Unaware Unethical Behavior and 'Learning from Error' through the Knowledge Sharing

Concetta Metallo[1], Rocco Agrifoglio[2], Concetta Cristofaro[3], Maria Ferrara[2], Paolino Fierro[2], Reina Reina[3], Mauro Romanelli[2] and Roberta Oppedisano[2,1]
[1]Department of Science and Technology, University of Naples "Parthenope", Naples, Italy
[2]Department of Business and Economics, University of Naples "Parthenope", Naples, Italy
[3]Department of Law, Economics, and Sociology, University of Catanzaro "Magna Graecia", Catanzaro, Italy
concetta.metallo@uniparthenope.it
rocco.agrifoglio@uniparthenope.it
concetta.cristofaro@unicz.it
maria.ferrara@uniparthenope.it
paolino.fierro@collaboratore.uniparthenope.it
rreina@unicz.it
mauro.romanelli@uniparthenope.it
roberta.oppedisano@uniparthenope.it

Abstract: The paper focus on fraudulent or unethical behaviors in which there is no awareness, reasoning, or intention, but an incorrect action that results from lack of knowledge in terms of action errors. Using error management framework, we focus on the potential positive effects of errors, to link the errors with the more general goal of learning. Literature has shown that errors are often related to communication failures and of sharing of information. To enrich our understanding about fraudulent or unethical behaviors, this article contributes to the extant literature by investigating how knowledge sharing behaviors impact on the process of learning from error within the firm, to preventing future fraudulent or unethical behavior. The study reports a case study for examining the characteristics of the knowledge sharing behaviors, and how these behaviors characteristics impact the process of learning from error within the organization, to preventing future fraudulent or unethical behavior.

Keywords: unethical behaviors, fraudulent behaviors, knowledge sharing behaviors, error management, learning from error

1. Introduction

Previous research has theoretically and empirically examined fraudulent or unethical behaviors in organizations. However, the reasons why individuals act unethically are not clear and well defined (Brief et al. 2001; Lewicki et al. 1997). Unethical behaviors are defined as acts that are harmful to others and are "illegal or morally unacceptable to the broader community" (Jones, 1991, p. 367). Kish-Gephart and colleagues (2010, p. 2) add additional attributes to Jones' definition by delineating unethical behaviors as "any action by members of the organization that violates widely accepted (social) moral norms". Much research incorporates the intent behind the fraudulent or unethical action that is behaviors intended to benefit the organizations, its members, or both. But often individuals are unconscious of fraudulent behavior and do not consider their behavior non-compliant.

We focus on fraudulent or unethical behaviors in which there is no awareness, reasoning, or intention, but an incorrect action that results from lack of knowledge in terms of action errors (Van Dyck et al., 2005). In fact, there are some situations in which individuals do not recognize that the behavior is fraudulent or unethical (Tsang, 2002), but it's about actions involving errors, mistakes, or unconscious negligence (e.g., Asare and Wright, 1995).

The error that generates fraudulent or unethical behavior can represent for organization a learning opportunity, by understanding causes and implementing changes that will prevent future errors or reduce the negative consequences when errors reoccur (Reason, 2000). Errors are defined as the actions of multiple participants in the organization that deviate from the organization's specified rules and procedures and that can potentially lead to adverse organizational outcomes (Bell and Kozlowski, 2009).

[1] Corresponding author

Lipshitz et al. (2002, p. 81) state that learning must be seen as "a cyclical process of evaluating past behavior, discovering the mistake or opportunity, inventing new behaviors and implementing them". The evaluation of past behaviors and acting based on the awareness that errors support useful information are in fact considered important practices to learn from error (Van Dyck et al., 2005).

Several scholars argue that error communication facilitates learning from error (Ledva et al., 2017). Communication is one of the most important conditions to learn from the occurrence of the error (Edmondson, 1996; van Dyck et al., 2005). Edmondson (1996) points out that creating an environment that fosters frequent knowledge sharing supports learning from error. In fact, errors are often linked to errors in communication and in updating and sharing information (Bell and Kozlowski, 2011).

