© *Academy of Management Perspectives*
2013, Vol. 27, No. 1
Online only
http://dx.doi.org/10.5465/amp.2013.0026

RESEARCH BRIEFS

BAD EMPLOYEES OR BAD POLICIES: WHAT CAN ORGANIZATIONS DO TO STOP MISUSE OF INFORMATION TECHNOLOGY RESOURCES?

ALEXANDER T. JACKSON AND SATORIS S. CULBERTSON
Kansas State University

RESEARCH QUESTIONS

Many organizations today must grapple with employees spending time browsing Facebook, tweeting, or sending personal emails, and management is keen to find ways to discourage such misuse of company technology. Do formal sanctions work the best, or do employees respond better to informal sanctions, such as feeling guilty and experiencing disapproval from peers? Also, are some people (telecommuters, for example) more likely than others to abuse technology?

These questions were the focus of a recent study by John D'Arcy (University of Delaware) and Sarv Devaraj (University of Notre Dame) looking at the risks organizations face, including damage to the company's image, reduced stock prices, and decreased productivity, when employees misuse company technology.

D'Arcy and Devaraj explored how organizations might prevent such incidents by examining what types of sanctions best prevent employees from misusing technology. They proposed that the certainty and severity of formal sanctions, along with the informal consequences of social pressure and the employee's moral beliefs, would be associated with less technology misuse, arguing that employees' need for social approval and desire to avoid feeling shame or guilt would prevent them from engaging in inappropriate technology behaviors.

The study also investigated whether misuse of technology is associated with different organizational contexts, including an employee's virtual status and his or her level within the organization. This is particularly topical given that an increasing number of employees are working remotely.

In addition, they examined the employee's level within the organizational hierarchy. An individual's role in an organization is shaped by others' expectations, social norms, and organizational policy. For example, managerial roles are shaped by responsibilities to stakeholders and the moral responsibility associated with being a manager. These responsibilities may make managers less likely to misuse company technology.

In conducting their study, D'Arcy and Devaraj set out to formally test a contemporary deterrence theory model. Classical deterrence theory argues that people are rational and try to maximize their rewards while minimizing their costs. In other words, penalties (such as fines or imprisonment) that are certain and severe enough tend to dissuade people from engaging in inappropriate and illicit behaviors. However, classical deterrence theory does not address informal penalties or sanctions, especially in the context of technology misuse. Although digital and software piracy researchers have begun to examine the role of informal sanctions, the findings are mixed. According to the authors, this may be because previous researchers have poorly defined and measured sanctions and behaviors. And while researchers have also shown that personal characteristics and situational factors (e.g., self-control and ethical orientation) predict piracy behaviors, important gaps remain in the literature. As such, D'Arcy and Devaraj attempted to fill these gaps by examining the added value of incorporating informal sanctions, managerial level, and virtual status into deterrence theory.

STUDY DESIGN AND METHOD

To examine how to best prevent technology misuse and the contexts under which technology misuse occurs, D'Arcy and Devaraj used surveys to obtain data from 411 employed adults across seven industries (roughly 23% were managers). These employees were presented with four technology misuse scenarios. Each scenario portrayed an employee misusing technology, including sending an inappropriate email, using unlicensed software, accessing data without proper authorization, and modifying data without proper authorization. For example, in one scenario, "Jordan" is given a personal computer on which he can do his work. However, he is missing some software that is needed. Because the company will not purchase the software, he decides to download an unlicensed version of the software.

After reading the scenarios, the participants then answered questions about each scenario, including the likelihood that they would behave similarly, their moral beliefs about the situation, and their perceptions regarding the certainty and severity of the consequences for misusing the technology. The participants also responded to questions about their virtual status and their tendency to engage in socially acceptable behaviors.

An important point to note with regard to the study's methodology is that the study was cross-sectional, with participants completing measures at a single point in time. As such, D'Arcy and Devaraj aptly noted that all relationships must be interpreted as just that—relationships—without inferring any causality.

