DEVIANT CLOUD USAGE IN PUBLIC INSTITUTIONS – A MATTER OF PERSONAL INNOVATIVENESS?

Born Friedrich  
*Goethe University*, fborn@wiwi.unifrankfurt.de

Julia Krönung  
*University of Mannheim*, kroenung@bwl.unimannheim.de

Follow this and additional works at: [http://aisel.aisnet.org/ecis2016_rip](http://aisel.aisnet.org/ecis2016_rip)

Recommended Citation

[http://aisel.aisnet.org/ecis2016_rip/19](http://aisel.aisnet.org/ecis2016_rip/19)

This material is brought to you by the ECIS 2016 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in Research-in-Progress Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
DEVIANT CLOUD USAGE IN PUBLIC INSTITUTIONS – A MATTER OF PERSONAL INNOVATIVENESS?

Research in Progress

Born, Friedrich, Goethe University Frankfurt, Frankfurt, Germany, fborn@wiwi.uni-frankfurt.de
Krönung, Julia, University of Mannheim, Mannheim, Germany, kroenung@bwl.uni-mannheim.de

Abstract

The emergence of cloud services offered many benefits for less tech savvy individuals, because it offers easy accessible computing or storage solutions for every customer. The adoption among individuals surpassed the adoption by organizations like businesses or public institutions due the tremendous benefits of cloud services for customers. Due the lacking adoption by public institutions, we see an increasing deviant use of such services in environments, where the IS policy actually prohibits a use of not approved third-party service. Current research has only a basic understanding on what drives the deviant cloud usage within organizations and the apparent influence of personality traits on the usage of Shadow IT has not been evaluated, yet. It is expectable that individuals with an affinity towards IT innovations use information systems before they are approved by organizational IS security policies and not users reluctant towards technology. A granular knowledge of different types of deviant users is helpful in order to develop strategies to address specific mechanisms of justifying violations of IS policies by using not approved cloud services. Our preliminary findings among public officials show that users with a high personal innovativeness are less likely to behave in compliance to the IS security policy.

Keywords: Shadow IT, Public Sector, Personal Innovativeness, Traits.

1 Introduction

The wide adoption of cloud services among individuals is one of the most trending topics of IS practice for several years (Haag & Eckhardt, 2014a). The emergence of cloud services offered many benefits for less tech savvy individuals by offering easy accessible computing or storage solutions for every customer (Zimmermann & Rentrop, 2014). The adoption among individuals surpassed the adoption by organizations like businesses or public institutions due the tremendous benefits of cloud services for customers (Haag, 2015; Walters, 2013). The public sector is also acknowledging the benefits of cloud applications for increasing the productivity of public officials, its potential benefits for increasing inter-organizational connectivity, and for increasing its transparency (Janssen & Joha, 2011). Despite the apparent benefits of cloud services, the adoption of cloud services among public organizations is generally underwhelming (Janssen & Joha, 2011; Polyviou & Pouloudi, 2014). Some of the lacking adoption might be grounded in the lacking legal frameworks for introducing remote cloud applications, security concerns, or simply the generally slow bureaucratic process (Polyviou & Pouloudi, 2014). Where the use of remote cloud applications is not yet adopted or even planed, the IS policy usually prohibits an use of not approved third-party services (Györy, Cleven, Uebernickel, & Brenner, 2012; Haag & Eckhardt, 2014a; Walters, 2013; Zimmermann & Rentrop, 2014). However, not every user and thus public official does comply with the binding IS security policies and we see an increasing deviant use of such services in environments. Individuals might not even violate the policies with
harmful intentions (Alper & Karsh, 2009), but they are nonetheless opening their organizations to potential harm and loss of control over their data (Janssen & Joha, 2011). Notwithstanding the apparent relevance, the deviant usage of cloud computing among organizations received little attention in research. Only Haag (2015) analyzed the determinants of individuals deviant cloud usage within organizations and Haag & Eckhardt (2014b) addressed the influence of different bring your own cloud (BYOC) strategies within businesses.

