Carrot or Stick: Overcoming Silos in Enterprise Architectures

Marcel Cahenzli[1]

[1] University of St. Gallen, Architectural Coordination Group, St. Gallen, Switzerland;
marcel.cahenzli@unisg.ch

Abstract. Silo mentality is a phenomenon describing the aversion of sharing e.g. talent, data, and know-how beyond one's immediate functional and hierarchical environment. Thereby, these silos are mental constructions, which are reflected in procedures and therefore information systems. In an economic environment that is information-driven, getting business units to share information across these organizational silos is highly relevant. This paper uses an enterprise architecture management (EAM) view on silos, where some actors (e.g. architects) guide other actors (e.g. project managers) towards contributing to enterprise-wide goals. To reach desired outcomes in EAM, compliance with enterprise architecture guidelines should be reached. For this setting, the present study investigates drivers for information sharing policy compliance. It combines General Deterrence Theory with Compliance Theory and employs an online experiment. The results reveal that sanctions, rewards, and their interaction significantly affect compliance, whereas the certainty of these sanctions or rewards to materialize did not.

Keywords: General Deterrence Theory, Silo Mentality, Sanction, Reward, Compliance Theory, Enterprise Architecture Management.

1 Introduction

Typically, organizations are structured horizontally in hierarchical layers based on decision-power, as well as vertically, in areas of specialization. This structuring is one of the major reasons for the emergence of silos [1] and silo mentality. Silo mentality is highly relevant to the field of Information Systems (IS) because of the agile and interconnected, information-driven economic environment [2]. Therein new technologies offer new opportunities [3], where the ability to derive insights from data analytics based on combined rich data from across and beyond the organization enables competitive advantages [4]. However, to this end data must be identified, collected, and integrated across silos. Since those silos also exist in business processes and therefore information systems, achieving this interoperability is difficult [3]. The downsides of silos are apparent: conflicting priorities, lack of information flow, duplication of processes, and ultimately waste of resources [2, 3, 5]. In the end, not only has the silo mentality and thus the absence of systemic thinking to be overcome

15th International Conference on Wirtschaftsinformatik,
March 08-11, 2020, Potsdam, Germany

https://doi.org/10.30844/wi_2020_m3-cahenzli

[1], but also the barriers that map to the supporting information technology (IT) and processes [3].

Silos are maintained by conscious and unconscious structures in the minds of the employees. It is therefore not possible to tackle silos with technological solutions only [2, 6]. While the technical optimization of core processes and data storage within organizations is difficult to conceptualize, Ross et al. [3] found that "the corresponding management challenges are even more demanding. Standardizing shared data and core business processes (…) is a much harder sell to business managers than technology standardization" [3]. Similarly, a global survey with more than 1200 executives revealed that "getting business units to share information across organizational silos" is perceived as the biggest challenge in gaining value from data [7, 8].

One way of addressing these challenges may lie in enterprise architecture management (EAM). EAM can be effective with regards to the creation of policies, frameworks and technological solutions. Within an enterprise architecture, the latter can prescriptively and conceptually offer solutions to deter undesirable behaviors. However, the presence of policies alone may not directly lead to policy compliance, since social practices must be considered as well. One theory that has been successfully used to explain the use of counter-measures against non-system-compliant or even anti-social behavior is General Deterrence Theory (GDT). Its central premise is that certain actions may deter policy violations [9] by ensuring that people perceive the ensuing punishment as being likely and severe [10]. The certainty of sanctions and the severity of sanctions should both be inversely correlated with undesirable behavior [11]. GDT may be extended by combining it with Compliance Theory (CT) [12], as inspired by [13]. According to CT, compliance may be enforced through coercive control (negative stimuli, "the stick"), remunerative control (positive stimuli, "the carrot"), and normative control. While most of the EAM literature assumes that organizational responses to EAM initiatives (incl. policy implementations) are either compliance or non-compliance [14], there is a need for gaining a deeper understanding of these compliance mechanisms [15]. There is some existing research that has already addressed the more social and behavioral aspects of EAM [16-19]. This study takes a further step toward closing this gap by combining GDT and CT to investigate the effectiveness of punishment, reward, and certainty of enforcement on compliance with an information sharing policy (ISP), as indicated in the research questions:

RQ1: How does announcing sanctions affect employees' ISP compliance?
RQ2: How does announcing rewards affect employees' ISP compliance?
RQ3: How does enforcement certainty affect employees' ISP compliance?
RQ4: What is the combined effect of sanctions and rewards on ISP compliance?

By employing a scenario-based online experiment, the investigation of these questions revealed that sanctions, rewards, and the combination of sanctions and rewards are positively related to the intention to comply with ISP. However, the

https://doi.org/10.30844/wi_2020_m3-cahenzli

enforcement certainty was not significant, which is unexpected, based on the theorized hypotheses.
The following sections of this papers are structured as follows: Section two summarizes related research on silo mentality, enterprise architecture management, and theoretical backgrounds. Section three contains the research design. Sections four and five contain the results and the discussion.

