2021

# An Empirical Investigation of the Influence of Organizational Virtues on Information Technology Security Policy Compliance

Dora Chatterjee
*Coral Academy of Science, Las Vegas*, sutirthadora@gmail.com

Shuktika Chatterjee
*University of Nevada, Las Vegas*, shuktika.chatterjee@unlv.edu

Sutirtha Chatterjee
*University of Nevada, Las Vegas*, sutirtha.chatterjee@unlv.edu

## Recommended Citation

Chatterjee, Dora; Chatterjee, Shuktika; and Chatterjee, Sutirtha, "An Empirical Investigation of the Influence of Organizational Virtues on Information Technology Security Policy Compliance" (2021). *ACIS 2021 Proceedings*. 2.
https://aisel.aisnet.org/acis2021/2

# An Empirical Investigation of the Influence of Organizational Virtues on Information Technology Security Policy Compliance

## Full research paper

**Dora Chatterjee**[1]
Coral Academy of Science, Las Vegas
Henderson, NV 89052
USA
Email: sutirthadora@gmail.com

**Shuktika Chatterjee**
School of Public Policy and Leadership
University of Nevada, Las Vegas
Las Vegas, NV 89154
USA
Email: shuktika.chatterjee@unlv.edu

**Sutirtha Chatterjee**
Lee Business School
University of Nevada, Las Vegas
Las Vegas, NV 89154
USA
Email: sutirtha.chatterjee@unlv.edu

## Abstract

While studies have proposed multiple factors that influence information technology (IT) security policy compliance, this research tries to understand this phenomenon from an alternate perspective of organizational ethics. Drawing upon the theory of virtue ethics in philosophy, we conceptualize how organizational virtues can create a positive impact on IT security policy compliance in organizations. Our theory considers four cardinal organizational virtues: wisdom, justice, courage, and temperance. We propose that an organization that develops, practices, and implements these virtues achieves greater compliance with IT security policies. An empirical study conducted with managers in public organizations provide support for our theory. Ultimately, our work promotes a novel, virtue ethics-based perspective to better understand and address the crucial challenge of achieving IT security policy compliance.

**Keywords**: Organizational virtues, IT security, policy, compliance, public organizations.

[1] Authors contributed equally and are listed in alphabetical order.

# 1 Introduction and Motivation

This paper investigates how organizational virtues (central to defining the ethical nature of an organization) can influence information technology (IT) security policy compliance in organizations. Security is one of the major challenges in today's organizations. Organizations store and access sensitive data, which are potentially vulnerable to security threats - therefore, organizations today design IT security policies which they expect the employees to comply with (Cram et al. 2017). However, the success of instituted IT security policies in an organization is largely dependent upon the compliance achieved with those IT security policies (D'Arcy and Lowry 2019).

Critically, it has been observed that compliance with IT security policies is challenging to achieve (D'Arcy and Lowry 2019) and research continues to be devoted to achieve a better understanding of this phenomenon (Cram et al. 2019). Existing research often tries to unearth factors that can lead to increased IT security policy compliance (D'Arcy and Greene 2014). However, while there is work on how organizations can improve IT security policy compliance, a consistent omission is a consideration of organizational virtuous characteristics that can influence such compliance. In fact, a recent meta-analysis of IT security compliance research (Cram et al. 2019) reveals no consideration of organizational virtues in the IT security policy compliance literature.

We contend that the omission of virtue ethics from research on IT security policy compliance creates gaps in our understanding of this phenomenon. To illustrate our point, we present a summary review of the major theories used in the IT security policy compliance literature in the *Appendix*. A look at the *Appendix* allows us to infer that, while multiple theories have been used to study IT security policy compliance, these theories have certain limitations which a focus on virtues can help address (please see the *Appendix*). Even beyond what is discussed in the *Appendix*, a focus on virtue ethics allows a paradigm shift in our understanding of compliance. In contrast to existing theories, which often focus on extrinsic motivation for compliant action (e.g., rewards or punishments), virtue ethics provides us a way to understand compliance as being fostered through an intrinsic pursuit of excellence (Solomon 2003). By focusing on organizational virtues, we draw upon what organizations "aspire to be when they are at their very best" (Cameron et al. 2004, p. 767), especially when they are pursuing excellence (Weaver 2006). Virtue ethics thus allows us to address the issue of compliance from the ethical perspective of organizational excellence – a departure from prior studies on IT security policy compliance. In fact, it has been shown in the literature that virtues possessed and practiced within an organization lead to desirable outcomes like innovation, employee satisfaction, productivity, and profits (Caza et al. 2004). It has also been observed that ethical organizations are more successful in the long run than organizations that are not (Hosmer 1996).