However, the apparent influence of personality traits on the usage of Shadow IT and general IS usage (Barnett, Pearson, & Pearson, 2015; Devaraj, Easley, & Crant, 2008; McElroy, Hendrickson, & Townsend, 2007) has not been evaluated. It is expectable that individuals with an affinity towards IT innovations engage in using information systems before they are approved by organizational IS security policies and not users reluctant towards technology. The impact of personal dispositions on individuals’ IS usage is widely acknowledged (Devaraj et al., 2008). The personality of an individual and the traits of the personality are partly responsible to how and why individuals behave in specific ways and situations (Ajzen, 2005). Besides general personality traits, multiple studies have shown the influence of IT-specific traits like personal innovativeness in the domain of IT (PIIT) on the usage of IS (Agarwal & Prasad, 1998; Maier, 2012; Venkatesh, Sykes, & Venkatraman, 2013). Surprisingly, the influence of personal dispositions on violations of IS security policies or even general safety violations has been scarcely considered (Alper & Karsh, 2009). We will thus analyze whether personal innovativeness has any predictive power when it comes to not approved adoption and use within public institutions. This objective leads to our research questions:

RQ: Is personal innovativeness in the domain of IT a predictor of deviant cloud use within public institutions?

We expect that our research has the potential to advance our understanding of Shadow IT usage by accounting for IT-specific personality traits of deviant users. A more granular knowledge of different types of deviant users is helpful in order to develop strategies to address specific mechanism of justifying violations of IS policies by using not approved cloud services. We understand cloud services generally as SaaS and thus accordingly as a “software delivery model in which services are installed, assembled and maintained on the systems of the SaaS provider and used by others over the internet” (Janssen & Joha, 2011). Accordingly, our study addresses cases such as violating the IS security policy by using one owns private Dropbox or Google Drive account or cases, where a similar data transport to a remote provider happens. The expected outcome can help understanding the psychological driver of deviant behavior and can help managers with addressing such potentially critical behavior by employing more granular countermeasures.

2 Shadow IT Usage of Cloud Computing

The adoption and use of cloud services is an ongoing topic within IS research (Haag & Eckhardt, 2014a), because it can be a great asset in moving forward an organization. Cloud services are promising for many organizations, because they offer an increase in the efficiency, simplicity, and creativity of services (Venters & Whitley, 2012). Especially the first two appeal not only to managers and public administrations, but also to individual users within those organizations. Individuals can ease their own work by using more efficient and easier to use services instead of the provided tools. However, the usage of not allowed, approved, or even prohibited applications with a non-malicious intent by the customer is understood as shadow IT use (Haag, 2015; Haag & Eckhardt, 2014b; Zimmermann & Rentrop, 2014). The use of shadow IT, especially if this shadow IT is a cloud storage service, is problematic in several ways. The organization, public or private, loses partial or even full control of its data (Walters, 2013). Even if an employee does not have malicious intents and uses cloud services to improve her productivity, the use presents potential hazard for organizations because it cannot control who can access the data or how the cloud service provider treats his own security (Walters, 2013). Based on a recent review of current research on cloud computing, the topics of control, compliance, and security are one of the major future research topics in the area of cloud computing (Haag & Eck-
However, the issue of Shadow IT has been barely scratched in prior research and remains scarce (Haag, 2015; Zimmermann & Rentrop, 2014). The literature on the specific case of Shadow IT use of cloud services is even less extensive and only includes a handful of studies. Zainuddin (2012) explores the problem by examining the organizational conditions in which an adoption of Shadow IT occurs. Haag & Eckhardt (2014b) examine the impact of different bring your own cloud strategies in organizations on their employees perception of risk in using Shadow IT use. Haag (2015) instead analyzed the determinants of individual Shadow IT uses in organization based on an extended TRA with the addition of perceived work norms and organizational identification, which could have been confirmed as determinants of Shadow IT use. Other work on individuals general Shadow IT usage have been almost nonexistent with the exception of Ortbach, Koeffer, Bode, & Niehaves (2013), which looked at the consumerization behavior of individuals with the help of the TPB and Alter (2014), who looked at the way users worked around present solutions.