2 Related Research

2.1 About Silos and Silo Mentality

Silos are not a new phenomenon to management literature and practice. One of the more concise definitions can be found in Hotaran [20], according to whom the silo effect describes "a lack of communication and common goals between departments in an organization." Similarly, silos have been described as an attitude of not being willing to share information or knowledge with people in the same organization, or as psychological spaces of compartmentalization, segregation and differentiation (for an overview, see: [6]). Generally, the (grain) silo metaphor stands for the disconnected functioning of an organization's parts [1]. While physical distance between organizational units can be a factor in the emergence of silos, the metaphor is used more generally for barriers within organizations: Technological, organizational, cultural, and divisional distance, to name just a few [5, 21]. Most effectively though, silos arise from intra-organizational structures. Based on which-ever horizontal (hierarchical) and vertical (functional) divisions an organization takes on, artificial walls are raised between units and between employees. Over time, these formal structures are recreated as informal networks among employees [22]. Barriers are thus present in the minds of the individuals and create dysfunctional fragmentation, dissociation, and disconnectedness, governing their relations through conscious and unconscious patterns [1, 6]. This dysfunctionality becomes apparent in organizational units' desire to contain their "own management team and talent, and lack (of) motivation or desire to work with or even communicate with other organizational units" (Aaker, 2008, in [21]).
The field of research dedicated to such questions of technological and procedural enterprise-wide coordination of information systems is enterprise architecture management (EAM). Therefore, the following sub-section illustrates the EAM perspective on how organizations' information systems and processes evolve and what issues exist along their evolution processes.

2.2 The Use of Enterprise Architecture Management in Overcoming Silos

According to The Open Group [14], EA is defined as a "formal description of a system, or a detailed plan of the system at component level to guide its implementation, including structure, interrelations, and governance of design/evolution over time." It may therefore not only cover current states, but also

https://doi.org/10.30844/wi_2020_m3-cahenzli

to-be architectures and principles guiding its design and evolution [23]. By employing artifacts (processes, methods, and tools) for aligning and prescriptively guiding local IS-related decision-making with global, enterprise-wide goals, EAM goes beyond this descriptive nature of EA [24-26]. With regards to EAM, there are two primary types of actors. The first group is the one that guides (e.g. architects or architecture teams), whereas the second group represents those stakeholders that are being guided (e.g. project managers, local decision-makers). Thereby, the guiding actors try to lead the guided actors towards contributing to enterprise-wide goals, rather than (only) local targets [27-29]. Thus, reaching conformity—or compliance—of local IS related actions with organizational goals is among the main purposes of EAM [25, 30]. The related activities include the adoption, maintenance, and continuous development of an organization's EA [3, 31].

EAM is a means for organizations to gain the ability to effectively use its distributed technologies across its various units and silos [25, 27]. The outcomes that organizations hope to achieve through EAM furthermore include IS efficiency and IS flexibility [16]. IS efficiency can be defined as "the extent and quality of business process support (or automation) through the provision, maintenance, and operation of application systems for the required information processing tasks" in relation to the total cost of the IS function [17]. IS flexibility is the extent to which an enterprise's IS can be adapted to changing requirements [17]. These goals of EAM can be split into factors or "benefit enablers", of which Tamm et al. [18] identified four: Organizational alignment, information availability, resource portfolio optimization, and resource complementarity. However, these benefits cannot be created directly, but only through intermediate steps, including compliance with EA policies [32].

With the above in mind, EAM fits right into the problem of compartmentalization into silos, the unwillingness of local stakeholders to share insights and data across intra-organizational borders, and the need for guidance toward organization-wide goals in local decision making. However, EAM was found to have decreasing marginal added value to organizations with increasing levels of EAM maturity [33, 34]. This effect has been rationalized as being the consequence of EAM's primary drivers being architects, and the stakeholders valuing it being IT professionals [34], but not necessarily the business side. In other words: In order to realize the full potential of EAM (and thus, to overcome the silo mentality and its downsides), new and effective ways of reaching "the other 90%" which are not actively involved in EAM have to be investigated [34]. Similarly Lange et al. [16] point out that there is a need for further research on EAM success factors and in particular taking into consideration the differences among stakeholders and their positions. Indeed, Hylving and Bygstad [15] underline the realization that the discourse on the evolution of architectures lacks an organizational perspective: "In order to improve EAM it is not enough to discuss frameworks and technological solutions, but we must also understand the social practices of EAM." The realization that social factors may play an important role has been reported in several studies, as noticed by Schilling et al. [35]: "EAM initiatives were struggling to achieve desired outcomes. This was mostly due to the prescriptive governance processes and guiding principles being insufficiently respected in organizations [16-18]." After all, stakeholders that are in charge of projects tend to

https://doi.org/10.30844/wi_2020_m3-cahenzli

have key performance objectives, and EAM compliance may not necessarily be (high) on that list of targets [15]. Instead of building and investing in even more sophisticated EAM artefacts, organizations may therefore focus more on the individuals that are confronted with existing EAM artefacts—such as ISP.
In order to better understand when or why individuals react with compliance or non-compliance, and thus substitute enterprise-wide goals for their local goal [16, 34], a deeper investigation of the compliance mechanism is required. The use of negative and positive stimuli is a classical strategy to discourage undesirable behavior and to encourage compliant behavior. I have therefore chosen this strategy for this study.