Mistakes are often related to communication failures and failures of updating and sharing of information (Bell and Kozlowski, 2011). Thus, communication about errors and knowledge sharing behaviors probably constitutes the most important error management practice (Van Dyck et al., 2005; Murphy and Dacin, 2011; Khorakian et al., 2019), enabling individuals to learn from error (Keith et al., 2020).

Knowledge sharing behaviors manifest when employees share their knowledge with other colleagues, through a mutual exchange of knowledge and providing an opportunity for the employees to acquire new knowledge (Khorakian et al., 2019; Yu, Yu-Fang, and Yu-Cheh, 2013).

Knowledge management research agrees that organizational improvement and change occur when employees are engaged in knowledge-related behaviors (e.g., Longo and Mura, 2011; Mura et al., 2013). Managers implemented a set of initiatives to improve daily work practices and to avoid fraudulent behaviors by mobilizing employees' knowledge (Mura et al., 2013).

To enrich our understanding about fraudulent or unethical behaviors, this article proposes a research model that integrates three research streams, namely error management, learning from error, and knowledge management. This article contributes to the extant literature by investigating how knowledge sharing behaviors impact on the process of learning from error within the firm, to preventing future fraudulent or unethical behavior. In particular, the research question of the study is: Can a fraudulent or unethical behavior generated by error represent for organization a learning opportunity through knowledge sharing behaviors?

2. Methodology

To investigate our research questions, we adopted a qualitative approach based on a single case study. We believe that this procedure is an opportunity to describe the process through which our phenomenon takes place (Taylor et al. 2011). In addition, the use of case study methodology is particularly useful for investigating the "how" and "why" of a set of contemporary events (Yin, 2009). The aim of the method used in this research is not to generalize the case under examination, but rather to understand it accurately in its peculiarity, uniqueness, complexity and in its specific social and economic context (Stake R., 1994). Our investigation looked in depth at a contemporary case within a real-life context (Yin, 2009), for understanding how a fraudulent or unethical behavior generated by an error can represent a learning opportunity for the organization through knowledge-sharing behaviors. The detailed analysis of the case allowed us to learn about the phenomenon through intensive exploration (Becker, 1970). We followed Yin's (2009) guidelines that ensure the regularity of the construct, planning, and execution of the case study. This methodology provided a comprehensive understanding of the phenomenon at hand without the rigidity of a predefined structure for observations and analysis (Fidel, 1984). The choice of case study rather than another method was dictated by several reasons. Firstly, the subject of the case study is specific and significant of unethical and fraudulent behavior. Secondly, the case study is representative of a unique situation and a phenomenon that has never been investigated before. Most importantly, it was chosen as a 'revealing case' to which researchers had a privileged access.

Moreover, the case study allowed us to investigate all those activities carried out within the company that are part of the " routine " and to understand the peculiarities of the context in which the organization operates. The data collection combined several methods: archival research, interviews, direct observations, and other sources (e.g., institutional documents, newsletters, and local newspapers). During the research, two of the authors attended meetings, workshops, and training sessions held at organization and observed the work practices of

employees going about their daily routines. In terms of secondary data, we also collected data by reviewing some of the extensive internal documentation that was shared with us by staff after an explicit request.

Data collected from a variety of sources between 2019 and 2020 were analyzed throughout the study, constantly reviewing any new data resulting from the research observations and surveys. In addition, the study was conducted through the observational mode to bring objectivity to the study and reduce bias. This technique ensures valuable information and a deep understanding of the individual case study in addition to leading to sound scientific conclusions (Yin, 2009; Reischauer, 2015).

2.1 The case study

The “XXX” (organization requested anonymity) founded in the late 1700s, is a private law organization under public control and has as its purpose the dissemination of musical art, the musical education of the community, as well as the artistic and professional development of its staff (Article 2, paragraph 2, of the Statute). The State, the Campania Region and the Municipality of Naples are the public founders participating in the activity of "XXX". It has a single headquarters in Italy in Naples and consists of about 400 operators including employees, collaborators, artists, and freelancers. The “XXX” carries out its activities in Italy and abroad and is a body of overriding national interest. It manages an important theater, a classical dance academy and a singing school for young artists as well as organizing world-class musical and artistic events annually. The "XXX" is a non-profit organization and is prohibited by its statutes to distribute profits or other assets. The purpose of the "XXX" is related to the dissemination of musical art, musical education to the community, as well as the artistic and professional development of its staff. It organizes opera, theatre, music, concerts, and ballets in Italy and abroad. For these reasons, the organization maintains institutional relationships with individuals (subscribers, school students, families) and with companies that provide the most diverse services from marketing to cyber security to communication.