3 Personality Traits in IS Research

The personality of an individual and the traits of the personality are partly responsible to how and why individuals behave in specific ways and situations (Ajzen, 2005). We understand traits as “dimensions of individual differences in tendencies to show consistent patterns of thought, feelings, and actions” (McCrae & Costa, 2006). Traits are continuous and not dichotomous, meaning that an individual can have more of a trait and thus show more of the associated tendencies, or she can have less of the trait and the tendencies (McCrae & Costa, 2006). Personality traits are also stable over a long period of time as soon as they are formed during the adolescence and young adulthood, albeit they tend to change towards a more social direction with seniority (McCrae & Costa, 2006). It is apparent that traits can determine an individual’s personality as stable dispositions, but the question remains what traits are sufficient to reflect a personality. Personality traits received only little attention in IS research and none in context of Shadow IT usage. However, we will discuss recent findings in general IS research and since our data focuses on the use of Shadow IT within public institutions, we also discuss research on personality traits in the domain of the public sector.

3.1 Traits in General IS Literature

Prior studies on the influence of personality traits in IS research can be categorized into what kind of personality traits where used in their research: Higher-order traits like the big five inventory, narrow traits for specific accounts, or IT-specific traits (Maier, 2012). A handful of studies applied more general trait models to identify the higher-order personality of an individual. Maier, Laumer, Eckhardt, & Weitzel (2012) further supports that dispositions are responsible for indirect effects. Jackson, Yi, & Park (2013) even addressed a complete study to the question whether traits show direct or indirect effects, with the conclusion that most behavioral models like TPB, TAM, and UTAUT are actually moderated by personality traits.

The second stream of narrow or IT-specific traits is similarly small compared to the higher-order traits studies. The most attention received the trait personal innovativeness in IT (PIIT), which was first introduced by Agarwal & Prasad (1998) and captures the general tendency and affinity of an individual towards new technology and IT innovations. The positive impact of PIIT on the adoption of IS has been confirmed several times (Lewis, Agarwal, & Sambamurthy, 2003; Lu, Yao, & Yu, 2005; Thatcher & Perrewe, 2002). Other narrow traits of relevance, which received some attention have been computer playfulness (Agarwal & Prasad, 1998), the negative effect of computer anxiety on the adoption of IS (Thatcher & Perrewe, 2002) and anxiety towards technology on the adoption of IS (Pramataris & Theotokis, 2009). However, every study either analyzed the adoption of household technology or the adoption of approved IS in the workplace. The adoption of not approved IS has not been considered from a traits perspective, yet.
3.2 Traits in Public Sector Research

Within the community of public sector and e-government related research, several studies also focused on the influence of traits on the adoption. Especially, the narrow and IT-specific traits received the majority of attention. H.-S. Doong, Wang, & Foxall (2010) found that PIIT has a positive effect on the ignition of e-government innovations by citizens, but the innovators remain less loyal towards the e-government system. Venkatesh et al. (2013) identified PIIT as one of the determinants of e-government system adoption among citizens in rural India. H. Doong (2011) on the other hand found that the personal innovativeness towards IT of managers is a significant predictor of managers intention to purchase e-government software. However, Hung, Chang, & Yu (2006) and Hung, Tang, Chang, & Ke (2009) found no significant relation between the adoption of e-government systems by citizen and their affinity towards IS (PIIT). Another important and often analyzed narrow trait is the disposition to trust, which is especially relevant in the context of government issued systems and portals (Carter & Belanger, 2005). It has been confirmed as an important determinant of e-voting machines (Moynihan & Lavertu, 2011) or various e-government systems in general (Bélanger & Carter, 2008; Lee & Rao, 2007). The focus has been primarily on the adoption of e-government systems by citizens and not how traits can affect the IT behavior of government or public officials.