Clearly, a research gap has emerged in the IT security policy compliance literature due to the non-leveraging of virtue ethics. Addressing this research gap, we draw upon virtue ethics to study IT security policy compliance. The major premise of this research is that an organization that promotes and practices certain virtuous characteristics will achieve higher degree of compliance with IT security policies. Virtues at the organizational level can be used to understand the nature of an ethical organization. It has been argued that an ethical/virtuous organization can promote desirable outcomes (Caza et al. 2004). Compliance with organizational IT security policies can be understood to be one such desirable goal/outcome. Formally, therefore, our overall research question can be stated as: ***What is the effect of organizational virtues on IT security policy compliance?***

# 2 Literature Review

## 2.1 IT Security Compliance

IT security is an important consideration in an organization. The aim of IT security is to protect the IT and information assets of an organization, thereby enabling the safe execution of organizational operations (Moody et al. 2018). IT security is also a significant challenge for organizations as organizations experience security breaches perpetrated by both insiders and outsiders (Chatterjee et al. 2015b). One of the ways in which organizations address this challenge is by designing and implementing IT security policies. IT security policies "are a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations" (Lowry and Moody 2015, p. 434). The adherence to the IT security policies, which we define as IT security policy compliance, is thus crucial to maintaining an organization's IT, data, and information assets. Achieving better compliance with IT security policies helps an organization to be more secure and work toward its desired outcomes. Otherwise, organizations may lose crucial and sensitive data and may not be able to function properly and even face lawsuits. Therefore, the factors that influence IT security compliance need to be investigated. In this study, we unearth a set of organizational factors, specifically organizational virtues, that impact IT security policy compliance.

## 2.2 Organizational Virtues

Virtues can be defined as follows: They are practiced and developed qualities, "the possession and exercise of which tends to enable us to achieve those goods which are internal to [a community of] practices and the lack of which effectively prevents us from achieving such goods" (MacIntyre 1985, p. 191). The school of virtue ethics was founded by the Greek philosopher Aristotle (Aristotle 1985). In his work, Aristotle discussed ethical attributes of entities which he called virtues, the possession of which allowed an entity to act in a "good" manner. Contemporary works have observed that virtues can be possessed both by individuals and collective entities (Chatterjee et al. 2015a; Chatterjee et al. 2020; Chun 2005). According to Aristotle, there are four major or cardinal virtues: wisdom, courage, justice, and temperance (defined later). It has been argued that these are cardinal virtues because they are the most basic ones, and other virtues can be developed from them (Chatterjee et al. 2015a).

Macintyre (1985) mentions that [virtue] ethics must be "reinterpreted and reformulated according to changing social perceptions of what the "good" means for particular communities at particular times" (MacIntyre 1985, p. 506). This observation can be interpreted to mean that virtues developed and possessed by a social collective guide valuable action within and by that collective (Chatterjee et al. 2020). If achieving IT security policy compliance is considered by organizations to be valuable, then organizational virtues arguably form a powerful set of antecedents influencing this outcome (Smith and Smith 2004). This paper considers Aristotle's cardinal virtues at the organizational level and theorizes that each of these virtues will have a positive influence on IT security policy compliance in an organization.

# 3 Research Model and Hypotheses Development

This section develops the theoretical model and the propositions. In each sub-section, the specific organizational virtue is discussed, and it is argued as to why that virtue will influence IT security policy compliance. The entire model is shown in Figure 1.

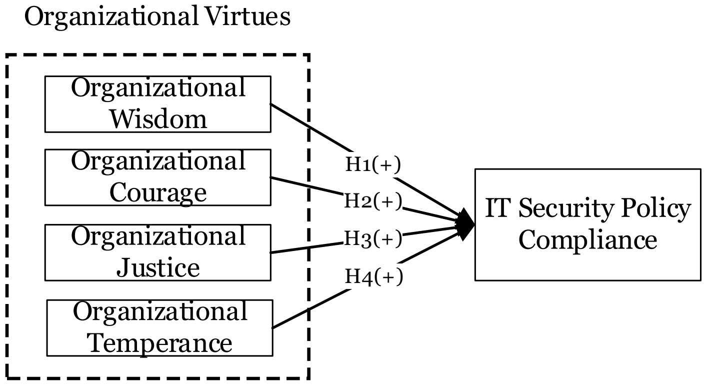

***Figure 1. The Theoretical Model***

## 3.1 Organizational Wisdom and IT Security Policy Compliance

Organizational wisdom is defined as "the judgement, selection and use of specific knowledge for a specific context" (Bierly et al. 2000, p. 597). The choice and application of appropriate knowledge, formed through an integration of individual knowledge through organizational social processes is what develops organizational wisdom (Spiller et al. 2011). Ultimately, organizational wisdom collects, transfers, integrates, and amplifies individual wisdom through institutional mechanisms to emerge as a defining and practiced virtuous characteristic of an organization (Kessler 2006).