2.3 General Deterrence Theory and Compliance Theory

If the performance of project managers depends e.g. on insights drawn from datasets that their project teams have gathered, they might not want to make that data and insights from it available to others. The silo mentality leads her to believe that it is better for her not to share data assets across silos (or show the social behavior that enterprise architects hope for). Organizations may thus employ some counter-measures to deter the employees from this behavioral tendency. One theory that has been successfully used to explain the use of counter-measures against non-system-compliant or anti-social behaviors is General Deterrence Theory (GDT). It essentially states that certain actions can deter potential implicit or explicit violations of organizational policies [9], "based on the collective assessment [within a social structure] that punishment is likely and will be severe" [10]. In other words, because people not only know about certain punishments for specific infringements, but because they additionally believe that they are likely to get caught, they refrain from certain negative behavior. The theory thereby refers to economic theory, where utility is the product of the magnitude of some positive and negative outcomes, multiplied by their perceived likelihood of materialization [10]. While this theory has been widely used in criminology to study criminals and anti-social personalities [10], it has also been used for studying social aspects of enterprise-wide IS topics, such as IT security and IT abuse from a user perspective [11, 13, 36]. Thereby, deterrents have been found to lower infringements with guidelines and policy statements. These deterrents discourage people from non-compliant decisions and actions, while at the same time clarifying what constitutes 'rightful' behavior [36]. However, the employees have to believe that the deterrents (or negative stimuli, or sanction) are indeed likely and probable to affect them [11, 13]. Furthermore, they must know about the focal policy and the sanctions, as well as their specific meaning. Employees otherwise use neutralization techniques, or make excuses for policy violations [37] and simply follow their day-to-day routines instead of showing the desired compliance [13]. Based on GDT I have derived the following hypotheses on the effects of sanctions and certainty of materialization:

H1: The severity of a sanction for ISP infringement is positively associated with the intention to comply with ISP.

https://doi.org/10.30844/wi_2020_m3-cahenzli

H2: The impact of sanctions on the intention to comply to ISP is moderated by the certainty of control.

According to compliance theory (CT) by Etzioni [12], compliance is enforced through three types of controls: coercive, remunerative, and normative control. Coercive control employs sanction or negative stimuli ("the stick") as indicated above, whereas remunerative control refers to positive stimuli that reward compliant behavior ("the carrot") [13]. Thus, in addition to the negative incentives used to lower the relative utility of infringing on organizational policies, CT suggests that positive and normative stimuli may also lead to the desired outcomes. With GDT and the underlying economic theory in mind, the utility of compliance and the respective cost of non-compliance are increased through all three types of stimuli. Thereby, the certainty of others knowing about oneself infringing or complying alone, without sanctions or rewards, may act as a normative stimulus. Combining GDT and CT yields these additional hypotheses:

H3: The value of reward for complying with ISP is positively associated with the intention to comply with ISP.
H4: The impact of rewards on the intention to comply with ISP is moderated by the certainty of control.
H5: The certainty of control of ISP compliance is positively associated with the intention to comply with ISP.

Boss et al. found that not all employees perceive organizational policies and procedures as mandatory, and that rewards can send a strong additional signal that compliance is indeed mandatory [38]. Furthermore, as opposed to the use of sanctions, rewards can create harmonious rather than hostile work environments [13]. To enforce compliance, many organizations therefore use both sanctions and rewards to effectively alter rational cost-benefit trade-offs with regards to compliance [13, 39]. From a control perspective, sanctions as well as rewards are control mechanisms, which can be employed to reach organizational goals [40]. This yields the final hypothesis:

H6: There is an interaction effect between the severity of announced sanctions and the value of announced rewards on the intention to comply.

Hence, based on GDT and CT using both severe sanctions and high rewards, while also making sure that the certainty of materialization of these is high, should lead to greater compliance to ISP. This paper investigates, whether these conclusions can be observed and thus, whether the employed theories apply to this specific aspect of EAM. The following section introduces the research design that I have used for this end.

https://doi.org/10.30844/wi_2020_m3-cahenzli

3 Research Design

The hypotheses provide the theoretically rationalized relationships between three independent variables (severity of sanctions, value of rewards, and the certainty of being sanctioned/rewarded) and one dependent variable (intention to comply with information sharing policies). To test the theorized relationship, the dependent variable should be measured while the independent variables are at various levels. To do so, conducting an experiment is highly suitable. After all, experiments' primary strength lies in testing theories by allowing to manipulate certain independent variables while holding the remainder of the environment constant. Therewith, causality can be identified and thus, the hypotheses above can be tested [41, 42].

3.1 Experiment Design

The experiment was based on scenarios in text format and it was conducted through an online survey tool (Questback). For the experiment, two levels per independent variable were operationalized: low and high. This yields the minimal number of conditions necessary to test the theory. The certainty of control was a between-subjects factor. This means that about half of the participants were randomly assigned to the low certainty and the other half to the high certainty condition. Sanction and reward manipulations were within-subjects factors. This results in four combinations (hereafter termed scenarios) of low or high sanctions and low or high rewards manipulations to which every participant was exposed. In order to control for carryover and order effects, I have employed a Latin square matrix design. The manipulations were iteratively developed through pre-tests (see section 3.3). I have used seven questions per scenario. Thereby 7-point Likert scales were used with three items measuring the intention to comply with ISP, as adopted from Chen et al. [13], who drew them from Herath and Rao [43], Ryan [44], and Venkatesh et al. [45], and four items as manipulation checks (see Appendix). The scale was "strongly disagree" to "strongly agree".

