12-15-2019

# Rhetorical appeals and legitimacy perceptions: How to induce information security policy compliance

Carlos Ivan Torres
*Washington State University*, carlos.torres@wsu.edu

Robert Ernest Crossler
*Washington State University*

# RHETORICAL APPEALS AND LEGITIMACY PERCEPTIONS: HOW TO INDUCE INFORMATION SECURITY POLICY COMPLIANCE

**Carlos Ivan Torres**[1]
Carson College of Business, Washington State University,
Pullman, Wa, USA

**Robert Ernest Crossler**
Carson College of Business, Washington State University,
Pullman, Wa, USA

## ABSTRACT

This paper intends to extend Protection Motivation Theory (one of the leading theories in Information Security research) based on innovation diffusion and institutional legitimacy theories. We postulate that legitimacy, in which fear is only a partial representation, is a more comprehensive antecedent to intention to comply with security policies. We argue the use of ethos, pathos, and logos appeals to complement the fear rhetoric traditionally present in information security research to elicit legitimacy judgments and indirectly intention to comply. We propose an experiment in which by manipulating the rhetorical elements of the communication, we can study its impact on legitimacy and ultimately intention to abide by the security policy.

Keywords: PMT, legitimacy judgments, rhetorical triangle, innovation diffusion, legitimacy, information security, information security policy compliance.

## INTRODUCTION

In spite of extant theorization efforts in information security (infosec) policy compliance, organizations are still struggling to enforce secure behaviors. In 2018 60% of the almost 1,200 C-level IT executives and infosec managers worldwide surveyed by Ernst & Young expressed that employee's careless practices are the leading infosec culprit (EY 2018). As a result employees' lack of knowledge or careless behavior has become the primary risk they believe they face and is currently at the highest level of concern as compared to the last five years (EY 2018).

IS scholars have theorized about the potential reasons for lack of compliance with infosec policies in an attempt to explain and prevent cybercrime (e.g. Bulgurcu et al. 2010; Johnston and

[1] Corresponding author. carlos.torres@wsu.edu

Warkentin 2010; Siponen and Vance 2010). Prior studies in infosec policy compliance focus on fear (e.g. Boss et al. 2015; Johnston et al. 2015; Moody et al. 2018) and other complementary structures and constructs such as habit, coping mechanisms, or neutralization techniques.

Even though the theories mentioned above suggest the use of fear to promote acceptance of infosec policies as a good strategy, organizations still struggle on the enforcement of security policies. This makes the study of new and different alternatives to elicit security behaviors a relevant topic of research as suggested by Wall and Buche (2017). In this project, we argue that a lack of legitimacy perceptions among users regarding the implemented policies maybe the underlying reason for the apparent lack of effectiveness of information security policies. Given this argument we study possible ways to increase legitimacy perceptions of infosec policies.

Considering that systematic investigation regarding the legitimacy of infosec policies from the user perspective has been mainly absent in the central and rich infosec policy compliance literature (few exemptions e.g., Hsu et al. 2015; Kam et al. 2013; Son 2011), this opens a research opportunity encompassed in our overarching research question: *What legitimizes an information security policy in the eyes of the user?*

The phenomenon under study requires a relevant and applicable solution to the problem of enforcing secure behaviors; our proposed research methodology will also address a more in-detail research question: *How can an organization induce legitimacy perceptions to increase infosec policy compliance?*

By drawing on organizational theories of legitimacy judgments (Tost 2011) and innovation diffusion (Green Jr 2004), we incorporate a new legitimacy construct and modify previous fear-based Protection Motivation Theory (PMT) (Boss et al. 2015) characterizing research in this field of knowledge. Our study brings a new contextualized and more comprehensive concept of rhetoric as a means to create legitimacy into the infosec field as a driver of intention to comply with the policy.

The first section of this paper discusses the theoretical background on legitimacy and innovation diffusion, as well as the concepts of fear and the infosec policy compliance literature. The second part describes our proposed research model. We finally include our proposed research method. Future versions of this paper will expand on data analysis, summarization of findings, and discussion of the results. Limitations, implications for practice, and suggestions for future research will be included in future versions as well.

## THEORETICAL BACKGROUND

### Legitimacy

Legitimacy is a commonly used construct in organizational research. Kelley and Thibaut (1959) claim that in order to have compliance with regulations and policies, the power structure must be legitimate. They explain that only in the presence of legitimacy will a person conform to the norm or rule rather than to their personal interest.