A major criterion of a wise organization is sincerity (Seligman et al. 2005). Sincere organizations tend to care more for their employees thus creating an organization with higher levels of collaboration between workers (ibid). An organization which is sincere will encourage organizational employees to be sincere to organizational policies and take them seriously (Sahoo et al. 2021). Given that security threats to organizations are real, an organization with a sincere set of employees will take precautions to avoid security threats by instituting proper policies. Further, the employees of the organization will be internally motivated to adhere to those policies because of the positive relationship between the organization and the employees (Caza and Caza 2008). A sincere organization consists of trustworthy leaders who establish reliable relationships with their employees who in turn dedicate themselves to the organization. Thus, those employees engage in compliance with organizational policies. Combining the arguments presented in this section, it can be hypothesized:

H1. *Organizational wisdom will positively influence IT security policy compliance.*

## 3.2 Organizational Courage and IT Security Policy Compliance

A courageous organization means that the organization is smart and willing to accept challenges and risks of failure as to achieve organizational goals (Chatterjee et al. 2020). A courageous organization is persistent, zestful, and goal oriented (Chun 2005; Peterson and Seligman 2004; Sekera et al. 2009). These organizational characteristics, which are subsumed by courage, have important implications for IT security policy compliance. For example, courage plays a significant role in organizational learning due to the courageous entity being zestful and persistent (Chun 2005). Organizational learning is crucial to formulating new IT security policies and practices (Schneider et al. 2012). These policies and practices can be developed only when the organization extends its knowledge base, and this is largely possible by a courageous organization that can act “mindfully and appropriately despite the possible negative consequences” (Kilmann et al. 2013, p. 22). Organizational IT security policies can often challenge the existing organizational work practices and it is only a courageous organization that can formulate innovative organizational policies to address persisting organizational problems (Koerner 2014), such as those related to IT security. Developing and following new policies requires intentional and calculated risk taking (Chatterjee et al. 2020; Koerner 2014) and thus organizations that are courageous are willing to support their employees in their following of new policies and practices.

New IT security policies often challenge organizational members by either forcing them to acquire new knowledge or unlearn their existing ways of work (Li et al. 2020). A courageous organization encourages its members to be brave enough to comply to new IT security policies. Often, IT security policies can create issues if not implemented properly, and these problems are not knowable beforehand (Herath and Rao 2009). However, if the organizational employees are brave enough to accept this new policy, despite the foreseeable challenges, then it is likely they will be in adherence with it. Furthermore, they will also be persistent in their compliance, as persistence is also a critical characteristic of courage (Siponen et al. 2014).

There is also another reason why we argue that organizational courage has a positive influence on IT security policy compliance. Courage, as a virtue, is considered as being a mean between rashness and cowardice (Young 1996). Interpreting this to our context of compliance, we can infer that a rash individual can flout existing IT security policies and thus be noncompliant with existing organizational policies. Again, cowardice will not allow a person to use IT systems in an organization in a meaningful way to serve the organization. In contrast to rashness and cowardice, in a courageous organization, employees will use IT systems mindfully, while also making sure that security policies guiding the use of those systems should be obeyed. Courage involves decisive acting in the face of challenges, while also being cognizant that the actions should not be foolhardy or dangerous (Koerner 2014).

In sum, an organization that is courageous instils decisive action in its employees, while also ensuring that they are aware that this decisive action should be defensible and well thought-out. In the context of using IT systems, as policies of organizations guide the secure use of such systems, employees of a courageous organization will be more prone to use the IT systems for their work, while at the same time keeping in mind that the policies guiding the secure use of these systems should be complied with. Combining the above arguments, it can be posited that a high level of organizational courage will ensure a high level of IT security policy compliance. Therefore, it can be hypothesized:

H2. *Organizational courage will positively influence IT security policy compliance.*

## 3.3 Organizational Justice and IT Security Policy Compliance

Organizational justice is concerned with fairness in decision-making and allocation of resources employees (Colquitt et al. 2001; Greenberg 1990). Fairness has an intricate relationship with compliance of organizational policies. This is because organizational employees are often in explicit and implicit organizational contracts (Feld and Frey 2007; Tyler 2006) and if they are treated well by their organization then there is a greater likelihood that they will obey the organizational policies even if it comes as a personal cost to them (in terms of time, effort, learning difficulty etc.)(Han et al. 2017).

In fact, an organization that follows fairness in various aspects of organizational life, will also develop IT security policies that upload this fairness, causing employees to be further obedient to these policies (Bulgurcu et al. 2009). It has been empirically verified that fairness perceptions with regards to the IT security policy lead to greater compliance (Sommestad et al. 2014). It can be contended that an organization that possesses the virtue of justice will exhibit fairness in all its operations, procedures, policies, and communications (Payne et al. 2011).

