Winter 12-13-2018

Collective Deviance in IS

Gabriela Labres Mallmann
Federal University of Rio Grande do Sul

Andreas Eckhardt
German Graduate School of Management and Law

Antônio Carlos Gastaud Maçada
Federal University of Rio Grande do Sul

Collective Deviance in IS

Gabriela Labres Mallmann[1]
School of Management, Federal University of Rio Grande do Sul
Porto Alegre, Brazil

Andreas Eckhardt
German Graduate School of Management and Law (GGS)
Heilbronn, Germany

Antônio Carlos Gastaud Maçada
School of Management, Federal University of Rio Grande do Sul
Porto Alegre, Brazil

ABSTRACT

Scholars in social psychology and criminology have long argued that deviance is a group phenomenon. Based on the collective deviance literature, we aim to investigate the mechanisms behind deviant behaviors among people in groups, uncovering reasons for collective deviance within organizations. We are performing case studies among work groups (teams and departments) that commit deviances by interviewing employees and managers from those groups. Preliminary findings suggest that several deviances are committed by workgroups and, in most cases, the group's members are aware they are violating security policies, although their intention is to increase work performance. Furthermore, in some cases, the IT department knows about the deviance, but do not take action to try solving the issue. Understanding employees' behavior toward collective deviance can aid to cope with IS policy violations, providing new insights into policies development and strategies to mitigate such behaviors and increase information security.

Keywords: collective deviance, IS deviant behavior, information security, shadow IT.

[1] Corresponding author. gabilmallmann@gmail.com or gabriela.mallmann@ggs.de

INTRODUCTION

Groups of employees, such as teams or departments, are autonomously implementing and using technologies to perform their work tasks that deviate from IS security policies. A sales department, for example, implements Salesforce to be used by all employees in their daily activities and provide good services for clients and external partners. This implementation is led by the manager of the sales department, but without permission and support from the organizational IT department and violating IS security policies.

In decades of digitization, cases as the one described above have been recurrent in many companies. The massive development of technology has also brought several opportunities for deviant behavior in society and within organizations (Rogers et al. 2006). Not only technologies are widely available nowadays, but also individuals are able to autonomously find new solutions and exploit the functionalities it provides (e.g., Carter and Gruver 2015), leading to the use of unauthorized technologies in the workplace that violates security policies and threaten the organization (e.g., Haag and Eckhardt 2017). Thereby, it is essential to know what aspects lead to higher organizational compliance, but can be even more relevant to understand why people deviate from IS security policies. While there are many studies in the IS field on why people comply with IS policies (e.g., Bulgurcu et al. 2010) that are designed for protecting organizational IT assets, just a small number of articles investigate why people deviate or violate security policies, and even fewer studies take a group-level perspective to investigate deviance.

Studies in social psychology and criminology (e.g., Gardner and Steinberg 2005; McGloin and Piquero 2009; McGloin and Thomas 2016) have shown that most offense, misbehavior, deviance or even crime has been conducted in groups, referring to this phenomenon as collective deviance or co-offending. Taken that perspective to management research, we can

argue that the possibility of individual non-compliance is even more likely if an individual is part of a group, where all or at least a majority of the group members perform the same non-compliant action, such as using an information system that is not allowed by organizational IS policies, a phenomenon that some researchers label as shadow IT usage (e.g., Haag and Eckhardt 2017).

Considering the above arguments, the following research questions emerge: *How these group processes occur and why they lead to collective deviance*? This research aims, thus, to investigate the mechanisms behind the deviant behaviors among people in groups, uncovering reasons for collective deviance within organizations, which has not yet received sufficient attention in IS literature.

By understanding deviant behavior of employees within organizations, we can provide contributions for information security community. Investigating employees' behavior toward collective deviance can aid to cope with IS policy violations, providing new insights into policies development and strategies to mitigate such behaviors and increase information security.

COLLECTIVE DEVIANCE

Most studies on deviant behavior, or simply deviance, come from sociology, psychology and criminology literature. Deviance has been defined as conduct that violates social rules or norms, and a deviant then defined as a person who has engaged in such conduct, either habitually or occasionally (Wells 1978). Acts also can be considered deviant according to the reaction to them by others, which tend to compare a particular act with alternative behaviors to define if it is desirable or acceptable (Akers et al. 1979). Specific forms of deviant behavior can be crime, delinquency, drug addiction, suicide, etc.

