Issues in Information Systems
Volume 15, Issue II, pp. 185-189, 2014

INSIDER THREATS AND EMPLOYEE DEVIANCE: DEVELOPING AN UPDATED TYPOLOGY OF DEVIANT WORKPLACE BEHAVIORS

David Green, Governors State University, dgreen@govst.edu

ABSTRACT

Insiders are trusted individuals in an organization, such as current or former employees, contractors, consultants, or vendors (Keeney et al., 2005; Steele and Wargo, 2007). Insiders pose a threat to the security of information due to their intimate knowledge of an organization's internal operations, processes, data, systems, or other resources (Steele and Wargo, 2007). Because trusted individuals have the power to violate one or more rules in a security policy, an insider threat occurs either (1) through the violation of a security policy using legitimate access, and/or (2) through violation of an access control policy by obtaining unauthorized access (Bishop, 2005; Bishop and Gates, 2008).

Keywords: Insider threats, deviant workplace behavior

INTRODUCTION

Insiders are trusted individuals in an organization, such as current or former employees, contractors, consultants, or vendors (Keeney et al., 2005; Steele and Wargo, 2007). Insiders pose a threat to the security of information due to their intimate knowledge of an organization's internal operations, processes, data, systems, or other resources (Steele and Wargo, 2007). Because trusted individuals have the power to violate one or more rules in a security policy, an insider threat occurs either (1) through the violation of a security policy using legitimate access, and/or (2) through violation of an access control policy by obtaining unauthorized access (Bishop, 2005; Bishop and Gates, 2008).

Recommendations for organizations combating insider threats have focused on the development, enforcement, and communication of a wide variety of policies and procedures. In addition, technical controls are emphasized for both protection of systems, networks, and data, and for tracking and monitoring access, traffic, and system/data integrity (Keeney et al., 2005).

While research of insider threat is increasing (Warkentin and Willison, 2009), the existing body of workplace deviance literature has largely been ignored.

This paper builds on the work of Robinson and Bennett (1995) by proposing development of an updated typology of deviant workplace behaviors that includes information and communications technologies (ICT) based deviant behaviors that may not have existed or been common in the workplace during the period of the earlier study. The paper presents research in progress that uses multidimensional scaling techniques to determine (1) the underlying dimensions of deviant workplace behaviors, including both ICT and non-ICT based behaviors and (2) differences that may exist between the attributes of similar ICT and non-ICT based deviant workplace behaviors.

INSIDER THREATS

Negative work-related events, such as employment termination, demotion, or conflicts with coworkers or management, trigger most of insiders' attacks against an organization's systems, networks, and data (Keeney et al., 2005). The recommendations from the same study by CERT [1]and the Secret Service largely focus on identifying and intervening in the case of potential insider threats through a set policies and procedures. It is suggested that insiders' motives tied to negative work-related events may be eliminated or weakened through the efforts of management in all areas of the organization as well as the human resources department.

To protect against insider threats, managers should also attend to employees that have experienced a negative work event. Implementation of a formal grievance procedure and additional forums for employees to voice their concerns is also recommended (Keeney et al., 2005). Others have suggested employers be aware of the common personal characteristics of malicious insiders as a way to identify potential threats. Some of the personal characteristics of malicious insiders as a way to prevent attacks. Personal characteristics may include sense of entitlement; history of

[1] "CERT is not an acronym; it is a name and a registered service mark. ("CERT" an`d "CERT Coordination Center" are registered service marks of Carnegie Mellon University.) " http://www.cert.org/faq/ [Accessed July 8, 2014]

personal and social frustrations; computer dependency; ethical flexibility; reduced loyalty; and lack of empathy (Shaw, Post, and Ruby, 2002).

WORKPLACE DEVIANCE

Examples of incidents committed by insiders include any compromise, manipulation of, unauthorized access to, exceeding authorized access to, tampering with, or disabling of any information system, network, or data (Randazzo et al., 2004). Intentional incidents by insiders may be considered examples of workplace deviance. Workplace deviance is a "voluntary behavior that violates significant organizational norms and in so doing threatens the well-being of an organization, its members, or both" (Robinson and Bennett, 1995, p. 556). Workplace deviance typically focuses on employees, while insiders also include former employees, vendors, and contractors. Cyberdeviance has also been used to describe the specific examples of workplace deviance that include the category of counterproductive workplace behaviors involving misuse of information and communications technologies (Weatherbee and Kelloway, 2006).