An organization that has the virtue of justice imbibes responsibility and accountability among its employees (Rupp et al. 2014). Therefore, if employees feel that an organization is just, they also respect the organizational actions in implementing IT security policies. Ultimately, organizational justice influences IT security policy compliance by building social capital with other employees and leaders of the organization which ultimately translates to trust and loyalty amongst employees (Leana III and Van Buren 1999; Turel et al. 2008) – leading to compliance. Hence, we can hypothesize:

H3. *Organizational justice will positively influence IT security policy compliance.*

## 3.4 Organizational Temperance and IT Security Policy Compliance

Temperance is the organization's capacity to be balanced and controlled during its operations (Chatterjee et al. 2015a; Fehr and Gelfand 2012). The key idea of temperance is in balancing continuity and change in organizations is crucial to smooth organizational functioning (Chatterjee et al. 2015a; Huy 2002). The idea of temperance becomes especially useful in IT security contexts. Employees tend to get irritated if they perceive that the organization is being overtly oppressive about implementing its IT security policies. For example, if an organization mandates that its employees change the password to their IT systems every two months, employees may resent it. On the other hand, if the password change requirements are more "reasonable" – such as once in a year – then employees may be more prone to obey it. Again, if policies governing the use of IT systems are felt as being too restrictive, employees may not be motivated to comply with those policies, or worse even avoid the use of the IT systems that need such restrictive policies.

In contrast, if the security policies are perceived as too lax, then employees may not take them seriously. In other words, very restrictive security policies as well as very lax security policies will be detrimental to compliance. However, if the organization is temperate, then it will likely develop policies that can be regarded as more reasonable by its employees. Consequently, they will likely be compliant with those policies. Thus, we can hypothesize:

H4. *Organizational temperance will positively influence IT security policy compliance.*

# 4 Empirical Study

## 4.1 Collecting data via third party firms

An online survey was used for the data collection. To conduct this survey, we recruited a third-party market research firm named *Qualtrics*. There are advantages when using third-party market firms to collect data. Reaching out to high-level organizational employees and convincing them to complete a survey is often difficult for researchers. Using a third-party market research firm allows researchers to address such challenges.

Lowry et al. (2016) observe why the method of data collection by using third-party firms is not only efficacious, but also appropriate. Building upon their observations, use of third-party firms (with an established formal contract which details the data collection process) has been used in recent studies (e.g., Chatterjee et al. 2021). The advantages of this approach include sampling, identification of distorted responses, incentivizing the respondents, and improving data quality as well as generalizability (ibid). We followed the guidelines provided by Lowry et al. and Chatterjee et al. to ensure that our study design was appropriate.

## 4.2 Sample

This study was part of a larger effort investigating IT, virtues, and organizations and was conducted with the help of a third-party market research firm, *Qualtrics*. Our study used a sample of public organizational employees (at the level of manager or above) who were knowledgeable about IT related issues in their organization (checked through screening questions). It has been observed that there are differences between how IT security policies are implemented in public vs. private organizations (Wallace et al. 2011). This is why public organizations have often been the focus of IS security compliance studies (e.g., Doherty and Tajuddin 2018). Furthermore, due to the sensitive community data that public organizations often own, security issues can be more damaging if they occur in public organizations. Again, public organizations, with their immediate focus on community welfare may ascribe more salience to organizational virtues than, say private organizations (van Steden 2020). Therefore, the initial focus was to test this theory on public organizations. Of course, the findings need to be further investigated in private, for-profit organizations.

The contracted sample size was 200 for the study from Qualtrics. We paid Qualtrics US$4000 for the contracted sample of 200. In addition to being managers (or above) in public organizations, and being knowledgeable about IT, the respondents were required to have at least 5 years of experience in the organization. We included screening questions (e.g., whether they were knowledgeable about IT and were managers in their organizations) in our questionnaire to eliminate inappropriate respondents from the sample.

### 4.3 Pilot and Final studies

Qualtrics helped us conduct a pilot study. The pilot size was 22 respondents and consisted of subjects that were eligible for our full study. We analysed the items for reliability and validity to identify any problems. Following some minor changes, the final data collection was launched. The total amount of responses returned in the final data collection was 178 (22 less than our contracted sample size of 200). 94 males responded and 84 females responded to the final study. These 178 responses were used for our empirical analysis.

### 4.4 Measures and Controls

Measures for virtues were adopted from Chatterjee et al. (2015a) and adapted from Wang and Hackett (2016). IT security policy compliance measures were adapted from Herath and Rao (2009) and customized to capture actual compliance behavior. Drawing upon prior literature for the items raised our confidence on their appropriateness. Items were measured on a standard Likert-type 7-point scale (from Strongly Agree to Strongly Disagree). Table 1 shows the measurement items. Our study also included control variables such as respondent age, education level, position at organization, experience, and gender as well as organizational level variables such as size and age.