The act of committing the deviance in groups has been referred as collective deviance or co-offending. Collective deviance or co-offending embraces the actual collective execution of an offense, that is, a violation of a law or rule, an illegal act (e.g., Weerman 2003). Studies have shown that being in a group can produce significant changes in behavior, including a tendency for people to demonstrate a shift toward risky or deviant behavior when in the presence of others (e.g., Gardner and Steinberg 2005; McGloin and Thomas 2016). In that sense, researchers have used group processes to understand and explain crime and other forms of deviance.

According to a model of collective behavior proposed by Granovetter's (1978), an individual's belief about whether an act will maximize his utility is conditional on the behavior of others, that is, others' actions serve as situational contingencies affecting decision-making. The subjective perceptions regarding rewards, informal social costs, and sanction risks vary under group conditions (McGloin and Thomas 2016). Moreover, an individual's decision to engage in a collective action depends in part on how many others participate in that action (Granovetter 1978; McGloin and Piquero 2009). Thus, the decision to participate in collective deviance may be conditional on the behavior of others because the anticipated experience of formal sanctions, social costs, and rewards are conditional on the individuals' behavior engaged on that deviant act (Gardner and Steinberg 2005; McGloin and Thomas 2016).

Introducing the concept of collective deviance in management and IS

Few studies on management field approach deviance as a group phenomenon. The concept of workplace deviance proposed by Robinson and Bennett (1995) can be insightful here. Those authors define employee workplace deviance as voluntary behavior that violates significant organizational norms and in so doing threatens the well-being of an organization and/or its members. They also highlight that the study of workplace deviance is distinct from the

study of ethics because in the first case the focus is on behavior that violates organizational norms, while the second case focus on behavior that is right or wrong when judged in terms of justice and law (Robinson and Bennett 1995). Therefore, although a certain behavior can be both deviant and unethical, the two qualities are not necessarily linked.

In the IS literature, most studies on deviance are from security and IS policy violation literature. Crossler et al. (2013), for instance, labeled as deviant behavior those acts that are intentional, such as sabotage, stealing, and industrial or political espionage, and those that are unintentional, are called misbehavior such as selecting a simple password or clicking on phishing links on emails. Siponen and Vance (2010), in turn, rely their analysis on the concept of Akers and Sellers (2004), also from criminology literature, to explain deviance as any deviant behavior that violates social norms, whether or not such behavior also violates the law. Here is taking into account the difference between deviant and unethical behavior (Robinson and Bennett, 1995).

Studies on security and IS policy violation discuss a wide range of deviances, such as using another person's password without authorization, using or writing a virus, sending confidential information unencrypted, using laptops carelessly outside of the company, among others (e.g., Siponen and Vance 2010). However, it is not only dishonest employees that try to commit computer crime or unmotivated employees who put security in risk by doing careless actions (e.g., Warkentin and Willison 2009) because the reasons and motivations behind deviance can be more complex, mainly when we consider a group of people acting together.

As discussed above, it is well documented that most misbehavior, deviance or even crime has been conducted in groups. In line with previous research in the social psychology and criminology (e.g., McGloin and Thomas 2016), we integrate the group deviance and collective

behavior literature to understand how group processes affect behavior in the IS field as a way to explain security deviant behavior, such as shadow IT usage, within organizations.

METHOD

Our method consists of an exploratory multiple case study based on a qualitative approach. A case study is a detailed and empirical investigation that considers the real context and multiple variables of a recent, broad, and complex phenomenon and it is useful when a holistic and in-depth investigation is needed (Yin 2009, Dubé and Paré 2003).

In order to obtain a rich set of data that captures the contextual complexity, we are performing interviews based on an interview guide with open questions among managers and employees of different work groups (teams or departments) from several companies that deviate from IS security policies. Notes and direct observation are also being considered to capture contextual relevant factors since a multiple data collection techniques and sources are important for data triangulation (Yin 2009). We defined a priori based on literature constructs and categories to ensure that important issues are not overlooked, and to guide the interpretation when conducting theory-building research (Dubé and Paré 2003).