3.2 Participants and Procedure

I have recruited all the participants from Amazon Mechanical Turk, an online crowdsourcing platform which has been found to be a suitable data source for online experiments in behavioral research (for a discussion on specific advantages and drawbacks, see: [46]). In the four pre-tests, 30, 30, 100, and 30 people participated, whereas the final experiment was conducted with 250 participants. Participants could only take part once throughout the entire study and all data was collected in July 2019. Participation was remunerated with 0.9 USD. Since any employee is a relevant source for insights on ISP compliance, the general public was chosen as the target population. The participants themselves live in the USA and Canada and they were required to have a track record of >99% acceptance rate of their HITs (human intelligence tasks). The participants in the final experiment covered the whole range of the working population, starting from 18 years old up to 68 years. Mean, median

https://doi.org/10.30844/wi_2020_m3-cahenzli

and mode (32.4 years, 31 years, and 28 years) were rather close together with a skewedness to the younger ages. Most participants either finished college (27%) or have received a bachelor's degree (39%) as the highest educational degree. 48.8% of the participants were women. The participants were directly acquired through the Amazon Mechanical Turk platform, from which they accessed the survey and through which they received their remuneration.

In the final experiment, each participant was greeted with a welcome message, before seeing the shared scenario. The latter introduced all participants to the same hypothetical environment, in which 'Mike' is confronted with a new 'information sharing policy' (see Appendix). On a subsequent page, the participants had to repeat in their own words, what the text was about (attention check). 98.0% of the participants have provided a correct answer, which led me to believe that the participants were attentive and understood the setting. Thereafter, the participants were assigned to the low or high certainty condition. The certainty of materialization was implemented such that either a compliance officer randomly controls five out of one hundred employees every year (low), or a monitoring software constantly supervises the employees' actions (high). Given the certainty condition, each participant was asked to answer the seven questions per combinatorial scenario. These scenarios featured all four combinations of low or high sanctions and rewards respectively. The sanctions were framed as automated messages informing that one got caught and should comply (low), along with a 5% cut of the year-end bonus (high). The rewards were consisting of an automated message congratulating that one was found to be compliant (low), along with a 5% bonus increase (high). The entire experiment took on average 10.6 minutes.

3.3 Scenario and Manipulation Development

I have developed the scenarios and the manipulations such that they are easily understandable. In order to achieve this, I have kept the text sequences short and the wording clear. To ensure clarity and understandability I have conducted two pre-tests with 30 people from the same population as for the final experiment. Based on these pre-tests, I have iteratively adapted and simplified the text sequences for the shared scenario.

The manipulations themselves required two more pre-tests, one with 100 persons (trial of the full experiment), and another one with 30 persons (testing alternative manipulations). With regards to the manipulations, several problems surfaced in the larger pre-test: First, the initial manipulations did not have a significant effect. Especially the rewards were not effectively manipulated, where the high level of reward was perceived as less attractive than the low level of reward. Second, the participants appeared to be highly susceptible to the low level of sanctions chosen in the initial design, which was oral critique in a routine meeting. Lastly, since the participants see four nearly identical texts with the scenarios, there is a probability of them not reading each manipulation carefully. From the outset, I have used a short disclaimer indicating that the scenarios are similar but not exactly the same. Some participants noted that this was an important piece of information, and that they would

https://doi.org/10.30844/wi_2020_m3-cahenzli

have thought that there was a bug in the survey otherwise. Therefore, I have made the disclaimer more visible by using an additional page just before the manipulations were shown. Furthermore, I have colored the sections containing the manipulations to make sure that they were read.

To improve the manipulations for rewards and sanctions, I have tested a series of four alternative sanctions and four alternative rewards. The item with the lowest (automatic email) and highest rating (-/+ 5% bonus) replaced the ineffective manipulations. Thus, the constructs could be manipulated more adequately, such that the 'high' condition yielded consistently and significantly higher values. Table 1 shows the mean values from the manipulation checks of the third pre-test (initial) and the fourth one (improved manipulations). (The detailed texts used in the final experiment are in the Appendix.)