## 5 Results and Analysis

### 5.1 Measurement Model

Partial least squares (PLS) was used for model testing. PLS is an SEM approach that is particularly useful for exploratory investigations in theory development (Chatterjee et al. 2015b). WarpPLS7.0 was the tool used to conduct the analysis. In PLS assessing the measurement model involves analysing reliability and convergent and discriminant validities (Fornell and Larcker 1981). The composite reliabilities of our four constructs were 0.807 (wisdom), 0.873 (courage), 0.875 (justice), 0.899 (temperance), and 0.907 (IT security policy compliance). These reliabilities are all higher than the recommended threshold, and therefore it can be inferred that our instrument was reliable (Nunnally 1978). Convergent validity can be demonstrated by showing that t-values of the Outer Model Loadings are above 1.96" (Gefen and Straub 2005, p. 97), that is they are significant loadings at the $p<0.05$ level. All the items satisfied this benchmark, thereby demonstrating convergent validity.

Discriminant validity was assessed in two steps. First, we confirmed that the items loaded much higher on their respective constructs than on other constructs. Next, we confirmed that the square root of the average variance extracted (AVE) was substantially higher than the correlation between any latent construct pair. We observed that the loadings of the items on their respective constructs were all higher than the recommended benchmark of 0.7 (Nunnally 1978), with one exception for the second wisdom item, where the loading was 0.65. As this loading was sufficiently close to 0.7, it was retained in the final analysis. The square root of the AVE was also higher than the correlation between the latent variables. In addition, the AVEs were all greater than the recommended benchmark of 0.5 (Fornell and Larcker 1981). The analysis shows that our measurement model is adequate.

| **Items** |
|---|
| **Wisdom:**<br>*Overall, my organization...* |
| ...is wise |
| ...can be labeled as prudent. |

...possesses good judgment.

**Courage:**

*My organization...*

...often makes bold decisions

...is willing to take a chance on a good idea

...takes calculated risks

...occasionally takes big risks

**Justice:**

*My organization...*

...allocates valued resources in a fair manner.

... resolves conflicts in a fair and objective fashion

... respects individual interests and rights when allocating responsibilities

**Temperance:**

*My organization...*

...balances change with stability.

... avoids imbalance between organizational change and stability

... is balanced in its pursuit of both organizational change and stability

**IT Security Policy Compliance:**

Employees in my organization follow organizational IT security policies

Employees in my organization comply with organizational IT security policies in place to protect the organization's information systems.

I am confident that employees in my organization follow organizational IT security policies.

Employees in my organization are compliant with organizational IT security policies

Employees in my organization adhere to organizational IT security policies

***Table 1. Measurement Items***

## 5.2 Structural Model

The structural model testing is shown in Figure 2. The R-squared for the endogenous construct (compliance) was much higher than the recommended benchmark of 10% (Falk and Miller 1992). The variance explained for compliance was 47%. The level of variance explained demonstrates that our model had high predictive power. All the paths were significant, supporting our hypotheses. Temperance had the greatest effect on the dependent variable (compliance) followed by wisdom, justice, and courage.

# 6 Discussion of the Results

The results show strong support for all our four hypotheses. Organizational virtues do have an important and significant positive effect on IT security policy compliance. However, it is also noticeable that the effects of the virtues are different. Wisdom and temperance have the strongest effect on compliance. This is not surprising because wisdom is often considered fundamental to decision-making, and a wise entity acts in a prudent manner. Following established IT security policies is prudent. Again, an organization that does not go overboard with any of its objectives (i.e., practices temperance) can also achieve more compliance, because it does not make excessive demands from its employees. The strong effect of justice (though less than wisdom and temperance) is also understandable, as a fair organization promotes a culture of conformity, thus improving compliance. However, the effect of courage, which is the weakest (though significant), provides an interesting insight. Courage, while being valuable to being decisive and bold, can also foster elements of somewhat rash behaviour. If not checked, courage may become instrumental to defying organizational policies rather than following them. This could be the cause of the relatively muted effect of courage on compliance.

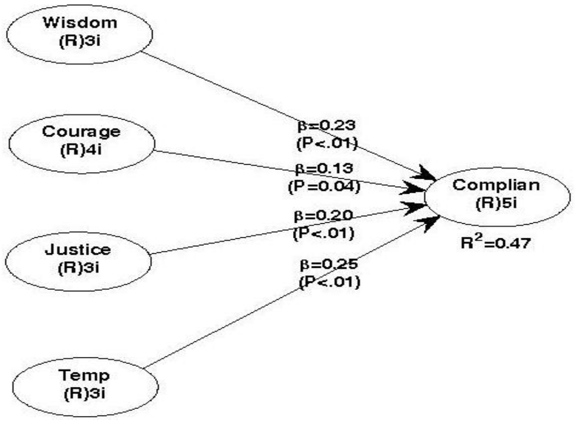

***Figure 2. Structural Model***

# 7 Contributions and Future Research

This paper makes important contributions to the area of IT security policy compliance in organizations. One contribution is that it provides a way to understand IT security policy compliance using the lens of virtue ethics. Virtue ethics is a powerful lens to investigate organizations, but sadly it has been underutilized (van Steden 2020). By proposing and illuminating the key organizational virtues, this research paves the way to understand better the behavioural and organizational aspects of IT security. It has been argued that organizational IT security is most susceptible to the insider threat, that is from its own employees (Warkentin and Willison 2009). Therefore, understanding how the organizational employees can be made more compliant with IT security policies is crucial. The concept of organizational virtues, embraced by the organization, practiced by its leaders, and followed by its employees, provides useful guidance to researchers on how to improve IT security policy compliance.

