

Failing to Plan, Planning to Fail:

Gaps in Business
Continuity Preparedness
Reveal Vulnerability

Introduction

Continuity and disaster recovery plans are increasingly ubiquitous in business, but many plans fail to adequately consider a variety of contingencies and risk scenarios.

While most companies have a Business Continuity Plan (BCP) of some sort in place, a significant number do not account for security breaches, or proactively prepare for key events such as deliberate or malicious actions. Evidence suggests, moreover, that plans are not being adequately tested, in terms of both frequency and scope. Finally, the overall breadth of business continuity planning is still narrow. Communication channels between different functions are weak or nonexistent, thereby leaving companies exposed. What's needed is more effective end-to-end continuity planning that acknowledges a wide range of contingencies.

This white paper examines the findings and implications of a recent Compass survey of over 50 senior business and IT executives from large UK-based organisations in a variety of industry sectors, including finance, retail, manufacturing, media, and government/public sector bodies.

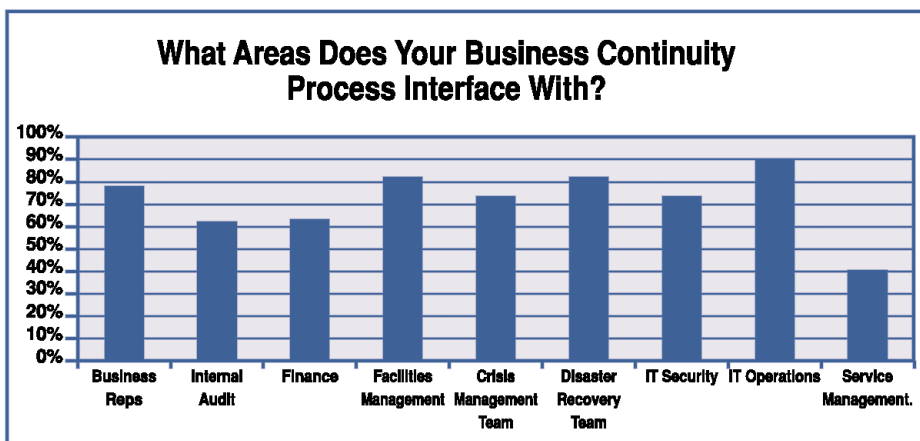
Survey Results: State of Planning

Among executives surveyed, 98 percent report that their company has a BCP in place. Business Impact Analysis and Risk Assessment, meanwhile, were less well established (more on the implications of this later). A surprising 38 percent of companies fail to account for malicious intent, and 44 percent don't consider security breaches in their planning. Only half, meanwhile, plan for the loss of key personnel.

Independent research carried out in the UK shows that over 70 percent of service-affecting incidents are generated from within an organisation. It's therefore surprising that malicious intent and security breaches are not covered more adequately, given that many threats of this nature occur within an organisation. These findings suggest a narrowness of breadth in business' approach to continuity planning, a focus on external factors and a neglect of the threats that can emanate from within an organisation.

The Information Technology Infrastructure Library (ITIL) standards advise that the business continuity process can be seriously compromised if it does not interface with other service management processes. However, only 40 percent of the companies surveyed by Compass have such formal interfaces in place. (See table one for details.)

Table One



This disconnect, in terms of formal communication between IT and service management, suggests that many organisations rely on pockets of preparedness, rather than developing and implementing effective end-to-end plans that account for a wide range of contingencies and scenarios. The absence of established interfaces with, for example, Capacity, Availability and Change Management, could mean that companies will struggle to ensure that their BCP provides sufficient capacity for recovery, required availability levels within needed timescales, and sufficient flexibility to respond to changing business requirements.

Testing and Review are Inadequate

Another flaw revealed by the survey is a tendency for companies to view maintenance of the BCP as an occasional activity, rather than an ongoing requirement. According to the survey, 30 percent of companies do not review their BCP regularly. The BCP needs to be regularly reviewed, updated, and tested to take account of changing business requirements and risks, the introduction of new systems, and the phasing out of old ones.

Many companies employ 'multiple' testing strategies, but ultimately still focus primarily on IT systems. For example, the survey found that IT Operating System Recovery is still the most widely used testing strategy at 69 percent while Business Systems Recovery lags behind at 47 percent.