KEY FINDINGS

As expected, D'Arcy and Devaraj found that both formal and informal sanctions are associated with less technology misuse and that moral beliefs explain these relationships. Specifically, they found that technology misuse is lower when employees (1) perceive that the formal consequences for misusing the company's technology are severe and certain, (2) have a tendency to behave in socially acceptable ways, and (3) believe that misusing company technology is morally wrong. Regarding moral beliefs explaining these relationships, D'Arcy and Devaraj found that employees who perceive consequences to be severe and certain are likely to believe that misusing technology is immoral, which in turn leads them to misuse technology less. Similarly, employees who have a need for social approval are more likely to view misusing technology as immoral, and consequently less likely to misuse technology.

Regarding the influence of organizational context on technology misuse, as predicted, when employees work remotely and spend more time away from the office, the likelihood of technology misuse is higher. Contrary to their predictions, however, managers and non-managers did not differ in their likelihood of technology misuse.

CONCLUSIONS AND IMPLICATIONS

D'Arcy and Devaraj's findings reveal that both formal and informal sanctions can effectively deter technology misuse. Furthermore, they demonstrated that employees who spend more time away from the office are more likely to misuse technology. Surprisingly, one's level within the organizational hierarchy (managers vs. non-managers) was not associated with technology misuse. One explanation for this may be the low number of managers that were in the study and the way in which employment level was coded. Specifically, D'Arcy and Devaraj coded all technical, professional staff, and administrative/clerical respondents as being non-managerial employees. This could have been problematic if, for example, a technical respondent was also a manager. Nevertheless, the authors did find that formal sanctions are a stronger deterrent for managers than for non-managers with regard to technology misuse, which they attribute to the fact that managers may be more committed to the organization, and therefore have more to lose if they are caught engaging in such behaviors.

These findings have important implications for managers, especially for managers whose employees regularly use company technology. First, it is clear that formal sanctions serve as a strong deterrent to technology misuse for employees. As such, managers should make sure that policies exist that emphasize that there are mechanisms in place to detect technology misuse and that penalties for such behavior are both severe and certain if an employee is caught. With such policies in place, an organization may notice decreases in information technology security concerns, such as user downtime and malware infestations. As an added benefit, results suggest that having such formal sanctions in place also adds to employees viewing technology misuse as immoral, which in turn reduces the likelihood that employees would misuse technology.

Another practical implication of this study involves the importance of individual and contextual differences in predicting and preventing technology misuse. D'Arcy and Devaraj found that individuals who have a greater need for social approval are more likely to view technology misuse as morally wrong, and are less likely to intentionally engage in technology abuse and misuse. With this in mind, managers may do well to incorporate social desirability into their staffing procedures, selecting applicants who indicate a stronger need for social approval. Additionally, employers could incorporate the immorality of misusing technology into training in order to raise the level of moral development of employees. In fact, research from the criminal justice literature has found that informal sanctions have a bigger impact on preventing criminal activity than formal sanctions, with the anticipation of social disapproval being better at deterring criminal behavior than anticipation of formal punishment. By selecting employees who have a need to be socially accepted and training employees about the immorality of misusing technology, organizations may reduce the financial and legal risks associated with inappropriate technology use.

A final potential solution to the problem of employee misuse of technology resources is to make sure that employees do not feel psychologically separated from their coworkers. The findings from D'Arcy and Devaraj's study suggest that, as the number of remote workers increases, so too does the probability that employees will misuse the company's technology resources. As such, employers should take steps to ensure that these remote workers feel as if they are valuable members of the organization. In addition, managers should require security awareness training for all employees, whether they work remotely or otherwise, in order to make them aware of what constitutes appropriate versus inappropriate use of company technology. As part of this training, formal sanctions for engaging in misconduct can and should be communicated. By incorporating practices such as these, organizations may help employees feel less like outcasts, which in turn may prevent the headaches associated with severe security breaches, such as data theft, damage to company technology, or damage to company networks.

SOURCE

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43,* 1091–1124.