

This issue:

- ▶ Managing the risk of workplace bullying
- ▶ Getting value from your Business Continuity Plan

## Workplace bullying: a risk to employees and organisations

Since the tragic case of Brodie Panlock's suicide following prolonged bullying from her work colleagues at a café in Melbourne, and WorkSafe Victoria's subsequent prosecution, the issue of bullying in the workplace has received a great deal of attention.

The charges brought by WorkSafe Victoria in this important case included "failing to provide and maintain a safe working environment" (refer to [case](#) and a [report](#)). The inadequate "information, instruction, training and supervision" provided by the employer was the critical failure, and fines were imposed.

Other cases have come to light which have reinforced that bullying claims are, in the appropriate circumstances, compensable (for example a case at RMIT in 2010) whether the alleged harassment was "real", or only believed by the claimant. (Although, somewhat paradoxically, other cases (<http://www.austlii.edu.au/au/cases/cth/aat/2010/245.html>) have shown that stress induced by bullying may not be compensable if the stress is successfully argued to be "a normal response to a hostile environment".)

Most Australian legislation dealing with health and safety either explicitly or implicitly requires employers to appropriately manage this issue. For example, under the Queensland *Workplace Health and Safety Act 1995*, an employer must identify and manage exposure to the risk of death, injury or illness created by workplace harassment, including bullying.

However, these legal considerations simply support the underlying fact that bullying and harassment in the workplace pose a real risk to both employees and their organisations, a risk that must be appropriately managed. In many organisations, large and small, the risk



has not been identified or assessed, paving the way to both individual and organisational harm.

As WorkSafe Victoria highlighted in the aftermath of the Brodie Panlock case, trying to address the impact of bullying after the fact is ineffective - the damage is done by then and can't easily be fixed. The risk needs to be proactively managed. Employers must be actively aware of the risk, its causes and consequences, and prepare systems and strategies to prevent or nip in the bud any instances of bullying or harassment in their workplaces.

Articulating a clear workplace policy defining acceptable and unacceptable behaviour, instituting appropriate training, developing communication channels to facilitate the identification of problems, and implementing systems supporting appropriate workplace supervision and monitoring are all potential controls for this risk. Each organisation's circumstances will be different, and therefore undertaking a formal risk assessment using the processes in ISO 31000 *Risk Management* is a critical first step.

There are a range of sources of useful information to assist employers and employees, including the following:

- Workplace Health and Safety Queensland published the [Prevention of Workplace Harassment Code of Practice 2004](#) which includes advice about the prevention or control of risks stemming from workplace harassment.
- The ACT Work Safety Commissioner released materials to provide guidance to employers and has been conducting a series of awareness and prevention workshops (<http://www.worksafety.act.gov.au/bullying>).

- WorkSafe Victoria released guidance materials for both employers and employees ([Prevention and responding to bullying at work](#) and [What to do if bullying happens to you](#)).

For more assistance or advice, contact your state's safety authority.

# Ensuring you get value from your Business Continuity Plan

Business Continuity Management (BCM) in a form that provides real value to businesses is not a once-off or solely compliance-based process. To be truly useful, it needs to be an ongoing process that becomes embedded in the culture of the organisation.

Occasionally there are good-news stories of business disruption being painlessly resolved (for example, the ability of Queensland Emergency Services to successfully manage a [systems failure](#) earlier this year).

However, more commonly, we hear stories of unanticipated business disruption resulting in disastrous and uncontrolled impacts, and businesses struggling to get back to normal. The first domino falls and, rather than short-circuiting the cascade with well planned action, the organisation watches in dismay as the rest tumble down.

There are many reasons why BCM fails to achieve good results for businesses of any size. The first one is clearly that an alarming proportion of businesses don't undertake any formal BCM process at all. However, even for those that do, there are common pitfalls to be avoided:

## 1. Don't assume business continuity is only about natural disasters.

If BCM is about natural disasters, there's only so much that can be planned, and this assumption will heavily skew the focus of any efforts to prepare. However, events such as power failures, IT problems and human error are more likely to cause business disruption. Organisations engaging in BCM need to consider and plan for all potential causes of business disruption in their organisational context.

## 2. Don't assume the creation of a business continuity plan (BCP) means the job is done.

A plan, however well crafted, is useless if no-one understands it or is prepared at short notice to implement it. The BCP must be continually reviewed



and updated, communicated, tested and improved. Personnel who only need to glance at the plan as a reminder can respond competently to a crisis. Those trying to read and understand it for the first time will end up developing a response on the fly.

## 3. Don't assume problems only come in "ones".

The underlying and unrecognised assumption that any disaster will be a singular event leaves organisations ill-prepared for evolving situations with multiple failures. The BCP needs the flexibility, and the depth of contingency planning, to respond in a situation that is continually evolving, for example when there's a change in the initial source of the disruption, or impacts from after-effects of the disruption, or newly emerging information.

## 4. Don't assume suppliers and customers will be there

If the BCP assumes that in a crisis key suppliers will be supportive, and key customers sympathetic, the organisation will be highly vulnerable if the assumption proves to be incorrect. BCPs need to assume the worst and prepare contingency strategies for that scenario (for example, identification of alternate suppliers, development of robust communication plans for customers, training all employees in their roles and responsibilities during a business disruption).

## 5. Don't assume that running a test of the BCP equals preparedness.

One basic run-through of a documented BCP does not necessarily indicate overall readiness. A wider view should be taken, including ongoing testing (using varying scenarios), regular training, and most importantly continuous improvement.

QRMC can provide advice and assistance in developing, reviewing, testing and training for your organisation's BCM needs. Contact details are below.

GPO Box 199, Brisbane Qld 4001  
Phone + 61 7 3229 1744 Fax + 61 7 3229 1844 Email [enquiries@qrmc.com.au](mailto:enquiries@qrmc.com.au)  
QRMC Risk Management Pty Ltd ABN 43 119 425 991

[www.qrmc.com.au](http://www.qrmc.com.au)



The material contained in this publication is in the nature of general comment only and neither purports, nor is intended, to be advice on any particular matter. No reader should act on the basis of any matter contained in this publication without considering and, if necessary, taking appropriate professional advice regarding their own particular circumstances.