4 Research Model

The impact of IT-specific personality traits on the usage of Shadow IT is not yet tackled, despite the apparent connection between the adoption of deviant IT innovations and the personal tendency towards innovations within the domain of IT. The theoretical foundation for the user behavior in context of compliance with an IS policy is often based on the neutralization theory by G. M. Sykes & Matza (1957), which is originally from the discipline of Criminology and addresses the rule-breaking by juveniles. The violation of IS security policies, which are usually the rules associated with usage of not approved systems (Siponen & Vance, 2010), is explained through the neutralization of rightfully perceived deviant behavior by the user (Haag & Eckhardt, 2015; Siponen & Vance, 2010). In other words, the user knows he is breaking the rules, but he justifies his violation by rationalizing the violation of the policy (Siponen & Vance, 2010). The neutralization or rationalization of the violation is justified by six different mechanisms: Defense of Necessity, Appeal to Higher Loyalties, Condemn the Condemners, Metaphor of the Ledger, Denial of Injury, and Denial of Responsibility (Siponen & Vance, 2010). The denial of responsibility is the most apparent mechanism, where a user denies any responsibility for her action and thus justify her actions (Siponen & Vance, 2010). The denial of injury is apparent, when the user denies any harm caused by his violation of a policy (Haag & Eckhardt, 2015; Siponen & Vance, 2010). The mechanism of condemn the condemners addresses the blaming of an unreasonable security policy, whereas appeal to higher loyalties reflects the dilemma between following the policy or following the hierarchy (Siponen & Vance, 2010). The metaphor of the ledger, on the other hand takes the idea from a balance of good and bad deeds, where a good action rules out a deviant behavior (G. M. Sykes & Matza, 1957). The defense of necessity addresses a technique, where a user justifies his violation by rationalizing his actions as necessary to do his job (Siponen & Vance, 2010). The rationalization of the necessity can be also based on a technical argument, where the cloud enables an exchange between co-workers or provide increased computing power for necessary tasks. Defense of necessity is a mechanism, which might be influenced by an increased tendency towards IT, because some affinity and knowledge of the technical details might be necessary to apply this inner justification. The mechanisms, where at least some knowledge or skill in IT-specific matters is necessary can be influenced by a personal tendencies towards innovations in the domain of IT. The six justification mechanism described by neutralization theory are meant to capture a broad variance of justification mechanism (Siponen & Vance, 2010; G. M. Sykes & Matza, 1957) and some need at least an above average level of technological savviness. Without the savviness, the rationalization of the rule violation might not work for an individual. The defense of necessity and condemn of condemners mechanism seem like the most likely strategies, because in the context of deviant cloud usage, the
necessity of using it needs some understanding of the technology to rationalize the necessity. The same applies for the condemnation of the condemners, because it is hard to blame a policy, which cannot be rightly assessed.

We expect that at least the mechanism of defense of necessity, if not also the condemn the condemners’ technique are impacted by the level of personal innovativeness in the domain of IT. Both mechanisms benefit from technological knowledge and affinity in the context of IS policies. It is difficult to justify one’s guilt without the ability to assess the necessity of a policy. The same applies for the necessity of a violation, especially if it comes to the technical necessity to violate a policy. Those techniques seem viable to profit from technological savviness, when the rule violation is concerned with Shadow IT usage. As a first step to assess the influence of the individuals PIIT level on the compliance behavior, we will test whether the tendency towards IT has an influence on the compliance towards an IS policy and thus hypothesize:

\[ H: A \text{ higher level of PIIT decreases the possibility of complying to the IS security policy in force.} \]

We expect that users with generally higher affinity towards technology are able to violate the existing policies by using external cloud services, because using remote applications over a web browser is generally more difficult to prevent by the IT department than preventing the installation of local software applications. Many public officials do have access to the Internet from their work computer and blocking specific services is very tedious for IT departments and usually not even very efficient for keeping avid users from accessing the desired applications. From this perspective, the deviant use of cloud services is potentially more apparent to other forms of deviant usage in the IS context, simply because other local forms of deviant usage are generally easier to restrict.