In 2018, "XXX" began the complex process of adapting to the General Data Protection Regulation (GDPR) not only because the company has a regulatory obligation but also to assess the riskiness of the processing carried out, and to provide for security measures, technical and organizational, appropriate to the riskiness detected. The GDPR (EU Regulation 2016/6791) is the body of legislation designed to reinforce and standardize the personal data protection within the borders of the European Union by influencing extra European operators within EU borders. Its main objective is to reinforce the rights of individuals in terms of protection of personal data while facilitating the free circulation of data within the digital single market.

To this end, 'XXX' decided to use external consultants to adapt to the GDPR data protection model. In fact, since the company did not have the necessary resources to achieve the data protection objective, it chose external consultants, qualified specialists who were neutral with respect to the problem to be solved. The external consultants interacted with the company members, offering professionalism that enriched the company with skills and experience. Two researchers joined the company consultants to take part in this research and collaborated to draft interviews aimed at studying the working practices and procedures of the officers and whether these activities were in line with the provisions dictated and regulated by the GDPR. Thus, business advisers assisted by the researchers, during the interviews, detected incorrect, unethical, and fraudulent behavior in accordance with the GDPR.

Exploratory interviews were conducted with 14 key officers and 3 service providers, for understanding the cybersecurity procedures in relation to data management. They have been a very effective way of collecting large amounts of information, especially since the phenomenon of interest is not particularly frequent. All interviews were recorded and then transcribed to analyze the data. The information provided by the respondents enabled the company consultants to draw up a proper data management model according to the GDPR, and the researchers to conduct this research.

Here are some testimonials:
“*In the administration area there are 9 workstations that access the management system. For convenience we have only one user and password so that if someone is missing, anyone is able to operate*” (Employee). This interview testifies to incorrect behavior that exposes the organization to risks but is perceived as correct because it is legitimized and accepted by the context.

"*Cybersecurity is an issue that does not interest us, we are not a marketing company or a healthcare company*" (Key officer). The respondent shows reluctance to the correct procedures indicated by the business consultants and researchers involved in the drafting of the GDPR data management model.

"*If you force me to change my password every 120 days, I'll have to paste a post on the monitor to remind me!*" (Employee). In this case too, the employee's testimony indicates incorrect behavior that exposes the organization to risks, but which is perceived as correct because it is legitimized by the context.

Other misconduct also concerned the video surveillance system of the company 'XXX'. Company images were being recorded by the company without the employees' permission to use them. 'I didn't know it was a problem to record company images, I thought it was useful to protect all employees' (Company summit). Such behavior according to the GDPR is actionable.

These testimonies highlight a problem of awareness of one's roles and responsibilities, and of the consequences of non-compliance. Increasing employees' knowledge of the laws and regulations that affect their specific job role helps protect them and the organization from a range of damaging impacts such as personal fines, financial penalties, and loss of employment, to name but a few.

2.2 Results

Starting from an erroneous perception of the problem, the real challenge of external consultants was to change behaviors considered and perceived as correct by the staff as the result of a long process of action that has built up over time. In this sense, the consultants provided an alternative frame and the necessary support to define the necessary adaptation strategies and actions, stimulating people's awareness of the mistakes made by learning from them.

The approach was based on the identification of a sustainable path that was effectively commensurate with the specific needs of the organization. The path included several steps that ensured minimal adjustment in the short term (as per mandatory regulation), but at the same time became the basis for an evolutionary path aimed at developing full maturity on the Data Protection of corporate data (Fig. 1).

