (2015). The persuasive power of emotions: Effects of emotional expressions on attitude formation and change. *Journal of Applied Psychology*, *100*(4), 1124-1142.

Varpio, L. (2018). Using rhetorical appeals to credibility, logic, and emotions to increase your persuasiveness. *Perspectives on Medical Education*, *7*(3), 207-210.

Weizman, E., & Dascal, M. (1991). On clues and cues: Strategies of text-understanding.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*, 329-349.