5 Method and Data Analysis

In order to analyze whether the personal innovativeness trait can have an impact on the compliance behavior of employees across public institutions in Germany, we retained the personal innovativeness in the domain of IT with the help of the PIIT measurement scales from Agarwal & Prasad (1998). Our dependent variable is compliance behavior in the context of cloud usage within German public institutions. We adapted validated items from Vance, Siponen, & Pahnila (2012) and N. L. Piquero & Pique-\-ro (2006). We also controlled for the knowledge of the relevant IS policies. Our rule knowledge measurement instrument consisted of three, self-reported items. The first item addressed the general awareness of enforced IS policies within the organizations of the participants. The second and third item addressed actual rules within their institutions, which had to be rated on 7-point Likert scale. With the help of the three items, we could assess whether a participant’s perception of an IS policy matches the reality and how they score in terms of rule knowledge. The study was conducted during the spring of 2015 over a timespan of four weeks and we have been able to obtain the data as a pre-test during a differently focused study. We recorded a total of 1172 responses. The distribution of age, gender, and tenure span as a public official can be seen in Table 1. Due to privacy concerns by the survey public institutions, we were not been able to record the ages as numeric values and thus only collected the age as categorical variables. The demographics of our sample can be seen in Table 1.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age (in years)</th>
<th>Tenure (in yrs)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt; 18</td>
<td>18-21</td>
</tr>
<tr>
<td>Female</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Male</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 1. Demographics

We further analyzed our measurement items. Besides compliance behavior and personal innovativeness, we also surveyed the rule knowledge of our subjects as a control. All of our constructs are based
on validated multi item scales. For internal construct validity we calculated the Cronbach’s Alphas, which is a measure for the unidimensionality of a multi-item scale. It should exceed the threshold of 0.7 in all cases, but stay below 0.95 (Hair, Ringle, & Sarstedt, 2013). All of our constructs passed the threshold. We reported the results of our measurement model in Table 2.

<table>
<thead>
<tr>
<th>Source</th>
<th>Mean</th>
<th>STD</th>
<th>Cronbach’s Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal innovativeness in IT (PIIT)</td>
<td>3.94</td>
<td>1.87</td>
<td>0.94</td>
</tr>
<tr>
<td>Rule Knowledge (RK)</td>
<td>3.06</td>
<td>1.81</td>
<td>0.81</td>
</tr>
<tr>
<td>Compliance Behavior (CB)</td>
<td>4.76</td>
<td>2.04</td>
<td>0.85</td>
</tr>
</tbody>
</table>

Table 2. Descriptive Statistics of Constructs

5.1 Cluster Analysis

Since we are interested in different personal innovativeness profiles within our sample, we clustered our sample based on the individual scores on the PIIT scale by Agarwal & Prasad (1998). We applied Ward’s hierarchical clustering method to obtain the natural number of clusters within our sample. Ward’s algorithm is an agglomerative clustering method, which means that n clusters is the starting solution and the number of clusters is successively reduced until the within-group variance is minimized (Murtagh & Legendre, 2014). The ward method is well suited for multivariate data (Murtagh & Legendre, 2014), like our sample. We applied the Ward method with the help of the hclust package for R (Murtagh & Legendre, 2014). Figure 1 shows the resulting dendogram.

