When Deviant Behavior In The Workplace Gets Technical

Gladys Torres-Baumgarten, (Email: gbaumgar@kean.edu), Kean University
Elizabeth A. McCrea, (Email: e.mccrea@att.net), Seton Hall University

ABSTRACT

Workplace deviant behavior typologies typically include absenteeism, theft, incivility and violence. Three recent case studies are reviewed that indicate computer sabotage should be added to these classifications.

INTRODUCTION

This paper reviews and extends the research on workplace deviance. Specifically, it focuses on a type of deviant behavior in the workplace that has been largely overlooked by researchers to date - computer systems sabotage. We propose that, given the central and strategic nature of information resources, computer sabotage needs to be incorporated into the typologies of deviant behavior.

One of the most frequently cited typologies of deviant behavior in the workplace was devised by Robinson & Bennett (1995). The authors defined workplace deviance as "voluntary behavior that violates significant organizational norms and, in so doing, threatens the well-being of the organization or its members, or both." They found that two dimensions were useful in describing workplace deviance: degree of severity (severe vs. minor), and interpersonal vs. organizational. Robinson & Bennett defined interpersonal deviance as deviance that was targeted at individuals or members of an organization, while organizational deviance was deviance that is targeted at the organization. Robinson & Bennett argued that the distinction between interpersonal and organizational deviance is an important one because the type of individual that is prone to deviance against individuals in the workplace differs from one prone to organizational deviance. Bennett & Robinson's interpersonal vs. organizational deviance distinction was consistent with other work that has also conceptualized deviance based on its intended targets (Baron & Neuman, 1996; Giacalone & Greenberg, 1997; Skarlicki & Folger, 1997 as reported in Bennett & Robinson, 2000). A 2007 study conducted by Berry, Ones & Sackett, however, questions the separability of interpersonal vs. organizational deviance since they found that these two forms of deviance were highly correlated.

Based on these two dimensions, Robinson & Bennett identified four typologies (or 'families') of workplace deviance: 1) *production deviance* (includes such things as calling in sick when not; making personal calls while at work; wasting resources, etc.); 2) *property deviance* (includes things such as stealing from the organizations, misusing discount privileges, covering up mistakes, accepting kickbacks, sabotaging equipment, etc.); 3) *political deviance* (includes uncivil behavior, blaming others for one's own mistakes, starting negative rumors, spreading gossip, boss asking employees to work in ways beyond what is indicated in their job description); and 4) *personal aggression* (includes physical and verbal aggression, sexual harassment, etc.).

At first glance, information system sabotage seems to be a subset of property deviance. However, we argue here that, in today's knowledge economy, intentional damage to information systems is qualitatively different than deliberately damaging a photocopying machine or even a production machine. While causing damage to a piece of equipment can be a significant hardship and may impact a company's current financial bottom-line, destroying a firm's knowledge resources can have much more far-reaching implications to not only the firm but its stakeholders as well. It also can have strategic implications, by destroying the source of the firm's competitive advantage.

On a related issue, management scholars have argued that organizational behavior's traditional focus on the positive outcomes and contributions that employees make should be complemented with a similar emphasis on how to manage "problem" employees (i.e. those that misbehave), a source of even greater concern among managers (Vardi and Weitz 2004). Employees may become "problem employees" when they are frustrated, feel slighted by the company or have experienced a perceived injustice in the workplace. There is ample research, largely from the field of psychology, where the mediating role of emotions in fostering workplace deviance has been the focus (Barclay, Skarlicki and Pugh 2005). However, not all troubled employees choose to take revenge (or misbehave) against the organization or against specific individuals within the organization (Aquino, Tripp & Bies 2001 and 2006). Workplace deviance and the factors leading to it need to be better understood so as to minimize the adverse effects to the organization, stakeholder groups or other individuals.

Workplace deviance is an insidious and costly problem for organizations. It is estimated that the annual cost of workplace deviance in the U.S. alone resulting from workplace violence is as high as $4.2 billion per year (Bensimon 1994); $40 to $120 billion for theft (Buss 1993; Camara and Schneider 1994) and $6 to $200 billion for a wide range of other organizational misbehaviors (Murphy 1993).

Estimates on the cost of computer crime committed by employees, however, are very difficult to gauge. The difficulty arises because a large portion of insider-related security breaches are not reported by IT professionals (More 2007). Furthermore, the cost of these actions is difficult to measure because of the multi-dimensionality of cost in the case of systems sabotage: the actual/opportunity cost to the firm in the form of lost revenue, the potential loss of customer and employee confidence in the firm's operations; the damage to the firm's competitive advantage and the human cost, if people are put at risk because vital data has been destroyed.