Table 1. Manipulation Development

	Initial Manipulations (mean)			Improved Manipulations (mean)		
	Comment in meeting	-/+ 5% bonus		Autom. email	-/+ 5% bonus	
Manipulation check	Low	High	Δ[%]	Low	High	Δ[%]
Severity of Sanction	4.942	5.321	7.7	3.019	5.019	66.3
Value of Reward	4.909	4.790	-2.4	3.254	5.395	65.8
Certainty of Sanction	5.518	6.131	11.1	3.855	5.699	47.9
Certainty of Reward	5.140	5.142	0.04	4.117	4.742	15.2

https://doi.org/10.30844/wi_2020_m3-cahenzli

4 Analysis and Results

To test the discriminant validity of the intention to comply construct I have carried out an exploratory factor analysis (EFA). For doing so, the sample size must be large enough and there should be at least one correlation. The Kaiser-Meyer-Olkin measure of sample adequacy was 0.742 and therewith higher than 0.5, which is the minimal acceptable criterium, but lower than 0.8, which would be 'meritorious' [see: 47]. Bartlett's test of sphericity was significant and thus, there is at least one correlation. The EFA has yielded only one factor with an Eigenvalue of above the suggested 1.0, containing all three questions (Eigenvalue: 2.59). The factor loadings are high for each measurement construct (Comp_1: 0.821, Comp_2: 0.900, Comp_3: 0.871), which is why I have kept all three of them. Cronbach's Alpha has also exceeded the cutoff value of 0.7 with 0.921. Hence, the three questions for the intention to comply are reliable.

For the manipulation checks, I have conducted five one-way ANOVAs (analyses of variance), for the factors severity of sanction, value of reward, certainty, certainty of sanction, and certainty of reward. All manipulations were highly significant ($p < 0.001$). Hence, the manipulations of the theoretical constructs were successful.

I proceeded with checking the hypotheses with a univariate ANOVA. Thereby, hypotheses H1, H3, and H6 were highly significant with $p < 0.001$ (see: Table 2). Hence, sanctions and rewards have indeed increased the intention to comply, if these were set to high rather than low (H1, H3). Furthermore, using both sanctions and rewards has an additional interaction effect. The effect of punishment is moderated by the provision of rewards. With more valuable reward schemes, the motivating effect of sanctions is much smaller. Importantly, this effect arises independently of the certainty with which an employee might receive a reward. This was a consistent pattern, even though the manipulation check indicated clearly that the participants understood that they were less or more likely to get caught and punished, or to be found compliant and be rewarded. Thus, H2, H4, and H5 had to be rejected. Hence, the certainty of control did neither affect the participants' intention to comply by itself, nor did it cumulate with sanctions or rewards. Upon further investigation, I have identified highly significant effects of the certainty manipulation on the perceived certainty of getting sanctioned and the perceived certainty of getting a reward, as well as the perceived severity of the sanction (all with $p < 0.001$). Hence, the certainty manipulation affected the perceived certainty construct as intended. Yet the theorized effect was not observable.

Table 2. Hypotheses Tests

Hypothesis	Mean square	F-value	p-value	Accept?
H1: Sanction × Intention	59.865	40.564	< 0.001	Yes
H2: Sanction × Certainty × Intention	0.001	0.001	0.981	No
H3: Reward × Intention	65.977	44.705	< 0.001	Yes
H4: Reward × Certainty × Intention	0.683	0.463	0.497	No
H5: Certainty × Intention	0.137	0.093	0.761	No
H6: Sanction × Reward × Intention	26.521	17.97	<0.001	Yes

https://doi.org/10.30844/wi_2020_m3-cahenzli

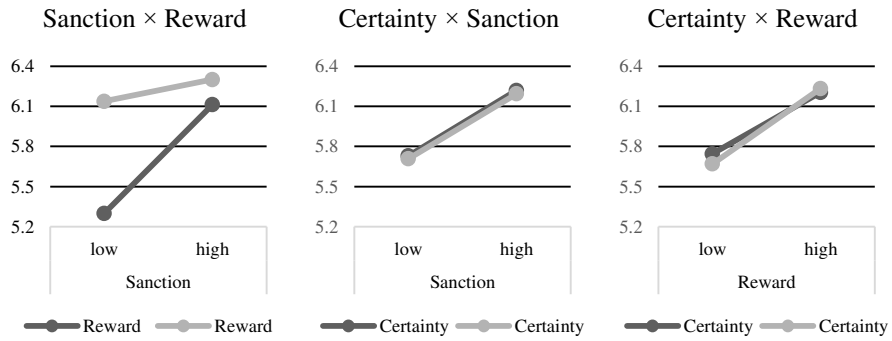

Figure 1. Correlation Effects

5 Discussion and Conclusion

This study has shown that sanctions and rewards are positively related to the intention to comply with policies requiring employees to share data and insights across organizational silos. This is in line with General Deterrence Theory, Compliance Theory and more generally: economic theory. Furthermore, a former finding on the interaction effect between the use of sanction and rewards could be replicated [13]: While the severity of sanctions is positively related to the intention to comply in general, this effect is much smaller in cases where a high reward for compliance is provided in addition. These effects could be observed under high and low certainty of receiving the reward as well as under high and low certainty of getting sanctioned. That certainty is ineffective however, was not expected based on GDT. The latter states that the sanction is only one part of the intention to change one's behavior. The other part is the certainty of getting caught. That certainty should therefore increase or decrease the effect of a sanction (and also of a reward, since GDT was merged with CT) depending on whether it is high or low. This was not the case though. In this point, the results strongly differ from Chen et al.'s [13] findings. Since this experiment conceptually replicates the latter, one could have thought that the effects would be similar. However, the certainty construct, while being adequately manipulated (as judged by the manipulation check), did not reach significance. While Chen et al. show a p-value for Certainty × Intention of p=0.017 in the information security policy experiment, the information sharing policy experiment's p-value was p=0.761. Hence, the certainty did not affect the intention to comply. This was also true for any interaction effects containing certainty. One possible reason for the different results is, that this experiment was conducted with the general public, rather than IT specialists [13]. The reason for choosing the general public was that the problem under investigation arises in the "other 90%", that is: information sharing between functional silos among the employees and not necessarily IT professionals. After all, the goal of this experiment was to investigate possible strategies to increase the value of Enterprise Architecture Management by reaching beyond the IT function and establishing Architectural Thinking [34]. Since this is the only relevant difference