It may be prudent to first attempt to operationalize workplace deviant behaviors that are ICT based. Workplace deviance may be a concept that is the same as or different than ICT based or "cyber" deviance, and those differences should be explored. An updated typology of workplace deviance may be necessary with the specific inclusion of ICT based deviant behaviors to determine if there are differences in the attributes for ICT and non-ICT based behaviors and allow for further research to be conducted using ICT based workplace deviance within the scope of non-ICT based deviance. Weatherbee (2010) developed conceptually modeled typology for cyberdeviant workplace behaviors based on Robinson and Bennett (1995) but notes that a "theoretical model is also needed for the purposes of establishing construct validity and for empirically testing a nomological network (p. 40)."

This study proposes using multidimensional scaling techniques to determine (1) the underlying dimensions of deviant workplace behaviors, including both ICT and non-ICT based behaviors and (2) differences in attributes that may exist between similar ICT and non-ICT based deviant workplace behaviors.

Attributes of Deviant Workplace Behaviors

According to Bordia et al., (2008) an incidence of workplace deviance may be considered major or minor, a measure of the behavior's seriousness. Seriousness was one of the six top attributes identified as part of the development of the original non-ICT based workplace deviant typology in addition to the level of harm to individuals, level of harm to the organization, ethicality, intentionality, and covertness or the behavior (Robinson and Bennett, 1995). Based on those attributes it may be useful to explore whether there are difference in the perception of workplace deviant behaviors that involve information and communications technologies (ICT) and those that do not involve ICT. Some attribute specific research questions include:

- Is there a difference in the perception of *seriousness* of non-ICT based workplace deviant behaviors and those that are ICT-based?
- Is there a difference in the perception of *harm to individuals* for non-ICT based workplace deviant behaviors and those that are ICT?
- Is there a difference in the perception of *harm to the organization* for non-ICT based workplace deviant behaviors and those that are ICT-based?
- Is there a difference in the perception of *ethicality* of non-ICT based workplace deviant behaviors and those that are ICT-based?
- Is there a difference in the perception of *intentionality* of non-ICT based workplace deviant behaviors and those that are ICT-based?
- Is there a difference in the perception of *covertness* of workplace deviant behaviors that involve information and communications technologies (ICT) and those that do not involve ICT?

METHODS AND EXPECTED RESULTS

Robinson and Bennett developed a typology of deviant workplace behavior (1995) using a multi-phase multidimensional scaling study. The original typology from the Robinson and Bennett study is shown in Figure 1.

Multidimensional scaling allows a researcher to produce a typology using perceptions of individuals. More specifically, multidimensional scaling (MDS) techniques can infer the underlying dimensions using a series of similarity or preference judgments about the objects provided by respondents as well as the number and relative importance of the dimensions respondents use when evaluating objects. In addition, MDS may also display how objects are related perceptually on the underlying dimensions (Hair et al., 2010).

