Chapter 9

Understanding Feral IT Practices as Deviance: The Contribution of Merton’s Theory of Anomie

Shubhankar Thatte
Swinburne University of Technology, Australia

Nick Grainger
Swinburne University of Technology, Australia

Judy McKay
Swinburne University of Technology, Australia

ABSTRACT

In this chapter, the authors discuss the concept of feral IT practices, which are defined as work practices of employees who use information technologies in ways that deviate from organizational norms. Such practices are in the main conducted beyond the control and/or knowledge of organizational IT management. The authors argue that feral practices can be looked at from many different perspectives, and thus may sometimes be viewed as innovative and beneficial for organizations, as opposed to being regarded as risky and potentially detrimental to the organization. However, such a view of feral practices is relatively under-theorized at present, and a challenge for researchers is to develop knowledge of how an organization can benefit from this unsanctioned innovation, while protecting itself through adequately managing the risks to which they may be exposed through these feral practices. Merton’s Theory of Anomie provides deeper insights into the phenomenon of non-compliance, and in this chapter, the authors aim to explore how the concept of deviance (non-compliance) can usefully be applied to offer new insights into the phenomenon of feral practices. A conceptual framework based on Merton’s theory is proposed that suggests that feral IT practices may arise from structural strain that inhibits the ability of an individual or group to achieve their goals and objectives. The organizational structure factors contributing to structural strain are discussed. The chapter concludes with a discussion of the potential contribution of Merton’s theory to understanding and ultimately managing feral practices in organizations such that risks are minimized and benefits maximized.

DOI: 10.4018/978-1-4666-5027-5.ch009
INTRODUCTION

Large scale changes in the organizational technology landscape over the last three decades have led to major changes in the way information technology is used in organizations. For instance, many employees are increasingly IT literate and savvy, in both their personal and professional lives, with the expectation that good, appropriate IT is available to hand to support their accomplishment of work tasks. As IT has become readily available, easy to use and relatively cheap, users have gradually gained more control over appropriating, configuring and using IT to perform work tasks. Moreover the rapid acceleration of IT advances over the last 10 years in areas such as mobile computing, cloud technologies, web 2.0 and other technologies, combined with the emergence of a range of ‘smart’, portable devices, for example, have further empowered users in organizations with the capability to not just perform work-related tasks with little direct assistance from the IT department but in fact to go further and develop additional IT tools themselves. Data to support this claim is appearing regularly in the professional literature. For example, according to a study by Gartner (as quoted by King (2012)), in the next three years “35% of the enterprise IT expenditures will happen outside of the corporate IT budget”, while PricewaterhouseCoopers has suggested that in the 100 top-performing companies, IT controlled less than 50% of the corporate IT expenditures. This seems to suggest that control over IT spending is constantly being pushed out of the control of IT into the hands of the users, offering them greater discretion and flexibility to meet their own perceived IT requirements. In the face of such significant changes in IT in organizations and the skills and expectations of many employees, IT departments are facing increasing challenges to manage and control the usage of the IT resources by employees to ensure that the expected benefits and value are delivered from organizational IT investments, while limiting the organization’s exposure to IT-related risk. Arguably, however, more and more users use IT outside the purview of the IT department and in ways that are not officially sanctioned by the organization.

In this chapter we will introduce the concept of feral IT practices, defined here as work practices involving the use of IT that deviate from standard organizational norms and that may occur without the knowledge and/or control of the appropriate business unit or IT management. Typical examples of such practices would be a financial accountant who, without any authorization, copies and pastes sensitive financial information into a spreadsheet and stores this information in a public cloud. Likewise, the action of an operations manager in a manufacturing department who, on his/her own initiative, extracts data from the formal information system into a spreadsheet, manipulates it for data analysis purposes and feeds the data back into the formal system, would also be regarded as a feral practice. These examples both exhibit unauthorized manipulation and storage of corporate data without adequate controls applied. While some of these practices may be innovative and beneficial to the user and potentially the organization, at the same time they may pose a significant threat to the organization. For instance, the financial accountant might have employed the spreadsheet in order to develop enhanced financial reporting capabilities lacking in the current formal corporate system. However, the storage of such critical information outside the company’s firewall might pose a considerable risk to the organization, particularly in the absence of formal contractual agreements with the service provider. Similarly, the