https://doi.org/10.30844/wi_2020_m3-cahenzli

from Chen et al.'s study, there is reason to believe that IT professionals might react differently to lower or higher levels of certainty of control, whereas other employees do not differentiate them.

Limitations and future research: First, the experiment employed in this study is of a laboratory character, being an online scenario-based experiment. Therefore, internal validity was focal, rather than external validity. Even though the manipulation checks indicated that the intended constructs were manipulated, and the reliability check showed that the measurement of the dependent variable was effective, the results might not map actual work scenarios. This is an inherent tradeoff in experimental research. However, since silo mentality and silos from an EAM perspective is barely researched in IS literature, I have deemed the internal validity to be more important at this stage than external validity. To adequately generalize these theoretical findings, further studies and in particular field experiments would help increase the validity. Second, the dependent variable measured the intention to comply, rather than the actual behavior. While this is one of the most common critiques in experimental research (and in particular in scenario-based experiments), this procedure is highly established. For this reason, this initial study of the relationships between sanctions, rewards, and certainty of control on compliance behavior also relies on the intention to comply only. Based on these results, field experiments or interactive laboratory experiments measuring actual behavior can be designed to further investigate the external validity of the effects. Third, rewards and sanctions can be studied on various levels. While this experiment studied rewards and sanctions for the participants (individual level), it disregards the possibility of rewarding and sanctioning e.g. project teams (group level). Since the idea was to keep the scenarios as simple as possible in this online experiment, further laboratory or laboratory-like experiments may replace or append the individual level by the group level (e.g. see [48]).

Contribution to practice: The findings of this study may help enterprise architects to increase the impact of EAM across organizations by adequately motivating employees to comply with data and insight sharing policies, and thus to abandon the silo mentality. The latter is highly relevant, because it is a non-technical aspect to EAM that has not been overcome yet and for which traditional technological means of EAM are not sufficient. Furthermore, in comparison to the findings of a former study with IT specialists, the results suggest that non-IT and IT professionals may respond differently to implementation strategies. Practitioners may take this into account.

Contribution to research: Little research has been conducted on the phenomenon of silo mentality when it comes to EAM. Traditionally, EAM focused on primarily technological aspects and thus, found greatest acceptance in IT functions. However, on the business side there is untouched potential for the benefits of EAM. In particular, silos inhibit the effective collection of enterprise-wide data, know-how, and insights from data. The coordination of employee behavior towards a more fundamental orientation on enterprise-wide goals rather than local compartmental goals, and thus sharing information freely across the organization is not primarily

https://doi.org/10.30844/wi_2020_m3-cahenzli

relevant for IT functions, but rather all employees in all (business) units. Literature suggests Architectural Thinking as a solution [34]. The findings form this paper append to the discussion on how Architectural Thinking might be implemented and how the entire organization's day to day decisions-making could be effectively included in EAM initiatives. In particular, this study investigated the effectiveness of sanctions, rewards, and certainty of control on the intention to comply with information sharing policies. To the best of my knowledge, no other study has investigated this implementation mechanism for overcoming silo mentality in general, and for the implementation of information sharing policies in particular. Furthermore, the findings question the applicability of GDT for silo mentality. Even though this theory seemed to apply to deter computer abuse [11, 36] and information security policy infringement [13], it did not predict information sharing policy compliance behavior.

6 Acknowledgements

This work has been supported by the Swiss National Science Foundation (SNSF).

References

1. Cilliers, F., H. Greyvenstein: The impact of silo mentality on team identity: An organisational case study. SA Journal of Industrial Psychology. 38(2) (2012)
2. Wilhelm, K.: Breaking down silos and coordinating across departments. In: Making Sustainability Stick, Pearson: Upper Saddle River, NJ, pp. 162-164 (2014)
3. Ross, J.W., P. Weill, D.C. Robertson: Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Boston, MA: Harvard Business School Press (2006)
4. Kitchens, B., et al.: Advanced Customer Analytics: Strategic Value Through Integration of Relationship-Oriented Big Data. J. Manag. Inf. Syst. 35(2), 540-574 (2018)
5. Bannister, F.: Dismantling the silos: extracting new value from IT investments in public administration. Inf. Syst. J. 11(1), 65-84 (2001)
6. Mohapeloa, T.: Effects of silo mentality on corporate ITC's business model. Proceedings of the 11th International Conference on Business Excellence. 11(1), 1009-1019 (2017)
7. Gardner, H.K.: When senior managers won't collaborate. Harvard Bus. Rev. 93(3) (2015)
8. Lyytinen, K., V. Grover: Management Misinformation Systems: A time to revisit? Journal of the Association for Information Systems. 18(3), 206-230 (2017)
9. Nance, W.D., D.W. Straub: An investigation into the use and usefulness of security software in detecting computer abuse. ICIS 1988 Proceedings. 36 (1988)
10. Pearson, F.S., N.A. Weiner: Toward an Intergration of Criminological Theories. Journal of Criminal Law and Criminology. 76(1), 116-150 (1985)
11. Straub, D.W., R.J. Welke: Coping with Systems Risk: Security Planning Models for Management Decision Making. Manag. Inf. Syst. Q. 22(4), 441-469 (1998)
12. Etzioni, A.: A comparative analysis of complex organizations : on power, involvement, and their correlates / by Amitai Etzioni. New York: Free Press (1975)
13. Chen, Y., K. Ramamurthy, K.W. Wen: Organizations' Information Security Policy Compliance: Stick or Carrot Approach? J. Manag. Inf. Syst. 29(3), 157-188 (2012)