Institutional theory argues that to achieve their goals, organizations require a control system with different mechanisms, such as rewards and sanctions. Individuals are motivated to perform and achieve such goals and comply with norms, regulations, and superior orders through that system. Furthermore, it is accepted that control is only possible if power/authority structures are created and solidified in organizations (Cooren and Robichaud 2013).

Suchman (1995) defines legitimacy as the acts of the organization being appropriate and bounded by the set of social norms and beliefs established in the organization. Three types of legitimacy are required to consolidate general legitimacy: pragmatic, moral, and cognitive. Pragmatic and moral legitimacy is induced by discussion and argumentations, while cognitive legitimacy is "taken by granted" which means institutions deem the latter as the ultimate stage of legitimacy (Suchman 1995).

Institutional theorists have defined different type of dimensions but fundamentally agreed on four types of legitimacy: pragmatic, moral, cultural-cognitive, regulative. Legitimacy is thoroughly identified by Suchman's work, the introduction of regulatory legitimacy (Greenwood et al. 2002) and refinement to the concept of cognitive legitimacy to include cultural aspects (Scott 2013). According to Deephouse et al. (2017), the four dimensions of legitimacy are a conceptual definition, but due to overlapping between them, they are not entirely separable empirical phenomena.

Pragmatic legitimacy is a person's self-interest calculation. Moral legitimacy puts others above personal interest thus motivating the public benefit. Cognitive legitimacy argues the necessity of the regulation and lack of other options (Barrett et al. 2013), Scott complemented this definition by including shared understanding (Deephouse et al. 2017). Regulative legitimacy is the legitimacy obtained from the law or collective regulation (Tost 2011).

Tost (2011) argues that to form a legitimate judgment, the person makes instrumental, moral, and relational evaluations. Immediately after the new judgment takes place, this

legitimacy judgment leads to intention to comply or reactance to it. When the legitimacy judgment has been already formed, instrumental, moral and relational evaluations create legitimacy, which in turn leads to intention to behave (Tost 2011).

## Innovation diffusion

Some of the aforementioned concepts have been used in IS research, particularly in IT governance research. Barrett et al. (2013) introduced the types of legitimacy in the diffusion of managerial practices and the use of rhetoric justifications (communication) from managers to persuade new practices in organizations (Green Jr 2004). Constantinides and Barrett (2014) considered legitimacy as the route organizations take when trying to gain control of a particular IT innovation diffusion and considered rhetorical appeals the instrument to guide the innovation diffusion process.

In regard to rhetorical appeals, since Aristotle, rhetoric has been associated with reasoned argumentation. Even though time has passed since Aristotle, the rhetorical triangle still stands as an effective motivator; studies demonstrate that rational discussions based on pure demonstrative arguments are not effective, and to be convincing and compelling, the argumentation needs to include all rhetorical triangle elements (O'neill 1998).

Green Jr (2004) argues that there have been three main types of rhetorical justification tied to the legitimacy types sought by the managers: "Pathos justifications impact emotions and are likely to elicit powerful yet unsustainable social action... Logos appeals affect the logical part of the mind; they tend to elicit methodical calculation of means and ends to achieve efficiency or effectiveness. Ethos justifications impact moral or ethical sensibilities" (Green Jr 2004, p. 659). Green Jr. also argued that a sequence of justifications starting with pathos and logos produce pragmatic legitimacy while ethos would generate moral legitimacy. He also states that the presence of both pragmatic and moral justifications is required to create cognitive legitimacy (Green Jr 2004).

Figure 1 synthesizes the main concepts which inform our proposed contribution and research model. The rhetorical justifications of innovation diffusion, together with the dimensions of legitimacy, suggest that the appropriation of a security policy can be achieved by the use of the different types of rhetoric in reasoned argumentation.

