Engaging IT

John Robinson explores the disconnect which exists between the IT continuity manager and the BCM manager, and considers steps which can be taken to build bridges

The British Standards Institute's website leaves little doubt that we should view IT continuity as a subset of BCM, describing BS 25777 – the information and communications technology continuity management code of practice – as a source of "…recommendations for ICT continuity management within the framework of business continuity management…".

This seems entirely sensible, since even in cases where IT is the business, stakeholders must be served, executives must make decisions and suppliers must be paid. In each case, IT enables and serves the legal business entity and its continuity is reasonably positioned as a critical and integral part of the business whole.

So why, in some organisations, is there an apparent discontinuity or gap between BCM and IT, and where this exists, is it a problem? This article considers factors behind this phenomenon in the light of the BCI Benchmark's findings to date.

The BCM/IT relationship

Consider for a moment what it means for IT to operate independently of the BCM remit. For IT to deliver service continuity to the business it must carry out detailed research, prioritising and dovetailing the recovery of many services to many parts of the business on terms the business accepts. If it doesn't do this research, it means imposing continuity service levels based on guesswork, intuition and experience, risking a significant percentage being incorrect. If it does the research, it will necessarily replicate work carried out by BCM.

Both options are wasteful, confusing, risky and potentially catastrophic if adopted strategies result in conflict or omission. It is entirely preferable for BCM and IT to operate seamlessly, hand-in-glove, delivering what the business needs when called upon in a concerted integrated manner. So if a gap exists, then yes, it's a potential problem.

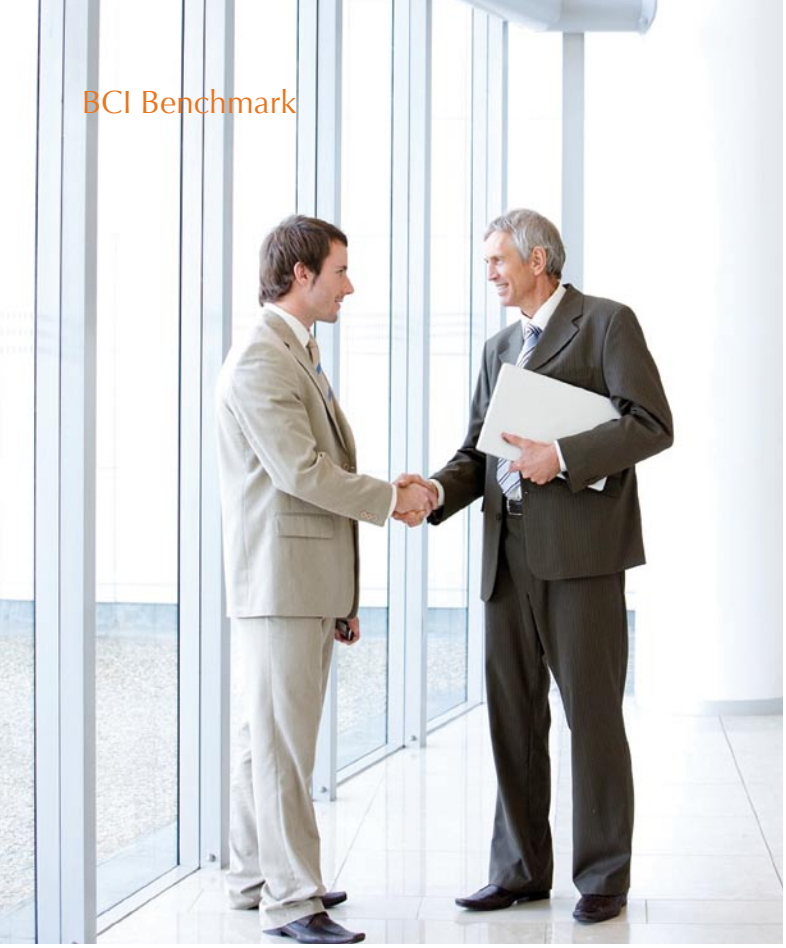
Closing the divide

Fortunately, where a divide is apparent there may be characteristic conditions we can identify, understand and work with to help improve matters:

- **History:** BCM may be seen by IT as the new kid on the block, an upstart evolution from the original realisation in the 1960s by some organisations that their mainframe computers represented a potentially catastrophic single point of failure and who then took steps to protect and duplicate them. The phrase IT DR was born then and is still pervasive in IT today. IT reasonably sees itself as the parent of the discipline, and within its domain the prime source of knowledge and experience. A role reversal is likely to be resisted, particularly when the depth of IT know-how is not well-matched by the BCM incumbent.
- **Power:** IT is the custodian and in many cases the expert creator of two prime corporate assets – process and information. IT is consequently influential and powerful often to the point where it can shape how, when or whether BCM is implemented, potentially leading to long delays.
- **Motivation:** IT is typically positioned as a/the core business enabler, helping the organisation to excel. It wants to be perceived as a forward-thinking source of value and not cost, justifying a healthy budget. The imposition of expensive BCM or risk strategies means: a) diverting resource and cash to activities that may disrupt and delay prestigious programmes; and b) have no immediate tangible return. In the absence of clear justification or sell-in, BCM becomes easy to sideline.
- **Culture:** IT often has many times the headcount of its internal peer continuity service providers such as human resources, public relations and facilities. It is inherently complex and has its own constantly changing environment and language – potentially, an organisational sub-culture. This has its own momentum and direction that is resistant to externally imposed rapid change.