https://doi.org/10.30844/wi_2020_m3-cahenzli

14. The Open Group: The Open Group Architecture Framework (TOGAF) Version 9.1. TOGAF Series. Zaltbommel: Van Haren Publishing (2011)
15. Hylving, L., B. Bygstad: Nuanced Responses to Enterprise Architecture Management: Loyalty, Voice, and Exit. J. Manag. Inf. Syst. 36(1), 14-36 (2019)
16. Lange, M., J. Mendling, J. Recker: An Empirical Analysis of the Factors and Measures of Enterprise Architecture Management Success. Eur. J. Information Systems. 25(5), 411-431 (2016)
17. Schmidt, C., P. Buxmann: Outcomes and Success Factors of Enterprise IT Architecture Management: Empirical Insight from the International Financial Services Industry. Eur. J. Information Systems. 20(2), 168-185 (2011)
18. Tamm, T., et al.: How Does Enterprise Architecture Add Value to Organisations? Commun. Assoc. Inf. Syst. 28(1), 141-168 (2011)
19. Schilling, R.D., S. Aier, R. Winter: Designing an Artifact for Informal Control in Enterprise Architecture Management. In: Proceedings of the 40th International Conference on Information Systems (ICIS 2019): Munich, Germany (2019)
20. Hotaran, I.: Silo effect vs. supply chain effect. Review of International Comparative Management. 10(1 (special issue)), 216-221 (2009)
21. Gyrd-Jones, R.I., C. Helm, J. Munk: Exploring the impact of silos in achieving brand orientation. J. Mark. Manage. 29(9-10), 1056-1078 (2013)
22. Vermeulen, F., P. Puranam, R. Gulati: Change for Change's Sake. Harvard Bus. Rev. 88(June), 6 (2010)
23. ISO/IEC/IEEE: Systems and Software Engineering—Architecture Description (ISO/IEC/IEEE Std 42010:2011). ISO/IEC and IEEE Computer Society (2011)
24. Lankhorst, M.: Enterprise Architecture at Work: Modelling, Communication and Analysis. Heidelberg: Springer Science & Business Media (2005)
25. Boh, W.F., D. Yellin: Using Enterprise Architecture Standards in Managing Information Technology. J. Manag. Inf. Syst. 23(3), 163-207 (2006)
26. Simon, D., K. Fischbach, D. Schoder: An Exploration of Enterprise Architecture Research. Commun. Assoc. Inf. Syst. 32(1), 1-72 (2013)
27. Brosius, M., S. Aier, K. Haki: Introducing a Coordination Perspective to Enterprise Architecture Management Research. In: Trends in Enterprise Architecture Research (TEAR), Quebec City: IEEE Computer Society, pp. 71-78 (2017)
28. Brosius, M., et al.: A Learning Perspective on Enterprise Architecture Management. In: International Conference of Information Systems, Dublin (2016)
29. van Steenbergen, M., S. Brinkkemper: The architectural dilemma: Division of work versus knowledge integration. (2009)
30. Richardson, G.L., B.M. Jackson, G.W. Dickson: A Principles-Based Enterprise Architecture: Lessons from Texaco and Star Enterprise. Manag. Inf. Syst. Q. 14(4), 385-403 (1990)
31. Aier, S., B. Gleichauf, R. Winter: Understanding Enterprise Architecture Management Design – An Empirical Analysis. In: the 10th International Conference on Wirtschaftsinformatik (WI 2011), Zurich, Switzerland (2011)
32. Foorthuis, R., et al.: A theory building study of enterprise architecture practices and benefits. Information Systems Frontiers. 18(3), 541-564 (2016)
33. Ross, J.W., A. Quaadgras: Enterprise Architecture Is Not Just for Architects. Center for Information Systems Research Sloan School of Management Massachusetts Institute of Technology: Cambridge, MA (2012)
34. Winter, R.: Architectural Thinking. Bus. Inf. Syst. Eng. 6(6), 361-364 (2014)