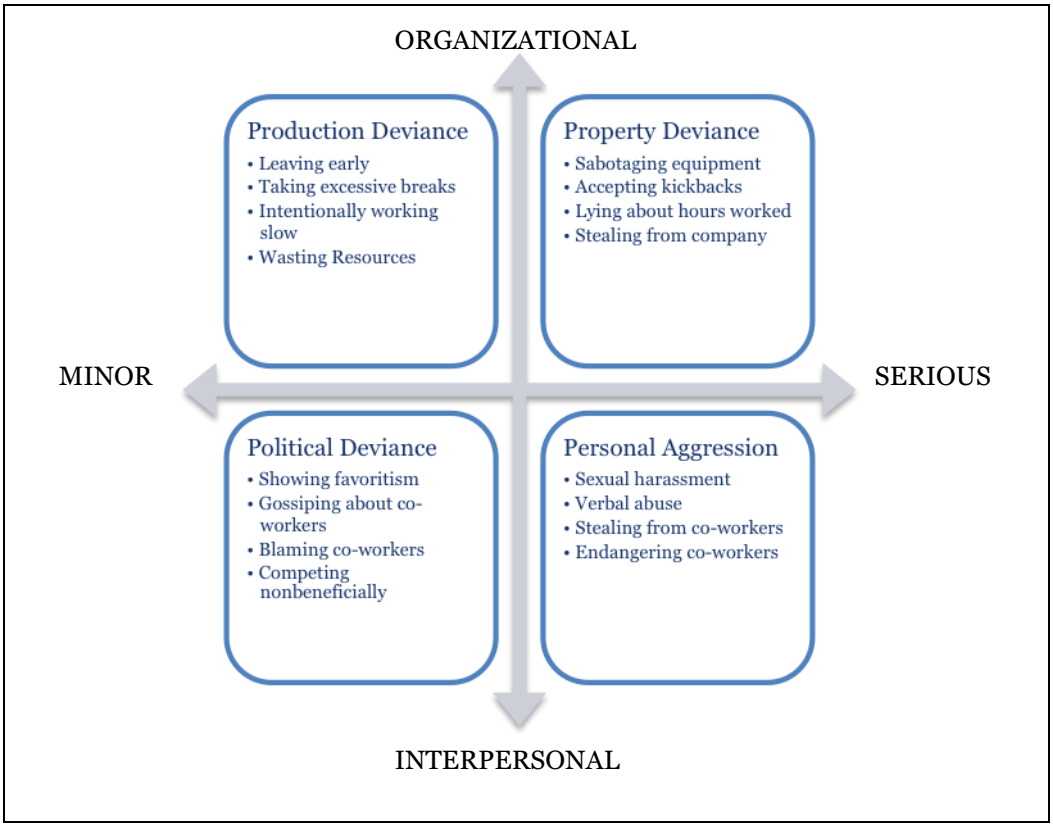

Figure 1. Typology of Deviant Workplace Behavior (Robinson and Bennett, 1995)

Phase 1 – Developing a Pool of Employee Deviant Behaviors

A sample of full-time working adult participants, including IT staff from a company, managers from an organization, and students from a part-time MBA program in the US. Approximately 100 participants will be solicited.

Based on the wording from the Robinson and Bennett (1995) study, participants will first be asked to describe two incidents of "someone at work engaging in something considered to be deviant, i.e., something that is considered to be wrong." Second, the participants will be asked to describe two incidents of "someone at work engaging in something considered to be deviant (i.e., something that is considered to be wrong specifically involving a computer, system, data, or network)." The two categories may be considered ICT based and non-ICT based workplace deviant behaviors. Third, the participants will be asked to define deviance in their own words. Demographic data such as gender, age, years of work experience, and level of technical expertise will be collected.

Once a list of workplace deviant behaviors is compiled, two researchers will independently consolidate, rephrase, and attempt to simplify the responses to ensure the behaviors could apply to a variety of organizations, industries, and positions. The researchers will also categorize the behaviors as ICT based or non-ICT based. Once the list of deviant behaviors is developed by the researchers, a panel of judges (i.e., management and information systems professors) will assess whether each behavior fits the definition of employee deviance and match specific non-ICT based workplace deviant behaviors that may be comparable to ICT based workplace deviant behaviors.

Phase 2 – Similarity Rating and Dimensions

A sample of 200 full-time working adult participants from a part-time MBA program in the US will be solicited to complete a survey that contains the list of non-ICT and ICT based workplace deviant behaviors along with a brief description of a target behavior. The participants will be asked to rate each deviant behavior in terms of similarity to the target behavior, using a nine-point Likert-type scale (1=very similar, 9=very different).

MDS typically involves participants comparing every possible combination of stimuli [n(n-1)/2]. If the number of comparable deviant behaviors from Phase 1 is too great, the participants may be given a random subset of stimuli (Thompson, 1983).

Phase 3 – Attribute Analysis for Labeling Dimensions

A separate sample of 200 full-time working adult participants from a part-time MBA program in the US, will rate of each of non-ICT and ICT based workplace deviant behaviors on the basis of six attributes. The attributes are taken from the Robinson and Bennett (1995) study and include five-point bipolar scales with attribute anchors of unintentional/intentional, not serious/serious, not harmful to company/ harmful to company, not harmful to individuals/harmful to individuals, very unethical/ethical, and covert/overt.

A multiple regression will be performed to measure the relationship with the attributes and the dimension configuration from the result of the MDS. The labels will be chosen based on the multiple correlation coefficients, F-values, and beta weights from the regression analysis (Kruskal and Wish, 1978).

Expected Results and Future Directions

The proposed research is expected to develop an updated typology of deviant workplace behaviors that includes ICT based deviant behaviors, using multidimensional scaling techniques.

The updated typology and determining the underlying dimensions of workplace deviant behaviors, including ICT based behaviors, will provide empirically supported constructs that will provide researchers with a basis to explore additional factors tied to workplace deviance, cyberdeviance, and insider threats in addition to examining antecedents.

One antecedent of workplace deviance is perceived psychological breach, which is positively related to workplace deviance (Bordia et al., 2008). A psychological contract is a "set of beliefs involving terms and exchange agreement between the employee and his or her employing organization" and "exists in the eye of the beholder" (Rousseu, 1995; Bordia et al., 2008). The psychological contract is based on the perceived understanding of employer obligations of the employer, and a breach of the psychological contract takes place when "one party in a relationship perceives that the other party has neglected to fulfill what has been committed or promised" (Rousseau, 1995). Social exchange theory predicts that an employee responds to perceived psychological breach in negative ways (Rousseau, 1995; Bordia et al., 2008) and shown to have a positive relationship with workplace deviance. Future research may address whether actions on the part of management, that may constitute psychological breach from the employee's perspective, result in ICT or non-ICT based workplace deviant behaviors, and would either type of deviant behavior be preventable and identified well in advance.