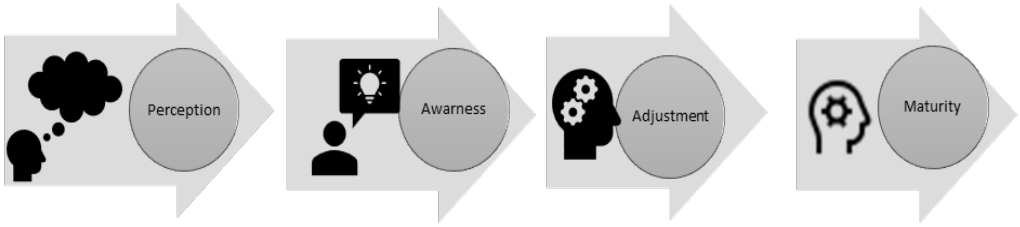

Figure 1: Process of prevention of unawareness unethical behavior

3. Perception

In the process of preventing unconscious unethical behavior, focus groups were evaluated as an adequate cognitive resource useful to collect data through group interaction. This technique allowed corporate counsellors and researchers to collectively elaborate the view of the phenomenon to be investigated and focus the debate on the topic in depth. It was preferred to use this tool to identify possible socialization processes and rationalization tactics. Taken together, rationalization and socialization practices allow perpetrators of wrong or unethical activities to believe they are behaving correctly, thus enabling them to continue to engage in these practices without questioning their compliance. Indeed, the focus group tool was used to build moments of active discussion with key officers and IT service provider of the company "XXX" to implement changes by identifying any problems and seeking new growth opportunities. Participants that were employees of "XXX", had to be convinced that compliant behavior was not an obstacle to operation. The evidence of such focus groups was verified through direct observation of behavior.

After an initial phase of sharing the analysis perspective, the focus groups focused on identifying errors and on correcting methods that could reduce the gap existing between the actual behaviors of the staff compared to those compliant with the GDPR. The role of moderator was assumed by the project leader, an external senior consultant, who urged, throughout the discussion, the participants to clarify as much as possible the meanings of the terms and expressions they use. In this way, the researchers collected it was possible to collect the many different meanings that are hidden behind the same term or expression.

3.1 Awareness

The phase highlighted a substantial discrepancy between the expected and actual behaviors. The discussion highlighted that often the behaviors that turned out to be wrong were assumed because they were perceived by all as organizational routines. To help develop awareness of cybersecurity among all employees of the company "XXX", a continuous training program was launched, to emphasize the contribution of IT security on the compliance. In addition to external regulations, internal regulations such as internal guidelines and operating instructions can also be relevant to adhering to compliance measures. In compliance with laws and regulations, the tool of the focus group brought to light the need to implement both technical and organizational measures. This is because technology is not always the cause of data loss; human behavior also plays a critical role.

3.2 Adjustment

At this point, the moderator asked for the contribution of all the participants (employees of 'XXX') for the drafting of an adjustment plan aimed at developing awareness of the potential consequences deriving from the assumption of incorrect (non-compliant) behavior. The adjustment phase generated a remediation plan or the implementation of the adjustment to the GDPR in terms of changes to organizational and technological models as well as to those of behavior. This plan considered lessons learned from mistakes, so in practical terms the unethical behavior of the employee who shared his username and password to colleagues in the office was recognized in the plan as an error not to be repeated.

3.3 Maturity

The last phase of the intervention involved the dissemination and sharing of a new wealth of organizational knowledge. The maturity phase corresponds to the follow up of the adjustment plan. The initial focus group has been transformed into a continuous improvement workgroup for the company "XXX" that mainly deals with defining the training needs of new hires and creating, in collaboration with the consultants, the so-called "training pills" lasting about 20 minutes, uploaded to the cloud. The employees themselves develop the content. As observed by an employee: "*It is better if a colleague explains certain topics to you than a superior or a consultant*". A monitoring system was also envisaged that made it possible to check whether all employees had taken advantage of the training pills. The key officers, on the other hand, with the collaboration of the consultants, contributed to defining the contents of the specialized training that is different from the role covered by each employee.

4. Conclusions

This manuscript contributes to the unethical behavior's literature focusing on unaware behavior and stressing the role of knowledge sharing behaviors on the process of learning from error within organizations.