https://doi.org/10.30844/wi_2020_m3-cahenzli

35. Schilling, R.D., K. Haki, S. Aier: Dynamics of Control Mechanisms in Enterprise Architecture Management: A Sensemaking Perspective. In: 39th International Conference on Information Systems (ICIS 2018), San Francisco, USA (2018)
36. Straub, D.: Effective IS Security: An Empirical Study. Inf. Syst. Res. 1(3), 255-276 (1990)
37. Siponen, M., A. Vance: Neutralization: New insights intot the problem of employee information systems security policy violations. Manag. Inf. Syst. Q. 34(3), 487-A12 (2010)
38. Boss, S.R., et al.: If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. Eur. J. Information Systems. 18(2), 151-164 (2009)
39. Bulgurcu, B., H. Cavusoglu, I. Benbasat: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Manag. Inf. Syst. Q. 34(3), 523-548 (2010)
40. Eisenhardt, K.M.: Control: Organizational and Economic Approaches. Manag. Sci. 31(2), 134-149 (1985)
41. Thye, S.R.: Logical and philosophical foundations of experimental research in the social sciences. In: Laboratory experiments in the social sciences, M. Webster and J. Sell, Editors, Elsevier/Academic Press: London, UK, pp. 53-82 (2014)
42. Webster, M., J. Sell: Why do experiments? In: Laboratory experiments in the social sciences, M. Webster and J. Sell, Editors, Elsevier/Academic Press: London, UK, pp. 5-22 (2014)
43. Herath, T., H.R. Rao: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Information Systems. 18(2), 106-125 (2009)
44. Ryan, M.J.: Behavioral intention formation: The interdependency of attitudinal and social influence variables. J. Cons. Res. 9(3), 263-278 (1982)
45. Venkatesh, V., et al.: User Acceptance of Information Technology: Toward A Unified View. Manag. Inf. Syst. Q. 27(3), 425-478 (2003)
46. Mason, W., S. Suri: Conducting behavioral research on Amazon's Mechanical Turk. Beh. Res. Methods. 44(1), 1-23 (2012)
47. Dziuban, C.D., E.C. Shirkey: When is a Correlation Matrix Appropriate for Factor Analysis? PsyB. 81(6), 358-361 (1974)
48. Hashim, M.J., J.C. Bockstedt: Overcoming Free-Riding in Information Goods: Sanctions or Rewards? In: 48th Hawaii International Conference on System Sciences, pp. 4834-4843 (2015)

7 Appendix

7.1 General Setting Presented to the Participants

Please read the following text carefully: Mike works in a project team for the "Idea Corporation" (iCorp for short), a large company that creates innovative products. Usually, they try to predict what people will want in the future and then build these products. To make these predictions, every project team gathers a lot of information and analyzes this data. At the end of each year, there is an evaluation of the work performance. For Mike this means, that he might get a bonus or a promotion, if his and his project teams' ideas are successful. At the same time, he might not be promoted or get any bonus at all, if his project team is weaker than the performance of other project teams.

https://doi.org/10.30844/wi_2020_m3-cahenzli

(click on next page)

Lately, the managers at iCorp have sent an e-mail with the company's new "information sharing policy" around. Here's what is says:

Information sharing policy:
For many years, we have worked in project teams. Each project team has gathered data and analyzed it themselves. This meant that sometimes two or more project teams investigated the same ideas, instead of just one team who then shares their insights. This is not efficient, and we therefore have decided on this new "information sharing policy":

1. All employees must share the data they gather with all project teams.
2. All employees must share the ideas they have with all project teams.
3. All employees can use the ideas and data from other project teams.

7.2 Scenarios Presented to the Participants

Condensed version with all manipulation combinations [low | *high*]
(The order of the manipulations is: likelihood, reward, punishment.)

"How does Mike react? Mike is aware that [iCorp makes compliance checks once a year. The compliance officer randomly chooses five out of 100 employees and checks whether they were compliant or not. The assessments are unscheduled. After each assessment a report is created. | *to enforce compliance with the information sharing policy, iCorp has its IT department monitor and record information sharing policy compliance. Therefore, a monitoring software is used on a regular basis. At the end of the year the management receives a report for every project team and every employee.*] If a controlled employee was found to be compliant, he/she will receive an automated email thanking them for [sticking to the corporate policies. | *sticking to the corporate policies. He/she also get a 5% increase of their bonus.*] The employees that were found to infringe on corporate policy will receive an automated email reminding them that [they must comply to the information sharing policy. | *they must comply to the information sharing policy. They will furthermore have a 5% cut of their bonus.*"]

7.3 Measurement Items Presented to the Participants

Compliance: "Given this hypothetical scenario and assuming you were Mike, please specify the extent to which you would agree or disagree with the following statements:"

1. It is possible that I will follow iCorp's information sharing policy.
2. It is probable that I will follow iCorp's information sharing policy.
3. I am likely to follow iCorp's information sharing policy.

Manipulation checks: "What do you think about this situation?"

https://doi.org/10.30844/wi_2020_m3-cahenzli

[likelihood - rewards:] If I follow the policies, the chance I would get rewarded is high.
[likelihood - punishment:] If I violate the policies, the chance I would get caught is high.
[severity - punish:] If I were caught violating the policies, I would be punished severely.
[size of the reward:] If I follow the policies I would be rewarded greatly.

https://doi.org/10.30844/wi_2020_m3-cahenzli