Situational employee scenarios may be examined to determine whether employees are more likely to behave in a deviant way using ICT or in a non-ICT way. For example, consider the scenario where an employee is aware, directly or indirectly, that management may soon fire them or lay them off. If the employer is attempting to find a way to fire the employee, the employee may become aware of the attempt directly through specific comments or action by management or indirectly based on inaction or behavior of management or co-workers. In a different, but related, scenario an employee may know they will be laid off days, weeks, or months before it happens. In some cases, the soon-to-be laid-off employee may even be asked to train a new employee as part of his or her remaining duties. In some cases the employee may be asked to train his/her own replacement.

Whether the cause for termination is justified or not, the employee may experience a range of emotions and stress that may make them consider acts of revenge and eventually deviant behavior. Future research may address whether ICT based deviant behavior more likely because of specific attributes, such as being perceived as less serious or more easily disguised than other acts of workplace deviance. In addition other theories such as justice theory

(Aquinas, et al., 1999) and variables from leader-member exchange theory may be applied to a current typology of workplace deviant behaviors that are both non-ICT and ICT based.

REFERENCES

Aquinas, K., Lesis, M.U., and Bradfield, M. 1999. "Justice constructs negative affectivity, and employee deviance: A proposed model and empirical test," *Journal of Organizational Behavior (*20), pp. 1073-1091.

Bishop, M. 2005. "Insider is Relative," in *Proceedings of the New Security Paradigms Workshop*, Nova Scotia, Canada.

Bishop, M., and Gates, C. 2008. "Defining the Insider Threat," in *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, Oak Ridge, Tennessee.

Bordia, P., Restubog, S., and Tang, R. 2008. "When employees strike back: Investigating mediating mechanisms between psychological contract breach and workplace deviance," *Journal of Applied Psychology* (93:5), pp. 1104-1117.

Dulac, T., Coyle-Shapiro, J. A-M., Henderson, D., and Wayne, S. 2008. "Not All Responses to Breach are the Same: A Longitudinal Study Examining the Interconnection of Social Exchange and Psychological Contract Processes in Organizations," *Academy of Management Journal* (51:6), pp. 1079-1098

Hair, J.F., Black, W.C., Babin, B.J., and Anderson, R.E. 2010. *Multivariate data analysis*, Upper Saddle River, NJ: Pearson Education.

Keeney, M. M., Kowalski., E.F., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. 2005. "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," National Threat Assessment Center, U.S. Secret Service, and CERT® Coordination Center/Software Engineering Institute, Carnegie Mellon, pp.21-34. Retrieved http://www.cert.org/archive/pdf/insidercross051105.pdf on February 10, 2009.

Kruskal, K.B., and Wish, M. 1978. *Multi-dimensional Scaling* in Sage University paper series on Quantitative Applications in the Social Sciences, 07-011. Beverly Hills and London: Sage.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. 2004. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," National Threat Assessment Center, U.S. Secret Service, and CERT® Coordination Center/Software Engineering Institute, Carnegie Mellon, August 2004. http://www.secretservice.gov/ntac/its_report_040820.pdf

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.

Shaw, E.D., Post, J.M., and Ruby, K.G. 2002. "Inside the Mind of the Insider" SecurityManagement.com.

Rousseau, D.M. 1995. *Psychological contracts in organizations: Understanding written and unwritten agreements*, Thousand Oaks, CA: Sage.

Steele, S., Wargo, C. 2007. "An Introduction to Insider Threat Management," *Information Systems Security* (16), pp. 23–33.

Thompson, P. 1983. "Some missing data patterns for multidimensional scaling," *Applied Psychological Measurement* (7), pp. 45-55.

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

Weatherbee, T.G. 2010. "Counterproductive use of technology at work: Information and communications technologies and cyberdeviancy," *Human Resource Management Review* (20), pp. 35-44.

Weatherbee, T.G., and Kelloway, E.K. 2006. "A case of cyberdeviancy: CyberAgression in the workplace," in *Handbook of Workplace Violence*, E.K. Kelloway, J. Barling, and J.J. Hurrell (eds.), Thousand Oaks, CA: Sage Publications, Inc., pp. 445-487.