ILLUSTRATIVE CASES

Three cases are used to illustrate how damaging computer sabotage can be to an organization and its various stakeholders. Computer sabotage is generally undertaken by network administrators who have felt that an injustice has been committed toward them in the workplace. In each of the three cases, a logic bomb was the preferred mode of computer sabotage. Logic bombs are simply additional lines of computer code, generally written by disgruntled IT personnel such as network administrators and inserted in an organization's existing computer code with the intention to cause serious harm to its computer systems. While a virus can result in similar damage, logic bombs differ from these in two key respects. Viruses are often released from an unknown, remote location with numerous, unidentifiable targets. Logic bombs, on the other hand, are knowingly and maliciously inserted into the computer code, generally by an insider (i.e. employee), triggered by an event (such as the dismissal of that disgruntled employee) and have one specific target (the employer's computer system). As a result, while viruses and logic bombs can yield similar end results (i.e., inflicting serious harm to company computer systems), their execution differs widely. Companies are generally concerned enough with the former that they spend considerable sums to protect their computer systems from hackers and computer viruses. However, the threat that insiders pose is taken into account less often. As the cases outlined below illustrate, in some instances, employees can pose an even more significant threat to the computer systems and ultimately, to a company's viability.

Case #1 - Omega Engineering Inc.

Omega Engineering, Inc. is an established, privately-held corporation headquartered in the United States. The firm is a global leader in process management and control. It designs and manufactures devices that regulate temperature, pressure, humidity, pH, conductivity, strain, force and flow. "Omega also provides customers with a complete line of data acquisition, electric heating and custom engineered products" (Omega website). Omega counts among its regular customers such impressive organizations as NASA, the U.S. Navy, McDonnell Douglas, Intel and the 3M Corporation.

One of the keys to Omega's success is its sophisticated, flexible, computer controlled production equipment located in its New Jersey, USA plant. Most machines in the plant are capable of making a wide range of products, simply by changing computer instructions. Ralph Michel, the company's Chief Financial Officer has been quoted as stating that, "the programs and code generators [allow] the company to manufacture 25,000 different products and to customize those basic products into as many as 500,000 different designs" (Gaudin, 2000a). However, without these programs—created through decades of design, engineering and programming work—the production equipment is virtually useless.

On July 31, 1996 the unthinkable happened: at the start of the first shift, when machinists tried to bring up new programs for their production machines, "all of the plant's tooling and manufacturing programs were gone" (Gaudin, 2000a). When the plant manager, went to get the backup tapes, they, too, were missing. By the time the nightmare ended, idle production workers had to be laid off while Omega Engineering had to recreate the programs that had been lost—at a cost of over $2 million. In the meantime, frustrated customers began taking their business elsewhere, resulting in an estimated $10 million in lost sales revenue (Gaudin, 2000a).

After a lengthy and complicated investigation that included cutting-edge computer forensics, the United States Secret Service determined that the devastating system crash was neither an accident nor the result of a computer malfunction. Rather, the programs' deletion had been a deliberate act. The server had been intentionally sabotaged, and the evidence pointed to Timothy Lloyd, a former employee, as the perpetrator.

Timothy Lloyd was hired by Omega Engineering in 1984 as a machinist at the New Jersey plant. Over the years, he was given increasing levels of responsibility and, when the decision was made to centralize all the production programs on the various machines onto a central computer server, Lloyd was selected to head the project. As a result, he had complete access to everything on the server and he alone was in charge of maintaining the system and backing up the computer files. Since he was a long-time, trusted employee, and because few managers in the plant fully understood the central Novel computer server, he was subjected to very little supervisory oversight in this area of his responsibilities.

In late 1994 his relationships with several fellow employees began to deteriorate. At his trial, "witnesses testified that he repeatedly elbowed, shoved and bumped colleagues in the hallways, and that he became verbally abusive" (United States of America v. Timothy Lloyd, 2001: p.2). He was also accused of "knowingly running faulty designs to make co-workers look bad and bottlenecking a project because he wasn't in charge" (Gaudin, 2000a).

In response to Lloyd's behavior, Omega managers followed a fairly standard progressive discipline procedure: first they warned Lloyd verbally; then they progressed to formal, written reprimands which were entered into his personnel file (Gaudin, 2000b); finally they transferred him to a non-supervisory position in another department. However, since maintaining the server did not involve managing other people, he was left in charge of the centralized computer system.