Figure 1. Dendogram

The graph shows how the clustering algorithm started off with the single observations as the leaves of the tree graph on the bottom and worked up to the trunk. The height of the tree represents the variance of the observations. The horizontal line shows the amount of clusters and at the same time how much variance is explained through the cluster itself. While the single leaves are hardly legible due the rather high number of participants, the graph nonetheless shows the even distribution of PIIT levels across our three subgroups. We can see that approximately 75% of the variance is explained by only three clusters (difference of total height and height of the horizontal line dived by total height). The resulting three clusters divided the sample in subgroups of 307 (cluster 1), 412 (cluster 2), and 453 (cluster
3). We can see that the clusters are evenly divided across the variance of PIIT of the public officials. We can observe a cluster with a very low, an average, and a high innovativeness. The distribution of tenure, rule knowledge, and compliance behavior is noted in Table 3.

<table>
<thead>
<tr>
<th></th>
<th>Cluster PIIT Low</th>
<th>Cluster PIIT Medium</th>
<th>Cluster PIIT High</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>307</td>
<td>412</td>
<td>453</td>
</tr>
<tr>
<td>TEN</td>
<td>6.23</td>
<td>5.51</td>
<td>5.53</td>
</tr>
<tr>
<td>PIIT</td>
<td>1.51</td>
<td>3.61</td>
<td>5.89</td>
</tr>
<tr>
<td>RK</td>
<td>3.00</td>
<td>2.99</td>
<td>3.17</td>
</tr>
<tr>
<td>CB</td>
<td>4.93</td>
<td>4.81</td>
<td>4.60</td>
</tr>
<tr>
<td>Mean</td>
<td>7.38</td>
<td>6.62</td>
<td>6.21</td>
</tr>
<tr>
<td>STD</td>
<td>0.52</td>
<td>0.76</td>
<td>0.70</td>
</tr>
<tr>
<td></td>
<td>1.73</td>
<td>1.76</td>
<td>1.90</td>
</tr>
<tr>
<td></td>
<td>2.05</td>
<td>2.00</td>
<td>2.06</td>
</tr>
</tbody>
</table>

Table 3. Cluster Profiles

5.2 Kruskal-Wallis Test

Our data is measured on interval scales, but does not fulfill the requirement of a normal distribution to justify using a parametric approach and hence a non-parametric approach was used (Kabacoff, 2015). We employed the Kruskal-Wallis test (Kruskal & Wallis, 1952) to analyze differences in public officials’ compliance across the various levels of personal innovativeness in the domains of IT. The Kruskal-Wallis test is the non-parametric analogue of a one-way analysis of variance (ANOVA), which allows evaluating smaller samples whose groups are neither normally distributed nor share equal variance (Kabacoff, 2015). It represents the expansion of the Mann-Whitney test for more than two independent groups (Kabacoff, 2015). In order to detect differences among population means, we tested the null hypothesis of equal compliance behavior for all three personal innovativeness clusters. The test statistics for the compliance behavior of 7.0316 (df = 2) shows that public officials’ compliance behavior varies significantly with the personal innovativeness at the level of p = 0.02972.

To identify which of the classes differ significantly, we performed a post-hoc test using Mann-Whitney and found a significant difference between the cluster with high and low personal innovativeness in the compliance behavior of public officials (statistic = 63320.5, p = 0.02821). The other comparisons with the average clusters yielded no significant differences. We also applied the Kruskal-Wallis test to control if the clusters differ in terms of rule knowledge. Significant differences in the knowledge of the rules could easily explain the differences in compliance behavior, but the test could not reject the null hypothesis of equal rule knowledge with a test statistic of 1.5719 (df = 2).

We can conclude that our data supports our hypothesis that a higher level of PIIT does increases the probability of IS policy violations by using cloud services.