FIRST INSIGHTS AND EXPECTED CONTRIBUTIONS

We are investigating two cases of security policies deviance from different companies so far, performing interviews with employees from these workgroups. The first case (C1) is a sales department leading by the manager of the department that implemented Salesforce with its own budget. C1 is from a large company from the publishing industry that operates in the national and international market. The organizational IT department is aware of the unauthorized tool used by the sales department. "*I use Salesforce to consolidate sales information and it is really useful for us (department). We know it does not have permission and support from the IT*

department so if we have a problem with the solution we have to solve by ourselves", said the respondent, who is a sales executive of the department.

The second case (C2) is a team of the marketing department that downloaded on company's devices Skype application to communicate with clients and external partners, including the manager of this team. C2 is from a multinational company from the IT industry that has rigorous IS security policy. The IT department is not aware of Skype usage, and the official technology they provide for communication does not meet the team's demands, according to the team's members. "*Many people that I have to communicate when performing my work tasks are externals, like clients and partners, and the instant communication would be impossible without Skype that is a common tool, everybody uses, and provides qualified resources*," said the respondent who is a marketing assistant in this team. To install the application on company's computers, they need admin rights, which should be provided by the IT department. However, the respondent did not know to answer how all employees from her team succeed when installing Skype. Although the company has strict security policies, the employees do not seem to be concerned with formal punishments from the organization. "*I need to talk very often with external people in my work, so I depend on Skype to do it faster*," argues the respondent. Perform work tasks and meet the goals seems to be more relevant to the team than any risk of punishment from their company.

Next steps we plan to expand the interviews by interviewing more employees from Case 1 and 2, as well as investigating more cases of collective deviance in other companies. We designed our investigation based on three primary elements. First, a person or people in the group that instigated the deviant act, seeking to understand how and who starts the deviance (e.g., Weerman 2003). Second, the perceptions of punishments, examining the influence of

formal punishments from organizations and the IT department compared to social punishment and informal social costs from group members, such as disapproval or exclusion (e.g., McGloin and Thomas 2016). Third, the role of the IT department regarding the deviance since some respondents reported that IT department knows about the deviant act.

To the best of our knowledge, this study is the first to investigate information security deviance as a group phenomenon, taking as a theoretical background the collective behavior and group deviance literature to explain work deviance in IS field. In that sense, we bring contributions to security community by investigating the collective deviant behavior of employees and providing new insights into policies development and strategies to cope with IS policy violations and increase information security within organizations (Warkentin and Willison 2009; Haag and Eckhardt 2017).

REFERENCES

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., and Radosevich, M. 1979. "Social learning and deviant behavior: A specific test of a general theory," American sociological review, pp. 636-655.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, (34:3), pp. 523-548.

Carter, M. and Grover, V. 2015. "Me, my self, and I (T): conceptualizing information technology identity and its implications". *Mis Quarterly*, (39:4), pp. 931-957.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research". *Computers & security*, 32, 90-101.

Dubé, L. and Paré, G. 2003. "Rigor in information systems positivist case research: Current practices, trends, and recommendations", MIS Quarterly, (27:4), pp. 597–636.

Gardner, M., and Steinberg, L. 2005. "Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study," Developmental psychology, (41:4), pp. 625.

Granovetter, M. 1978. "Threshold models of collective behavior". *American journal of sociology*, (83:6), pp. 1420-1443.

Haag, S., and Eckhardt, A. 2017. "Shadow IT," *Business & Information Systems Engineering*, pp. 1-5.

McGloin, J. M., and Piquero, A. R. 2009. "I Wasn't Alone: Collective Behaviour and Violent Delinquency," *Australian & New Zealand Journal of Criminolo*gy, (42:3), pp. 336-353.

McGloin, J., and Thomas, K. J. 2016. "Incentives for collective deviance: Group size and changes in perceived risk, cost, and reward," *Criminology*, (54:3), pp. 459-486.

Robinson, S. L., and Bennett, R. J. 1995. "A typology of deviant workplace behaviors: A multidimensional scaling study," *Academy of management journal*, (38:2), pp. 555-572.

Rogers, M., Smoak, N. D., and Liu, J. 2006. "Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis", *Deviant Behavior*, (27:3), pp. 245-268.

Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly*, pp. 487-502.

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

Weerman, F. M. 2003. "Co□offending as Social Exchange. Explaining Characteristics of Co□offending", *British journal of criminology*, (43:2), pp. 398-416.

Wells, L. E. 1978. "Theories of deviance and the self-concept," *Social psychology*, pp. 189-204.

Yin, R. K. 2009. "Case Study Research, Design and Methods," 4th edn. Sage Publications.