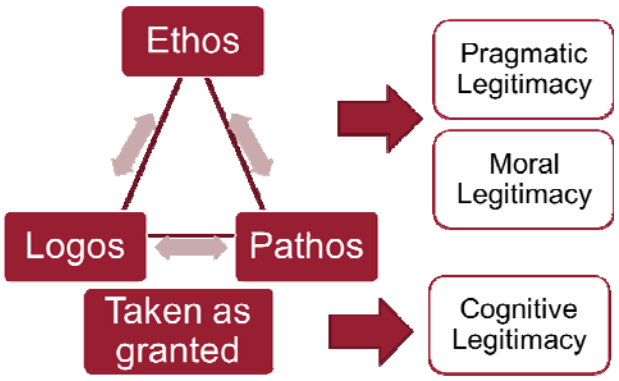


**Figure 1.** Rhetorical triangle and institutional legitimacy

**Legitimacy, Fear, and PMT in InfoSec Research**

At the same time when IT diffusion scholars were analyzing rhetoric and its relation to legitimacy, Son (2011) introduced legitimacy to infosec policy compliance, when explaining that intrinsic motivators are better predictors of compliance than traditional extrinsic motivators.

Kam et al. (2013) used legitimacy concepts as motivators of university implementations of different security policies. They demonstrated that external factors are legitimizers of organizational decisions regarding implemented policies. Kam et al. (2013) observe the phenomenon from the university perspective and its relations with the external world (i.e., how the university seeks legitimacy from external stakeholders). Even though our study draws on similar concepts of legitimacy as the ones mentioned above, we analyze it not from the organizational but individual perspective of how the institution legitimizes its policies and decissions towards the users of university's IT systems.

We had previously mentioned that infosec policy compliance theories have evolved around the concept of fear of a specific cybersecurity threat; fear is defined as a negative emotion evoked by a perceived threat, which regardless of being real or not, is considered to be harmful and pertinent, thus stimulating a sense of protection in the subject (Witte 1992).

Boss et al. (2015) theorized that intention to comply with the security policy is a factor of the threat appraisal, the fear of being attacked, together with the coping appraisal. In their work extending PMT, they include and emphasize the role of fear as a central construct to promote secure behaviors. Johnston et al. (2015) expanded the concept of fear appeal, concluding that not only fear of cybersecurity threat but also fear of a sanction for not complying to the policy

should be included in the communication strategy. Johnston et al. (2015) is a good example of how much of the infosec research has fear at the center of the theorization process.

PMT is a very mature theory, and it is also a parsimonious theoretical frame that we can modify by including legitimacy concepts to complement the fear-only rhetoric which has driven the infosec policy compliance research.

## RESEARCH MODEL

Figure 2 is a diagram of our research model, created to align infosec policy compliance with institutional theories. We aim to modify the full PMT nomology (Boss et al. 2015) to complement the fear-rhetoric, which has driven the infosec models to induce compliance in organizations.

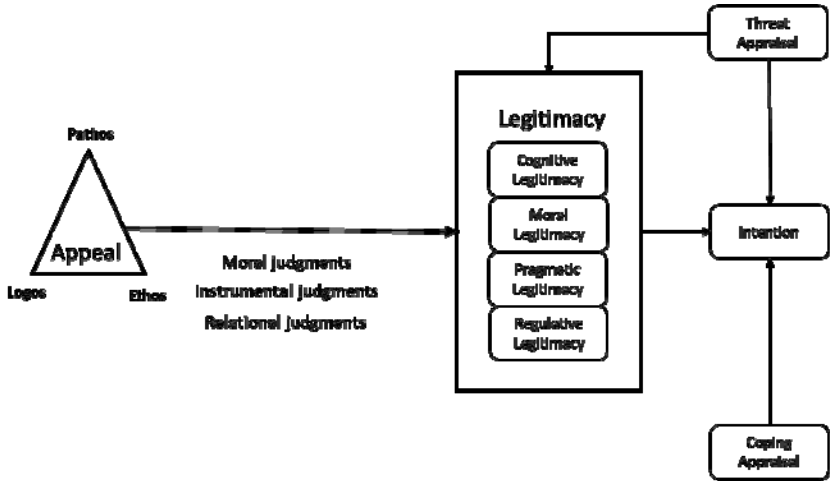


**Figure 2:** Research Model

We posit that legitimacy can be included in the current PMT nomological representation (Boss et al. 2015) since we can replace fear by legitimacy. We argue that fear appeals cater to only one of the dimensions of legitimacy, while the four types of legitimacy are required to be salient when an individual decides to comply with the security policy.