5.3 Discussion of Preliminary Results

Our preliminary results demonstrate that our participants show differences in compliance behavior, depending on the membership in the three different PIIT clusters. However, we found only a significant difference between the group associated with a low PIIT level and the group with a high PIIT level. We also controlled if the groups differ in their knowledge of the relevant IS policies, but our results show no indication of different rule knowledge across all three groups. Our findings show that a high level of personal innovativeness in the domain of IT might be resulting in a decreased compliance with the IS security policy in the context of deviant cloud usage within public institutions. Our results appear to confirm our assumption that personal innovativeness might influence the deviant cloud usage in public institutions. As we assumed, a higher personal innovativeness interrelates with a lower compliance with IS security policies. In order to confirm our expected effect of a high personal innovativeness on the mechanism of neutralization theory, we need to conduct a further study. Our preliminary results also add to the broader field of violation and safety research. The research of intended violations of safety regulations is an interdisciplinary research field and addresses violations.
within the healthcare industry (Amalberti, Vincent, Auroy, & de Saint Maurice, 2006), aerospace industry (Vaughan, 1995), or even among regular car drivers (Parker, Manstead, Stradling, & Reason, 1992). Violations are usually understood as intended non-compliance of safety rules, but those violations are not necessarily with a harmful intention (Alper & Karsh, 2009). An example for such a non-harmful violation is a shortcut during work routines in order to increase ones individual productivity. The deviant use of SaaS cloud services might be considered as a non-harmful intended violation in the majority of cases. The research on safety violations has already considered a vast amount of determinants, but surprisingly individual dispositions are not among those analyzed determinants (Alper & Karsh, 2009). However, an increase of worker skill has been associated with an increase of safety violations (Lawton, 1998). Worker skill and PIIT might show some overlap in an IS context, but PIIT addresses the personal disposition and subsequently the overall openness towards technology, which is often understood as a precursor of later acquired skills (Agarwal & Prasad, 1998). Our preliminary results thus add to the existing literature on determinants of safety violations by providing first evidence for the negative association between the IT-specific trait PIIT and IS policy compliance.

6 Next Steps and Expected Outcome

6.1 Future Steps

In the next steps we plan to collect a more data about the compliance behavior of public officials in the context of deviant cloud usage. We plan to measure the application of each of the six neutralization mechanisms. We plan to test the impact of various personal innovativeness levels on each of the mechanism and a possible mediation of PIIT on the compliance behavior through neutralization. We further expect to confirm our preliminary results of this study.

6.2 Expected Outcome

We expect to confirm our preliminary results and present a more granular account of the personal innovativeness on the compliance with IS security policies. This research is helpful on different levels for research and practice. First, it has the potential to advance our understanding of Shadow IT usage by accounting for specific traits of deviant users. A more granular knowledge of different types of deviant users is helpful in order to develop strategies to address specific mechanism to justify a violation of IS policies. The current research framework of neutralization theory is based on a macro account of deviance behavior and it is difficult to use it as a foundation to develop counter-measures.

Second, the expected outcome might be very valuable for practice as it empowers employers to develop and address different strategies to different personalities in terms of IT-specific innovativeness among their employees. In contrast to general models like the Big-Five Inventory, IT-specific traits like the personal innovativeness can be relatively easy approximated. Most managers should be able to categorize her direct subordinates in whether they have an affinity towards IT or a mere reluctance, without even performing a test. Such a categorization would most likely not withstand a scholarly account, but it might be necessary to address the employees with adjusted strategies. The most valuable outcome for practice would be thus a consideration of managers.

Finally, acknowledging the deviant use of SaaS cloud services as safety violations opens up the existing literature on safety violations. While our research can make a contribution to the safety violations literature by addressing personal dispositions as a determinant of violations, our research can also benefit from prior findings and thus a better understanding of why violations occur and how they can be used to improve the overall safety compliance within the public sector. Besides identifying potential violators, individuals with a high disposition towards technology can be used to improve the working procedures. Overall, the majority of violators might not even intend to cause any harm, but improve their work or their productivity. The research on safety violations offers various avenues, which might be reasonable to incorporate into IS research.
References