The second contribution is that virtues themselves are a powerful lens to study organizations. It has been argued that ethicality of current organizations is perhaps best captured by the notion of organizational virtues, which characterize a powerful form of human agency (Chatterjee et al. 2020). Given the myriad issues faced by current organizations, it is imperative that ethical considerations are at the forefront of academic discussion on organizations. Virtue ethics can contribute to this academic discussion.

Like any other study, ours also has its limitations, which can be addressed by future research. For example, our results are applicable to the US context and only to public organizations. It remains to be seen whether our theory holds true for private organizations, as well as other countries/cultures. So, there is a need to empirically test this model in private organizations and in organizations situated in other countries/cultures. Again, while this research focused on only one type of compliance (IT security policies), it can be argued that other forms of compliance may benefit from a discussion on organizational virtues. After all, virtues are argued to be the stimulator of organizational excellence, and compliance with organizational policies can be thought to be one form of such excellence. Therefore, future research can investigate if compliance with other types of organizational policies is similarly influenced by organizational virtues.

To conclude, we hope that this study creates interest amongst academics for studying IT security (and other IS phenomena) through the lens of virtue ethics. Virtue ethics can be a powerful ethical angle to augment our understanding of IS phenomena. Given the increasing discourse on ethics in the IS literature, we are confident that virtue ethics will invoke compelling discussions of alternate and ethical perspectives that will help us better understand how information systems shape businesses and society.

# 8 References

Ajzen, I. "The theory of planned behavior," *Organizational behavior and human decision processes* (50:2) 1991, pp 179-211.

Aristotle *Nicomachean Ethics, trans. Terence Irwin* Hackett, Indianapolis, 1985.

Bagozzi, R. P. "The self-regulation of attitudes, intentions, and behavior," *Social psychology quarterly*) 1992, pp 178-204.

Bierly, P. E., Kessler, E. H., and Christensen, E. W. "Organizational learning, knowledge and wisdom," *Journal of organizational change management*) 2000.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. "Roles of information security awareness and perceived fairness in information security policy compliance," *AMCIS 2009 Proceedings*) 2009, p 419.

Cameron, K. S., Bright, D., and Caza, A. "Exploring the relationships between organizational virtuousness and performance," *American behavioral scientist* (47:6) 2004, pp 766-790.

Caza, A., Barker, B. A., and Cameron, K. S. "Ethics and ethos: The buffering and amplifying effects of ethical behavior and virtuousness," *Journal of Business Ethics* (52:2) 2004, pp 169-178.

Caza, B. B., and Caza, A. "Positive organizational scholarship: A critical theory perspective," *Journal of Management Inquiry* (17:1) 2008, pp 21-33.

Chatterjee, S., D Moody, G., Lowry, P. B., Chakraborty, S., and Hardin, A. "The nonlinear influence of harmonious information technology affordance on organisational innovation," *Information Systems Journal* (31:2) 2021, pp 294-322.

Chatterjee, S., Moody, G., Lowry, P. B., Chakraborty, S., and Hardin, A. "Strategic relevance of organizational virtues enabled by information technology in organizational innovation," *Journal of Management Information Systems* (32:3) 2015a, pp 158-196.

Chatterjee, S., Moody, G., Lowry, P. B., Chakraborty, S., and Hardin, A. "Information Technology and organizational innovation: Harmonious information technology affordance and courage-based actualization," *The Journal of Strategic Information Systems* (29:1), 2020/03/01/ 2020, pp 1-23.

Chatterjee, S., Sarker, S., and Valacich, J. S. "The behavioral roots of information systems security: Exploring key factors related to unethical IT use," *Journal of Management Information Systems* (31:4) 2015b, pp 49-87.

Chun, R. "Ethical character and virtue of organizations: An empirical assessment and strategic implications," *Journal of Business Ethics* (57:3) 2005, pp 269-284.

Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O., and Ng, K. Y. "Justice at the millennium: a meta-analytic review of 25 years of organizational justice research," *Journal of applied psychology* (86:3) 2001, p 425.

Cram, W. A., D'arcy, J., and Proudfoot, J. G. "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance," *MIS Quarterly* (43:2) 2019, pp 525-554.

