Chapter 9

The Relationship between IT Director Values and Extent of IT Disaster Recovery Planning in the Banking Industry

Jordan Shropshire
Georgia Southern University, USA

Christopher Kadlec
Georgia Southern University, USA

ABSTRACT

Information technology plays a pivotal role in defining the success of organizations. Given its importance, one might assume that modern organizations take steps to ensure the recovery of IT services following disasters. Unfortunately, this is rarely the case. To understand the variation in degree of IT disaster recovery planning, this research focused on those responsible for managing IT resources and IT directors. For the study, a survey was mailed to 337 financial service institutions in the southeastern United States. Over 150 IT directors completed self-assessments for measuring the extent to which their organization engages in IT disaster recovery planning. In addition, they responded to a number of questions regarding their work-related values, and over 63% of the variance in degree of IT disaster recovery planning was explained by two predictors: uncertainty avoidance and long-term orientation. Results show that firms with IT professionals who prefer to avoid uncertainty and who have long-term outlooks have more developed IT disaster recovery plans.

INTRODUCTION

Stable, reliable IT services have become the required minimum. Most modern businesses cannot function without information systems for data processing, storage, and communication. Despite their importance, few firms create sufficient IT disaster recovery (ITDR) plans (Gold, 2007; Sheth et al., 2008). ITDR includes more than just data backups (Plotnick, 1999); it involves analyzing IT services, identifying potential threats services, preparing organizational members,
creating system recovery procedures, finding offsite storage, and conducting drills (Kadlec & Shropshire, 2010). Although many firms are investing in efforts to improve the security of their data, there is less consistency regarding ITDR planning (Lohrman, 2007; McLaughlin, 2008). The ITDR planning practices of some organizations are not in keeping with the sophistication of their information systems; in contrast, other businesses create and maintain exhaustive plans (Anderson, 2008; Ramsaran, 2005). Even within industries and geographic regions, there is much variation in degree of preparedness (Retelle, 2008). By understanding this phenomenon, it might be possible to improve ITDR capabilities and build more resilient organizations.

This research seeks to explain the differences in degree of ITDR planning by considering those who manage information systems and technology — IT directors. In general, IT directors are responsible for ensuring the continued provision of IT services (Chun & Moody, 2009). They lead efforts to leverage the capabilities of corporate information systems by organizing hardware, software, and human resources (Agarwal & Sambamurthy, 2002). The attributes of IT leaders have previously been linked with firm performance (Sobol & Klein, 2009). In this study, the work-related values of IT directors are analyzed. Values are long-lasting attributes of individuals; they may impact individual attitudes and behavior over time (Fishbein & Ajzen, 1975). Because ITDR planning consists of a series of actions which may take weeks (or even months), attributes more permanent than attitudes or intentions are necessary. Therefore, IT director values are used to explain degree of ITDR planning. Hypotheses concerning these relationships are conveyed and tested.

This paper is of value to IT researchers and professionals. This research represents one of the first efforts to predict organizational outcomes associated with IT disaster recovery planning. It overcomes previous obstacles in model design, testing, measurement, and analysis. It provides immediate guidance for consultants and managers of information systems by providing actionable recommendations for helping enterprises improve IT disaster recovery planning.

The rest of this manuscript is organized as follows: first, background information on IT disaster recovery planning is supplied. This section focuses on the definition of IT disaster recovery planning and covers the various components included in ITDR plans. Next, the relevant personal values of IT directors are described; these values are used as predictor variables. Next, the methodology, analysis, and results sections are presented. Finally, implications and concluding comments are made.

BACKGROUND

This section provides background information on the elements in the research model. First, the case for planning is made. Next, IT disaster recovery planning is described. Because the variable is relatively new to mainstream IT literature, some background information is provided. In addition, the personal values of the IT director are introduced. For each element, a basic definition, a rationale for inclusion into the present study, and an associated hypothesis are given.

The Case for Planning

Datacenters and systems are quite vulnerable. They rely on a steady stream of resources, such as energy, skilled labor, network connectivity, and cooling systems, to proper function. It is essential to understand that when it comes to IT-related disasters, history repeats itself. Hurricanes flood entire cities, earthquakes flatten buildings, and disgruntled employees destroy server rooms. These threats will occur again, and savvy managers and IT consultants will take these threats into account and prepare for the worst.

Unfortunately, too many enterprises fail to take the risks seriously. Consider, for example,