Case study focused on the data protection that is multidimensional concept. It has a broad meaning and emphasizes a change of perspective: the underlying problem is not simply to be in possession of sensitive data, but to be able to manage them in the right way. It therefore places the emphasis on a process dimension rather than content. In fact, findings have shown that the expressions and concepts that emerged from the interviews, it's possible to detect signs of employee behavior in the management of sensitive data that was in some cases incorrect, in others unethical or fraudulent, and therefore punishable under the GDPR.

Findings case study has shown that communication and knowledge sharing played a central role within of process of prevention of unethical behavior. In fact, the perception and awareness phases were aimed to highlight the existing gap between the behaviors and actions in the cyber security field of the organization's personnel compared to those compliant with the GDPR.

In particular, the sensemaking process implemented by focus group allowed clarifying individual positions, according to a sharing and comparing procedure (Morgan, 1998), for leading to the definition and explanation of subjective meanings. Through this process, the members of the group assigned an area of semantic

correspondence and a specific meaning to the terms and expressions that become part of the discussion. But the most relevant aspect that emerged from the focus group was that before implementing any adaptation plan, a continuous training plan should be provided to help develop the awareness of all employees on cybersecurity through participation, commitment, and relevance. Organizations can create a culture of privacy by educating employees of the role they play in protecting assets and information. Thus, it's necessary a rethinking of the concepts of privacy and protection of personal data, as well as an organizational action that points to the development of a new culture of data in organizations. From an organizational point of view, there's a requirement to comply with the provisions of the regulation. The concept of compliance, however, is often understood by organizations in a static sense, as a best fit between regulatory requirements and organizational action at a given historical moment. However, to comply with the GDPR, organizations are required not only to ensure the implementation of rules and regulations, but also to encourage a set of virtuous behaviors and cultural changes that transform compliance tout court in a process of dynamic and incremental change. In fact, the remediation plan (adjustment phase's output) was realized through an approach "learning from error" and knowledge sharing behaviors, such as the continuous improvement workgroup has represented a useful starting point for improving internal organizational processes defining new practices that contribute to the development of a new and mature awareness on compliance issues.

References

Anand, V., Ashforth, B. E., & Joshi, M. (2004). *Business as usual: The acceptance and perpetuation of corruption in organizations.* Academy of Management Perspectives, 18(2), 39-53.

Asare, S. K., and Wright, A. (1995). "Normative and substantive expertise in multiple hypotheses evaluation". *Organizational Behavior and Human Decision Processes*, 64(2), 171-184.

Becker, B. A., Glanville, G., Iwashima, R., McDonnell, C., Goslin, K., and Mooney, C. (2016). "Effective compiler error message enhancement for novice programming students". *Computer Science Education*, 26(2-3), 148-175.

Becker, M. H. (1970). "Sociometric location and innovativeness: Reformulation and extension of the diffusion model". *American sociological review*, 267-282.

Bell, B. S., and Kozlowski, S. W. (2009). *"Toward a theory of learner-centered training design: An integrative framework of active learning". In Learning, training, and development in organizations* (pp. 283-320). Routledge.

Bell, B. S., and Kozlowski, S. W. (2011). "Collective failure: The emergence, consequences, and management of errors in teams". In Errors in organizations (pp. 128-156). *Routledge*.

Chow, C. W., Deng, F. J., and Ho, J. L. (2000). "The openness of knowledge sharing within organizations: A comparative study of the United States and the People's Republic of China." *Journal of Management Accounting Research*, 12(1), 65-95.

Edmondson, A. (1999). "Psychological safety and learning behavior in work teams". *Administrative science quarterly*, 44(2), 350-383.

Fidel, R. (1984). "The case study method: A case study". *Library and Information Science Research*, *6*(3), 273-288.

Frese, M. (1991). *Error management or error prevention: Two strategies to deal with errors in software design.*

Hofmann, D. A., and Frese, M. (Eds.). (2011). *Error in organizations. Routledge.*

Huy LV, Rowe F, Truex D, Huynh MQ (2012) "An empirical study of determinants of e-commerce adoption in SMEs in Vietnam an economy in transition". *J Glob Inf Manag 20(3):23–54*

Jones, T. M. (1991). "Ethical decision making by individuals in organizations: An issue-contingent model". *Academy of management review,* 16(2), 366-395.