Despite the disciplinary actions, Lloyd's behavior did not improve, and in early July 1996, he had yet another altercation with colleagues. Eventually, the Human Resources Director at the manufacturing facility, decided that he had to terminate Lloyd, "due to his longstanding interpersonal problems and the repeated incidents of physical intimidation" (United States of America v. Timothy Lloyd, 2001: p. 1).

Several months before he was fired, however, computer forensic evidence indicated that Lloyd tested a "logic-bomb" program that would wipe out all the machine control programs. After making sure the logic-bomb would work, he left the embedded software on the system—if he was there to re-set the trigger date then the program would not run and everything would be fine. But if he was terminated, as he apparently anticipated, he would not be there to abort the command to completely erase the computer system, and all the programs would be destroyed.

In the end, a jury convicted Timothy Lloyd of computer sabotage on May 12, 2000. Several appeals followed, but eventually he was sentenced to "to 41 months of imprisonment and fined $2,043,394 in restitution damages" (Lloyd v. United States of America, 2005).

Case #2 - UBS

UBS Paine Webber is a global financial services firm headquartered in Switzerland, with extensive operations in the U.S. In February 2002, Roger Duronio, a UBS network administrator at one of UBS's offices in New Jersey, U.S. who had become increasingly dissatisfied with his salary and bonuses, resigned from his current post. However, before resigning, he devised a scheme whereby he stood to profit if UBS computer systems were rendered inoperative through the detonation of a logic bomb. Duronio then purchased over $23,000 in put option contracts for UBS stock, gambling on the fact that if a logic bomb were to cripple the company, that its stock price would decline, and he (Duronio) would more than recover his initial $23,000 investment. Duronio proceeded to embed a logic bomb into existing UBS computer code prior to his departure that resulted in the loss of critical files when the logic bomb detonated on March 4, 2002. The malicious code had been designed to delete data from over 1,000 computers (out of 1,500 in the "network") across branch offices and to prevent backed up data from running. Despite the damage to UBS systems, UBS's stock price remained stable following the logic bomb's detonation.

Not only did Duronio, 64, lose his $23,000 investment, but in December 2006, he was also sentenced to eight years in prison and more than $3 million in restitution to UBS for planting the logic bomb in its computer network. (Reuters; December 14, 2006)

Case #3 – Medco Health Solutions Inc.

Medco is a New Jersey based company that works with pharmacies to ensure that newly prescribed prescription drugs do not have any harmful or adverse interactions for individual patients. It maintains a key database known as the Drug Utilization Review, or DUR, and it lists all the medications that individual patients currently take. The DUR is used by pharmacies and physicians to identify the potential for dangerous drug interactions.

In December 2006, one of Medco's IT systems administrators, Andy Lin, 50, was charged with planting a logic bomb into the company's computer systems with the intent to damage over 70 Medco servers (Weiss 2006). One of the targeted databases was the DUR (outlined above). The deletion of this database would have clearly been devastating to Medco and its direct clients, the pharmacies and physicians it serves. More importantly, however, this logic bomb would have placed significant numbers of patients at great risk of potentially harmful drug interactions. Additional databases were also intended targets for the logic bomb, including some containing information on new prescription drugs as well as other billing/financial applications.

The significance of these databases did not dissuade Anthony Lin from intending to cause harm to Medco's computer systems. Lin's intentions were motivated out of concern that his position would be terminated. (Medco had been spun off from the pharmaceutical giant, Merck & Co. and recent consolidation within the company had led Lin to fear losing his job.) Over a period of a year and a half, Lin is alleged to have inserted the destructive code into Medco's computer systems, modified it, set a deployment date (which did not work), corrected it and reset the deployment date for April 2005. However, before the logic bomb was detonated, it was uncovered in January 2005 by another systems administrator looking into an unrelated systems error. The logic bomb was deleted by security officers and it never caused the damage allegedly intended by Lin. Given the recent indictment, this case has not gone to court yet, but the two counts of unauthorized changes to the company computer systems can each be punishable by up to 10 years in prison and a $250,000 fine (Weiss 2006).