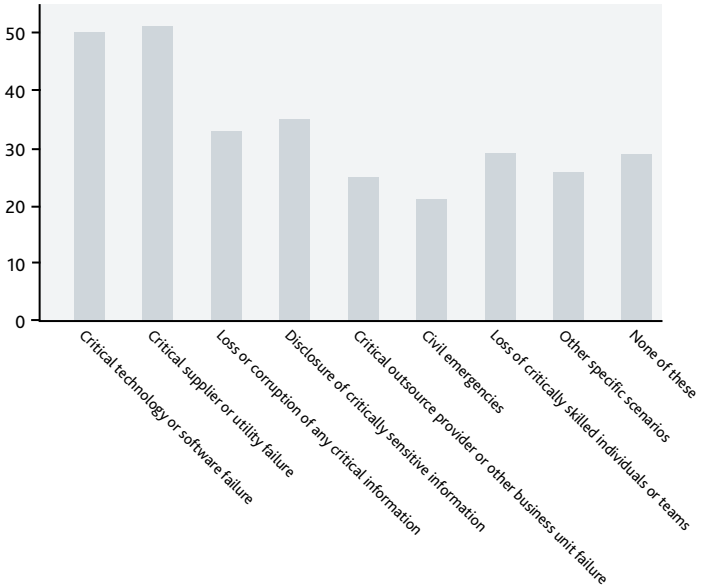
Where present, these factors mean that IT has the potential to be seen by BCM as an impenetrable or immovable object, making engagement on BCM's terms a challenging prospect. But are the conditions real and can they be cleared?

"If it doesn't do this research, it means imposing continuity service levels based on guesswork, intuition and experience, risking a significant percentage being incorrect"



Inside track

The answer to both parts of the question is a qualified yes. IT continuity is strongly represented in ITIL (IT Infrastructure Library) and mostly the issue at stake is one of achieving convergence of two sets of adopted ideals and interests. The graph below shows how Benchmarked organisations responded when asked if their continuity strategies fully and demonstrably enabled recovery from a range of event types. The leftmost scenario relates to critical technology or software failure and was selected by the majority of recipients in this sample. It suggests that more BCM managers believe IT can recover from any scenario as well as or better than other specific incident types.



And of course, it is never in IT's interest to be seen as a potential contributor or cause of business failure, however remote the possibility, and for this reason alone, the majority of senior IT executives positively embrace continuity.

Facilitating the process

So, engaged appropriately and despite the apparent obstacles BCM should find itself pushing at an open door. However, notwithstanding this, there are things we can do to make the process easier:

- **Adopt a collaborative approach:** strategic plans give IT substantial momentum and it's easy to burn time and energy insisting on a change in direction. Agreeing on a long term convergent compromise that integrates BCM into new and existing plans is often preferable.
- **Learn the language:** IT's ambassadors to the business are well-qualified, influential and speak both languages; BCM needs an equivalent deep understanding of IT for an effective working relationship to exist. This requirement extends to any highly specialised area of the business.
- **Establish positions of influence:** to be authoritative, BCM's role and position vis-à-vis IT must be reflected strongly both in policy and in mission-level business plans, with executive representation.
- **Sell on value:** the BCM team needs to be skilled in selling its value and benefits to the business, creating regular opportunities to do so. It also needs to be able to sell on behalf of IT, helping it realise the value of its risk management contribution in business terms.
- **Embed BCM ideas:** offer to raise BCM awareness in IT at levels that are relevant and meaningful for IT operational personnel.

> "IT is consequently influential and powerful often to the point where it can shape how, when or whether BCM is implemented, potentially leading to long delays"

Mutually beneficial

This brief examination tells us that an organisation's business continuity capability needs to be multi-faceted, capable of engaging the organisation at all levels and in all disciplines. It should expect to be challenged by, and needs a special relationship with IT, building connections that allow a true bi-directional flow of value and information, drawing parallel disciplines closer together for mutual benefit.

This has secondary implications for the required diversity of the BCM skill-set, demanding technical insights on the one hand, subtle business influencing skills on another, and operational capabilities to deliver training and testing somewhere in between. This mix and the workload it implies make it less likely that a BCM manager can achieve a sustained unified position in isolation. It emphasises the need for a strong team approach, drawing on executive sponsor, BCM manager and IT continuity manager working collaboratively toward a successful outcome.

JOHN ROBINSON FBCI

John Robinson is managing director of INONI Limited and author of the BCI Benchmark.

www.inoni.co.uk

info@inoni.co.uk