We will consider legitimacy as a formative construct, fully encompassed by the four dimensions of legitimacy (i.e., pragmatic, moral, cognitive-cultural, regulative); this in accord to different studies that theorize that one cannot be present without the other, or that there is an overlapping between the various dimensions that ultimately generate only one legitimacy. The different argumentations (Deephouse et al. 2017; Green Jr 2004; Suchman 1995; Tost 2011) suggest the perhaps a better option for the representation of the legitimacy construct would be to model it as a formative and not a traditional reflective construct.

Rational argumentation using rhetorical appeals spark the relational, moral, and instrumental judgments process in the individual (Tost 2011). Those judgments are the mental process through which the person analyzes and forms the complete legitimacy assessment of the policy. The judgment, in turn, produces the final result of secure behavior.

Different combinations of rhetorical appeals will induce different legitimacy judgments and a different level of legitimacy perception of an infosec policy. As suggested in the literature, fear of the threat or fear of the consequences for nom-compliance (Johnston and Warkentin 2010; Johnston et al. 2015) are a powerful pathos appeal (Green Jr 2004). However, the motivator produces results for as long as the feeling about the threat is present. Persuading moral evaluations requires long and conscious judgments (Tost 2011); thus, ethos justifications are necessary. For instrumental assessments (Tost 2011), logos justifications are the best possible generators of such judgment which produces pragmatic legitimacy.

We argue that in the case of infosec policies a communication following the rhetorical path proposed by Green Jr (2004) starting with an emotional –pathos- appeal (it can be a fear appeal), followed by an argumentative –logos – appeal, including a valid moral –ethos- appeal, will cause people to internalize the legitimacy of the policy thus creating the right environment for policy adoption.

*H1: A combination of pathos, ethos, logos appeals will produce the highest legitimacy score independent of its threat appraisal.*

The combination of rhetorical appeals (Green Jr 2004) seems to offer a successful way for infosec policy implementation compliance since not all appeals work the same for everyone, but by having different communication styles, there is an opportunity that people with different characteristics will judge the policy as legitimate. Users' interpretations of the benefits vs. the inconveniences of the policy exemplify the legitimacy induced by combined appeals (Barrett et al. 2013)

H2: *A combination of two of the three rhetorical (pathos, ethos, logos) appeals will generate a higher legitimacy sense, than communication with only one of the appeals, independent of its threat appraisal*

Tost (2011) accepts that all dimensions of legitimacy judgments comprise general legitimacy. We hypothesize legitimacy to be high when induced through a complete rhetorical appeal in which each of the three rhetorical appeals interacts in order to induce general

legitimacy (Barrett et al. 2013; Green Jr 2004); this, will in turn produce higher intentions to comply with the security policy.

*H3: High levels of perceived legitimacy will produce a higher intention to comply with the infosec policy, independent of threat and coping appraisal.*

## RESEARCH METHODOLOGY PROPOSAL

To understand the legitimacy of infosec policies, we plan to use a factorial survey experiment. This method allows for flexibility and the exploration of various combinations of the suggested manipulations. This methodology has been used by Vance et al. (2015) and Lowry et al. (2017).

We intend to experiment within a university setting. A university is an ideal choice to test alternative methods to induce security policy compliance considering its environment where decisions are debated, and knowledge creation is the raison d'etre. We will conduct the experiment in an R1 University (very high research activity) that recently went through a new password policy adopting a two-factor authentication system. Communication strategy of the IT department was mainly based on the mandatoriness of the process (Boss et al. 2009).

In our experiment, we will expose participants to a communication regarding the adoption of a new password policy in the organization. The different communications will include various combinations of rhetoric appeals (ethos, logos, pathos), and we plan to measure their intention to comply, as well as legitimacy perception. We expect to create manipulations for ethos, pathos and logos elements of the appeals. Each of these manipulations could have multiple levels affecting different judgments (moral, instrumental, and relational).

Once the communication is created with its different combinations of pathos, logos, and ethos appeals, we will have a panel of experts (doctoral students in English majoring in rhetoric), evaluate the presence of the elements of the rhetorical triangle. We will make changes and adaptations according to the panel suggestions. Do so will help to ensure the presence of the different rhetorical elements in the communications designed for the experiment.