CONCLUSION

These cases illustrate the wide-reaching impacts computer sabotage, especially logic bombs, can have on multiple stakeholders: from production workers at Omega to patients requiring Medco's input on drug interactions; from UBS Paine Webber shareholders to customers in all three cases. Given the fundamental nature of information resources to companies' competitive advantage in today's knowledge economy, subsuming computer sabotage under the umbrella of "property deviance" underemphasizes its importance. As a result, firms do not devote enough resources to protecting themselves from the threat from inside. Instead, external threats—which have received much more attention in both the popular and academic literature—garner the most attention. Therefore, despite the fact that organizations' competitiveness – and viability - are threatened by the potential actions of disgruntled or troubled systems administrators, the companies often fail to take the necessary steps that would increase oversight of their systems personnel, and protect their computer systems. The increased frequency of logic bombs suggests that companies need to be equally concerned (and equally willing to spend money) to guard against these insider threats.

REFERENCES

1. Anonymous, (2006). Logic bomb backfires on hacker. Reuters. December 14.
2. Aquino, K., Tripp, T.M. & Bies, R.J. (2001). How employees respond to personal offense: The effects of blame attribution, victim status, and offender status on revenge and reconciliation in the workplace. *Journal of Applied Psychology*. 86 (1): 52-59.
3. Aquino, K., Tripp, T.M. & Bies, R.J. (2006). Getting even or moving on? Power, procedural justice, and types of offense as predictors of revenge, forgiveness, reconciliation and avoidance in organizations. *Journal of Applied Psychology*. 91 (3): 653-668.
4. Barclay, L., Skarlicki, D., & Pugh, D. (2005). Exploring the role of emotions in injustice perceptions and retaliation. *Journal of Applied Psychology*. 90 (4): 629-643.
5. Baron, R.A., & Neuman, J.H. (1996). Workplace violence and workplace aggression: Evidence on their relative frequency and potential causes. *Aggressive Behavior*. 22: 161-173.
6. Bennett, R. & Robinson, S. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology*. 85 (3): 349-360.
7. Bensimon, H.F. (1994). Crisis and disaster management: Violations in the workplace. *Training and Development*. 28, 27-32.
8. Berry, C.M., Ones, D., & Sackett, P. (2007) Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology*. 92 (2): 410-424.
9. Buss, D. (1993). Ways to curtail employee theft. *Nation's Business*, pp. 36, 38.
10. Camara, W.J. & Schneider, D.L. (1994). Integrity tests: Facts and unresolved issues. *American Psychologist*. 49: 112-119.
11. Gaudin, S. (2000). Case study of insider sabotage: The Tim Lloyd/Omega case, *Computer Security Journal*, XVI (3). November 3. p.4
12. Gaudin, S. (Web posted June 27, 2000 at 11:01 a.m.). The Omega files: A true story, *Network World Fusion* (an IDG.net site)
13. Giacalone, R.A. & Greenberg, J. (1997). *Antisocial behavior in organizations*. Thousand Oaks, CA : Sage
14. http://www.howstuffworks.com/framed.htm?parent=logicbomb.htm&url=http://australianit.news.com.au/articles/0,7204,20925927%5E15306,00.html
15. http://www.Omega.com/info.html (accessed 9/11/05)
16. More, L. (2007). The threat from within: Internal fraud is on the rise and IT organizations must be prepared to address the problem. *Computing*. April 17.
17. Murphy, K.R. (1993) *Honesty in the workplace*. Belmont, CA: Brooks/Cole.
18. Robinson, S., & Bennett, R. (1995). A typology of deviant workplace behaviors: A multi-dimensional scaling study. *Academy of Management Journal*. 38: 555-572.
19. Skarlicki, D.P., & Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural and interactional justice. *Journal of Applied Psychology*. 82. 416- 425.
20. Timothy Lloyd, Petitioner, v. United States of America, Respondent. Civ. No. 03-813(WHW). United States District Court for the District of New Jersey; 2005; U.S. Dist. LEXIS 18158; August 15, 2005, Decided; August 16, 2005, Filed
21. United States of America, Appellant v. Timothy Lloyd, No. 00-2409 United States Court of Appeals for the Third Circuit 269 F.3d 228; U.S. App. LEXIS 2177; April 19, 2001 Argued; October 12, 2001 Filed.
22. Vardi Y. & Weitz, E. (2004) *Misbehavior in Organization: Theory, Research and Management*. Lawrence Erlbaum Associates. 337 pp.
23. Weiss**,** T.R. (December 20, 2006). Man indicted for planting 'logic bomb' in company's IT systems.*Computerworld*. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006361&intsrc=hm_l

NOTES