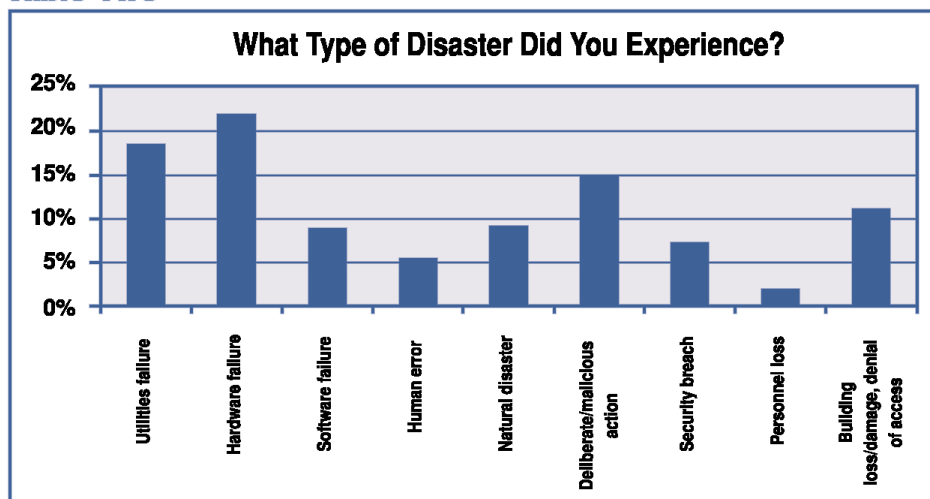
Paper walkthroughs, scenario simulation, and role play are deployed for less than 50 percent of tests, and only 4 percent of respondents included communication cascades as an additional testing option.

This evidence suggests that BCPs are not being regularly reviewed and tested. In many cases, the necessary level of discussion and cooperation between IT and the business hasn't occurred. Such communication is needed to ensure that the plan is covering the right things and delivering an appropriate level of recoverability. In light of the constant change that characterises business systems, these findings imply that the success of recovery and the investment in business continuity planning is being undermined and compromised.

Frequency of Disasters

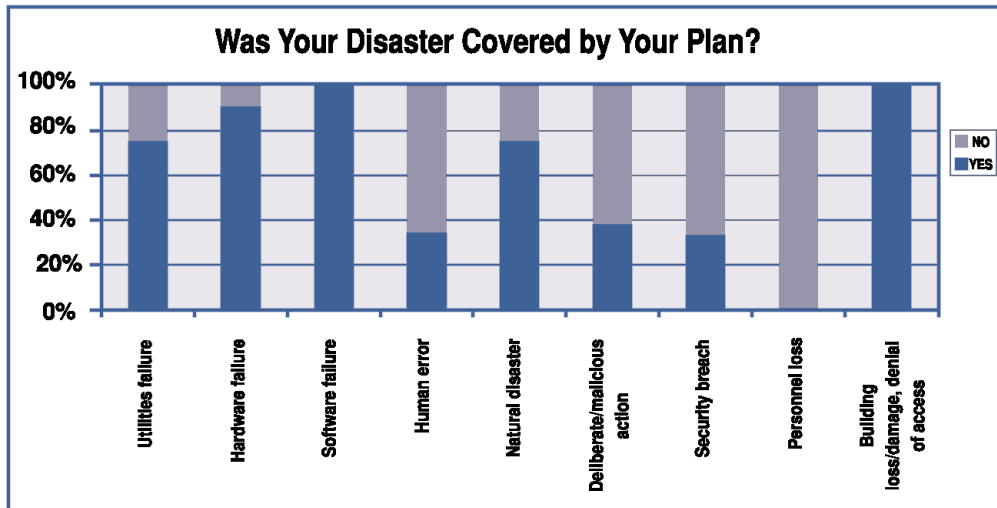
Compass found that 58 percent of companies surveyed have suffered a disaster during the past five years. In terms of causes, 40 percent were the result of utility or hardware failures, while 25 percent were caused by deliberate or malicious action, security breach and personnel loss - all areas currently under served within BCPs. (See table two for details.)

Table Two



Overall, 38 percent of surveyed companies have had to invoke their BCP. As table three below indicates, these BCPs catered for utility, hardware, and software failures, as well as loss of access to building facilities. The plans were less well prepared for addressing disasters related to human error, malicious action, security breach, or loss of personnel - all areas where risk mitigation measures can be taken. Natural disasters also presented challenges to existing BCPs, but these areas are recognised as being more difficult to plan for.

Table Three



Of companies surveyed that experienced a disaster, 71 percent indicated that their business was affected. The most common recovery timescale is 12 to 24 hours (21 percent). However, 16 percent of companies took over 24 hours to recover, with an additional 19 percent taking over a week to recover. Disasters resulting from malicious/deliberate action, security breaches, or personnel loss generally required a longer recovery time.