Cram, W. A., Proudfoot, J. G., and D’arcy, J. "Organizational information security policies: a review and research framework," *European Journal of Information Systems* (26:6) 2017, pp 605-641.

D'Arcy, J., and Greene, G. "Security culture and the employment relationship as drivers of employees’ security compliance," *Information Management & Computer Security* (22:5) 2014, pp 474-489.

D'Arcy, J., and Lowry, P. B. "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study," *Information Systems Journal* (29:1) 2019, pp 43-69.

Doherty, N. F., and Tajuddin, S. T. "Towards a user-centric theory of value-driven information security compliance," *Information Technology & People* (31:2) 2018, pp 348-367.

Falk, R. F., and Miller, N. B. *A Primer for Soft Modeling* University of Akron Press, Akron, OH, 1992.

Fehr, R., and Gelfand, M. "The forgiving organization: A multilevel model of forgiveness at work," *Academy of Management Review* (37:4) 2012, pp 664-688.

Feld, L. P., and Frey, B. S. "Tax compliance as the result of a psychological tax contract: The role of incentives and responsive regulation," *Law & Policy* (29:1) 2007, pp 102-120.

Fornell, C., and Larcker, D. F. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of marketing research* (18:1) 1981, pp 39-50.

Gefen, D., and Straub, D. "A practical guide to factorial validity using PLS-Graph:Tutorial and annotated example," *Communications of the Association for Information Systems* (16) 2005, pp 91-109.

Gibbs, J. P. *Crime, punishment, and deterrence* Elsevier, 1975.

Greenberg, J. "Organizational justice: Yesterday, today, and tomorrow," *Journal of management* (16:2) 1990, pp 399-432.

Han, J., Kim, Y. J., and Kim, H. "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," *Computers & Security* (66), 2017/05/01/ 2017, pp 52-65.

Herath, T., and Rao, H. R. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2) 2009, pp 106-125.

Hosmer, L. T. "RESPONSE TO ‘DO GOOD ETHICS ALWAYS MAKE FOR GOOD BUSINESS?’," *Strategic Management Journal* (17:6), 1996/06/01 1996, pp 501-501.

Huy, Q. N. "Emotional balancing of organizational continuity and radical change: The contribution of middle managers," *Administrative science quarterly* (47:1) 2002, pp 31-69.

Kessler, E. H. "Organizational wisdom: Human, managerial, and strategic implications," *Group & Organization Management* (31:3) 2006, pp 296-299.

Kilmann, R. H., O'Hara, L. A., and Strauss, J. P. "Developing and validating a quantitative measure of organizational courage," in: *Voice and Whistleblowing in Organizations*, Edward Elgar Publishing, 2013.

Koerner, M. M. "Courage as identity work: Accounts of workplace courage," *Academy of Management Journal* (57:1) 2014, pp 63-93.

Kohlberg, L. "Moral stages and moralization," *Moral development and behavior*) 1976, pp 31-53.

Leana III, C. R., and Van Buren, H. J. "Organizational social capital and employment practices," *Academy of management review* (24:3) 1999, pp 538-555.

Li, Y., Pan, T., and Zhang, N. "From hindrance to challenge," *Journal of Enterprise Information Management* (33:1) 2020, pp 191-213.

Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. "“Cargo Cult” science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels," *The Journal of Strategic Information Systems* (25:3) 2016, pp 232-240.

Lowry, P. B., and Moody, G. D. "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies," *Information Systems Journal* (25:5) 2015, pp 433-463.

MacIntyre, A. *After virtue* Notre Dame University Press, Notre Dame, IN, 1985.

Moody, G. D., Siponen, M., and Pahnila, S. "Toward a unified model of information security policy compliance," *MIS quarterly* (42:1) 2018, pp 285-312.

Nunnally, J. *Psychometric Theory, 2nd ed* McGraw-Hill, New York, 1978.

Paternoster, R., and Simpson, S. "Sanction threats and appeals to morality: Testing a rational choice model of corporate crime," *Law and Society Review*) 1996, pp 549-583.

Payne, G. T., Brigham, K. H., Broberg, J. C., Moss, T. W., and Short, J. C. "Organizational virtue orientation and family firms," *Business Ethics Quarterly* (21:2) 2011, pp 257-285.

Peterson, C., and Seligman, M. E. *Character strengths and virtues: A handbook and classification* Oxford University Press, 2004.

Rogers, R. W. "A protection motivation theory of fear appeals and attitude change1," *The journal of psychology* (91:1) 1975, pp 93-114.

Rupp, D. E., Shao, R., Jones, K. S., and Liao, H. "The utility of a multifoci approach to the study of organizational justice: A meta-analytic investigation into the consideration of normative rules, moral accountability, bandwidth-fidelity, and social exchange," *Organizational behavior and human decision processes* (123:2) 2014, pp 159-185.