Khorakian, A., and Sharifirad, M. S. (2019). "Integrating implicit leadership theories, leader–member exchange, self-efficacy, and attachment theory to predict job performance". *Psychological reports, 122(3), 1117-1144.*

Khorakian, A., Mohammadi Shahroodi, H., Jahangir, M., and Nikkhah Farkhani, Z. (2019). "Innovative work behavior in public organizations: The roles of ethical and knowledge sharing behaviors". *Creativity Research Journal*, 31(2), 164-173.

Kish-Gephart, J. J., Harrison, D. A., and Treviño, L. K. (2010). "Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work". *Journal of applied psychology, 95(1), 1.*

Ledva, G. S., Vrettos, E., Mastellone, S., Andersson, G., and Mathieu, J. L. (2017). "Managing communication delays and model error in demand response for frequency regulation". IEEE Transactions on Power Systems, 33(2), 1299-1308.

Lewicki, R. J., Poland, T., Minton, J. W., and Sheppard, B. H. (1997). *Dishonesty as deviance: A typology of workplace dishonesty and contributing factors. Elsevier Science/JAI Press.*

Lipshitz, R., Popper, M., and Friedman, V. J. (2002). "A multifacet model of organizational learning". *The journal of applied behavioral science,* 38(1), 78-98.

Longo, M., and Mura, M. (2011). "The effect of intellectual capital on employees' satisfaction and retention". *Information & Management, 48(7), 278-287.*

Morgan, D. L., and Krueger, R. A. (1998). *The focus group guidebook. Sage.*

Mura, M., Lettieri, E., Radaelli, G., and Spiller, N. (2013). "Promoting professionals' innovative behaviour through knowledge sharing: the moderating role of social capital". *Journal of Knowledge Management.*

Murphy, P. R., and Dacin, M. T. (2011). "Psychological pathways to fraud: Understanding and preventing fraud in organizations". *Journal of business ethics*, 101(4), 601-618.

Nonaka, I. (1994). "A dynamic theory of organizational knowledge creation". Organization Science, 5(1), 14–35.

Reason, J. (2000). "Human error: models and management". *Bmj, 320(7237), 768-770.*

Reischauer, G. (2015). "Combining artefact analysis, interview and participant observation to study the organizational sensemaking of knowledge-based innovation". Historical Social Research/Historische Sozialforschung, 279-298.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Sitkin, S. B. (1992). "Learning through failure: The strategy of small losses". *Research in organizational behavior, 14, 231-266.*

Stake, R. E. (1994). Case study: Composition and performance. Bulletin of the Council for Research in Music Education, 31-44.

Teigland, R., and Wasko, M. M. (2003). "Integrating knowledge through information trading: Examining the relationship between boundary spanning communication and individual performance". Decision Sciences, 34(2), 261-286.

Teigland, R., and Wasko, M. M. (2003). "Integrating knowledge through information trading: Examining the relationship between boundary spanning communication and individual performance". *Decision Sciences*, 34(2), 261-286.

Tsang, J. A. (2002). "Moral rationalization and the integration of situational factors and psychological processes in immoral behavior". *Review of General Psychology,* 6(1), 25-50.

Van Dyck, C., Frese, M., Baer, M., and Sonnentag, S. (2005). "Organizational error management culture and its impact on performance: a two-study replication". *Journal of applied psychology*, 90(6), 1228.

Van Dyck, C., Frese, M., Baer, M., and Sonnentag, S. (2005). "Organizational error management culture and its impact on performance: a two-study replication". *Journal of applied psychology,* 90(6), 1228.

Weiss, H. M., and Brief, A. P. (2001). "Affect at work: A historical perspective". *Emotions at work: Theory, research and applications in management, 133, 171.*

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). *Sage.*

Yu, C., Yu-Fang, T., and Yu-Cheh, C. (2013). "Knowledge Sharing, Organizational Climate, and Innovative Behavior: A Cross-Level Analysis of Effects". *Social Behavior and Personality: An International Journal,* 41(1), 143–156. http://doi.org/10.2224/sbp.2013.41.1.143

Zhao, B., and Olivera, F. (2006). "Error reporting in organizations". *Academy of Management Review,* 31(4), 1012-1030.