Chapter 22
The Risk Management Profession in Australia:
Business Continuity Plan Practices

Adela McMurray
RMIT University, Australia

Jean Cross
University of New South Wales, Australia

Carlo Caponecchia
University of New South Wales, Australia

ABSTRACT

This study aimed to identify to what extent Australian organizations have any plans to manage business continuity threats, and the nature and content of these plans. Sixty-four respondents who were risk management professionals were surveyed to explore the Business Continuity Practices within their organizations. The ANOVA analysis showed 39 per cent of the organizations had developed an enterprise-wide plan of which just over half stated that the plan was tested. However, 36 per cent of respondents had no plan, an "informal plan," were developing a plan, or did not know whether they had a plan. Standardized guidelines for a process to manage risks have been developed across many spheres and countries and are brought together in the international risk management standard ISO31000 (ISO, 2009), which presents a process applicable to all organizations and all risks. Human resource practices that promote consistent communication and an organizational culture that allows business continuity plan values, attitudes and beliefs to become embedded and to move across traditional organizational boundaries are therefore important for gaining the cooperation needed to implement plans in an organization's operational areas pertaining to business continuity.

DOI: 10.4018/978-1-5225-6195-8.ch022

INTRODUCTION

The growing importance of risk management is recognized by government and industry with regulation increasingly requiringorganizations to have a formal risk management policy and processes. Disaster response and emergency plans are integral to an organization's survival (Kahn, 2012). Safety and environmental regulations in most countries have required risk management processes for many years but following the Enron collapse in the United States, the Sarbanes Oxley Act was introduced requiring listed companies to have an enterprise risk management system such as outlined in the COSO Enterprise Risk Management – Framework (2004).Risk management has moved from the periphery to the centre of business planning. The US September11 terrorist attack reminded businesses globally of the need to incorporate adequate disaster recovery and business continuity planning into their policies and practices (Savage 2002). US President George W Bush issued an executive order within hours of the terror attacks to facilitate continuity of government, later making Executive Directive 51 (Presidential Directive NSPD 51, 2007). It required executive departments and agencies and provided guidance for other levels of government and the private sector to have a continuity program in case of catastrophic emergency, which is described as "any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions" (NSPD 2007).Standardized guidelines for a process to manage risks have been developed across many spheres and countries and are brought together in the international risk management standard ISO31000(ISO, 2009) which presents a process applicable to all organizations and all risks. Writing on the impact of this and new standards on the preparedness of business to recover from disaster Tucker (2014) reported that many emergency and business continuity managers believed that lessons were learned from September, but contrasts this with: "A simple study of the unclassified literature shows that the method of attack was entirely predictable and the only lesson learned was that we did not learn our lessons." (Tucker 2014, p.10). In light of the development of Business Continuity Planning, especially after major disasters such as the US 9/11 attacks, the UK Manchester and Westminster attacks, the Sydney Lindt Café seizure, Avian flu and Ebola, this study aimed to identify to what extent organizations in Australia have any plans to manage business continuity threats, and the nature and content of these plans. This is of interest and has relevance to other global organizations based in various countries as Australian organizations increasingly engage in global business practices.

BACKGROUND

A new twist on disruptive threats to continuity of government emerged in late 2016 with allegations of a State-sponsored information warfare by Russia against the Democratic party and, in turn, the US electoral process. Writing in Survival magazine (Inkster, 2016) former British Secret Intelligence Service operations director, Nigel Inksterstated: "It should hardly be surprising that the intelligence services of a foreign power in a confrontational relationship with the United States should take an interest in the latter's presidential election and seek to gather intelligence on the process and candidates, including through computer-network exploitation" (p. 23).

Risk management involves managing threats and opportunities, and includes communication, accountability in decision-making, rigorous, forward and balanced thinking and is viewed as a vital part of good business practice (ISO, 2009). In the context of disasters, areas of risk include telephone communications,