We will have one control group with the same communication style received in recent password manager change (based on mandatoriness). We will expose five groups to different combinations and levels of rhetorical appeals. We will asses the different concepts through an instrument with measures of the primary constructs of the proposed research model.

| | Pathos | Ethos | Logos |
|---|---|---|---|
| Group 1 | High | Not present | Low |
| Group 2 | Not present | Low | Low |
| Group 3 | High | High | Not present |
| Group 4 | High | High | High |
| Group 5 | Fear only. | Not present | Not present |

**Table 1: Rethorical** Appeals Experimental Design

We will adapt the measures from the literature: General legitimacy will be adjusted from the management literature (Tyler and Blader 2005). For threat appraisal and coping appraisal, we will also adapt previous items from Boss et al. (2015), Intention to comply will be based in Piquero and Piquero (2006).

After pretest, the complete instrument will be pilot tested. Cronbach's Alpha scores will be used to assess the psychometric properties of the scales, item loadings, and internal consistency reliability (ICRs). Also, different techniques will be used to control from common method bias. We will conduct a preliminary analysis, and possible modifications will be made to the instrument before collecting data from students, staff, and faculty at the University.

## REFERENCES

Barrett, M., Heracleous, L., and Walsham, G. 2013. "A Rhetorical Approach to It Diffusion: Reconceptualizing the Ideology-Framing Relationship in Computerization Movements," *MIS Quarterly* (37:1), pp. 201-220.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and 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), pp. 837-864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

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

Constantinides, P., and Barrett, M. 2014. "Information Infrastructure Development and Governance as Collective Action," *Information Systems Research* (26:1), pp. 40-56.

Cooren, F., and Robichaud, D. 2013. *Organization and Organizing*.

Deephouse, D. L., Bundy, J., Tost, L. P., and Suchman, M. C. 2017. "Organizational Legitimacy: Six Key Questions," *The SAGE Handbook of Organizational Institutionalism*), pp. 27-54.

EY. 2018. "Cybersecurity Regained: Preparing to Face Cyber Attacks. 20th Global Information Security Survey 2017–18." Retrieved November, 2018, from

https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf

Green Jr, S. E. 2004. "A Rhetorical Theory of Diffusion," *Academy of Management Review* (29:4), pp. 653-669.

Greenwood, R., Suddaby, R., and Hinings, C. R. 2002. "Theorizing Change: The Role of Professional Associations in the Transformation of Institutionalized Fields," *Academy of Management Journal* (45:1), pp. 58-80.

Hsu, C., Lin, Y.-T., and Wang, T. 2015. "A Legitimacy Challenge of a Cross-Cultural Interorganizational Information System," *European Journal of Information Systems* (24:3), pp. 278-294.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kam, H.-J., Katerattanakul, P., Gogolin, G., and Hong, S. 2013. "Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective," *PACIS*, p. 106.

Kelley, H. H., and Thibaut, J. W. 1959. *The Social Psychology of Groups*. New York: New York, Wiley.

Lowry, P. B., Moody, G. D., and Chatterjee, S. 2017. "Using It Design to Prevent Cyberbullying," *Journal of management information systems* (34:3), pp. 863-901.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285-311.

O'neill, J. 1998. "Rhetoric, Science, and Philosophy," *Philosophy of the Social Sciences* (28:2), pp. 205-225.

Piquero, N. L., and Piquero, A. R. 2006. "Control Balance and Exploitative Corporate Crime," *Criminology* (44:2), pp. 397-430.

Scott, W. R. 2013. *Institutions and Organizations: Ideas, Interests, and Identities*. Sage Publications.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Son, J.-Y. 2011. "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow Is Security Policies," *Information & Management* (48:7), pp. 296-302.

Suchman, M. C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *The Academy of Management Review* (20:3), pp. 571-610.

Tost, L. P. 2011. "An Integrative Model of Legitimacy Judgments," *Academy of Management Review* (36:4), pp. 686-710.

Tyler, T. R., and Blader, S. L. 2005. "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," *Academy of Management Journal* (48:6), pp. 1143-1158.

Vance, A., Lowry, P. B., and Eggett, D. L. 2015. "Increasing Accountability through the User Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *Mis Quarterly* (39:2), pp. 345-366.

Wall, J. D., and Buche, M. W. 2017. "To Fear or Not to Fear? A Critical Review and Analysis of Fear Appeals in the Information Security Context," *CAIS* (41), p. 13.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communications Monographs* (59:4), pp. 329-349.