Sahoo, K. K., Muduli, K. K., Luhach, A. K., and Poonia, R. C. "Pandemic COVID-19: An empirical analysis of impact on Indian higher education system," *Journal of Statistics and Management Systems* (24:2) 2021, pp 341-355.

Schneider, K., Knauss, E., Houmb, S., Islam, S., and Jürjens, J. "Enhancing security requirements engineering by organizational learning," *Requirements Engineering* (17:1) 2012, pp 35-56.

Sekera, L., Bagozzi, R., and Charnigo, R. "Facing ethical challenges in the workplace," *Journal of Business Ethics* (89) 2009, pp 565-579.

Seligman, M. E., Steen, T. A., Park, N., and Peterson, C. "Positive psychology progress: empirical validation of interventions," *American psychologist* (60:5) 2005, p 410.

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

Smith, M. E., and Smith, M. E. S. *Europe's foreign and security policy: the institutionalization of cooperation* Cambridge University Press, 2004.

Solomon, R. C. "Victims of circumstances? A defense of virtue ethics in business," *Business Ethics Quarterly* (13:1) 2003, pp 43-62.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Information Management & Computer Security* (22:1) 2014, pp 42-75.

Spiller, C., Pio, E., Erakovic, L., and Henare, M. "Wise up: Creating organizational wisdom through an ethic of Kaitiakitanga," *Journal of Business Ethics* (104:2) 2011, pp 223-235.

Turel, O., Yuan, Y., and Connelly, C. E. "In justice we trust: predicting user acceptance of e-customer services," *Journal of Management Information Systems* (24:4) 2008, pp 123-151.

Tyler, T. R. *Why people obey the law* Princeton University Press, 2006.

van Steden, R. "Blind spots in public ethics and integrity research: What public administration scholars can learn from Aristotle," *Public Integrity* (22:3) 2020, pp 236-244.

Wallace, L., Lin, H., and Cefaratti, M. A. "Information security and Sarbanes-Oxley compliance: An exploratory study," *Journal of Information Systems* (25:1) 2011, pp 185-211.

Wang, G., and Hackett, R. D. "Conceptualization and Measurement of Virtuous Leadership: Doing Well by Doing Good," *Journal of Business Ethics* (137:2), 2016/08/01 2016, pp 321-345.

Warkentin, M., and Willison, R. "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems* (18:2) 2009, pp 101-105.

Weaver, G. R. "Virtue in organizations: Moral identity as a foundation for moral agency," *Organization studies* (27:3) 2006, pp 341-368.

Witte, K. "Putting the fear back into fear appeals: The extended parallel process model," *Communications Monographs* (59:4) 1992, pp 329-349.

Young, C. M. "The doctrine of the mean," *Topoi* (15:1) 1996, pp 89-99.

# Appendix

**Existing Theories and Appropriateness of Virtue Ethics in IT Security Policy Compliance (developed based upon Moody et al. (2018))**

| **Theory** | **Major concepts of the theory** | **Shortcomings and how Virtue Ethics addresses that** |
|---|---|---|
| Theory of planned behaviour (Ajzen 1991) | This theory explains individual behaviour based upon individual and social characteristics | Does not investigate collective (organizational) behaviour; virtue ethics allows that |
| General deterrence theory and rational choice (Gibbs 1975; Paternoster and Simpson 1996) | This theory explains why individuals can be deterred against committing crimes. Specifically, it observes that individuals calculate the costs of the deterrents and compare them to the perceived benefits of committing a crime. | Does not investigate collective (organizational) behaviour; virtue ethics allows that. |
| Protection motivation theory (Rogers 1975) | This theory explains how people can cope with threats using two appraisal processes. One is the appraisal of the threat and the other one is an appraisal of how the threat can be reduced. | Coping with threats and fear appeals are only a small component of compliance. Virtue ethics subsumes these issues, and considers others, as virtues are multilayered and multidimensional constructs (Chatterjee et al. 2015a). |
| Cognitive moral development (Kohlberg 1976) | This theory proposes that human beings develop through stages of moral reasoning. The stages range from the pre-conventional stage, the conventional stage, and the post-conventional stage. | It does not define any critical characteristics that individuals will have to achieve compliance; in contrast, virtue ethics allows the understanding of key organizational virtues which are often an interaction of germane characteristics and the situation. Cognitive moral development does not allow this interaction. |
| Theory of self-regulation (Bagozzi 1992) | This theory discusses how one can self-manage goals based on thoughts and emotions | Only individual goals are considered; however, in the case of compliance, organizations goal also need to be factored in. Virtue ethics allows this. |
| Extended parallel Processing model (EPPM) (Witte 1992) | How threats and efficacy can be used to predict both protective and reactive responses toward security | Coping with threats and efficacy are only a small component of compliance. Virtue ethics subsumes these issues, and considers others, as virtues are multilayered and multidimensional constructs. |