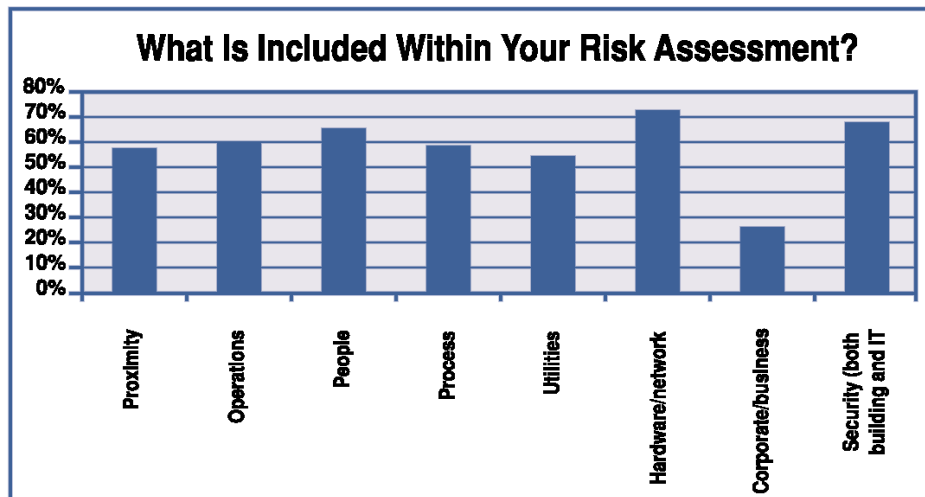
The relatively large proportion of companies that require more than 24 hours to recover from a disaster suggests a potential problem, given the previously-documented lack of communication between IT and the business. Specifically, if the BCP is not based on adequate input from the business, how can executives be confident that the timescales are appropriate to business needs?

The Trinity: BCP, Risk Assessment, and Business Impact Analysis

A comprehensive strategy to ensure business continuity in a strategic sense integrates a BCP together with a Risk Assessment (RA) and Business Impact Analysis (BIA). Without this “trinity,” a company undermines the considerable investment made in business continuity planning and gambles with its future longevity should disaster strike. Put differently, the appropriateness of the BCP is questionable if business needs are not assessed via a BIA and the risk profile not considered through an RA.

Eighty-five percent of companies surveyed reported carrying out a Risk Assessment. While a broad range of risks are covered, only 25 percent of companies include corporate and business risks (see table four for details). And, nearly 40 percent of companies fail to review their risk assessments on at least an annual basis.

Table Four



Sixty-nine percent of companies surveyed, meanwhile, have conducted a Business Impact Analysis, but at least half of those fail to conduct a regular review.

These statistics indicate that many organisations are characterised by a misalignment between the BCP and business requirements. While existing plans may be well defined in terms of the types of disasters that can be addressed, there's less evidence that the plans are responsive to business requirements in terms of strategic assets and time to recovery.

This disconnect may be explained in part by the longstanding management challenge of aligning IT services with business needs. Whatever their source, these gaps increase the likelihood that substantial investments in business continuity won't deliver the desired benefit.

Proactive Approach to New Standards

Apart from the obvious ramifications of inadequate disaster recovery and continuity planning, the looming prospect of stricter government security regulations should give pause to business organisations. In the United Kingdom, as well as in the United States and elsewhere, government regulators are implementing increasingly strict guidelines to protect consumers against fraud and identity theft. This is particularly the case in the financial services sector.

Businesses that take a proactive approach and work with regulators to craft standards and secure systems will have a distinct advantage, since they will be able to influence the process and won't be caught off guard. Companies that react to already-defined standards, meanwhile, will find themselves scrambling to catch up, and will face increased cost and disruption.

Debbie Rosario is a managing consultant in Compass' Guildford, UK offices. For more information on this topic, contact risk@compassmc.co.uk.



FACT BASED CONSULTING

Compass is an independent global management consulting firm that delivers fact based business and IT performance improvement recommendations to large organizations.

Services include Performance Improvement; Performance Management; Sourcing; Realization of IS Value; and Mergers and Acquisitions Planning and Implementation.

Compass combines a rigorous methodology, extensive global database, and consultant expertise to drive positive and lasting changes.

www.compassmc.com

Visit our Web site for local office contact information.

© Compass Publishing BV 2004

All rights reserved

For a free subscription to Compass E-Notes, a bi-weekly electronic newsletter offering insights into IT and business management, send a message to facts@compassmc.com with "E-Notes" in the subject line.

**Barcelona • Birmingham • Calgary • Chicago • Frankfurt • Guildford
Helsinki • Johannesburg • Milan • Montreal • New York • Paris
Rotterdam • Singapore • Stockholm • Sydney • Toronto • Washington, DC**