

Business Continuity Management - Bridging the divide

By Tony Stranack and Charlie Cornish

Business Continuity management has traditionally been associated with large enterprises and public sector organisations. Now however, organisations of all sizes are making sure that they are both resilient and prepared to get back to business in the face of an ever changing and challenging landscape. Indeed, the latest survey by The Chartered Management Institute (CMI) (1) found that the number of organisations with specific business continuity plans increased from 47 percent in 2008 to 52 percent in 2009.

Whilst it is now an essential requirement for every organisation, business continuity management brings challenges, especially to those who are implementing a BCMS (Business Continuity Management System) for the first time. This white paper will focus on the greatest challenge: how to ensure that business continuity planning is a holistic across-the-organisation effort, rather than one which is siloed in separate departments.

Business continuity is not the responsibility of the IT department

Perhaps the biggest myth about business continuity is that responsibility for it should reside within the IT department. It is easy to see where this originated, as business continuity has evolved from IT disaster recovery, where it was appropriate for the IT department to take the lead. IT downtime is still one of the biggest causes of business disruptions, so it is a natural, if flawed, assumption that business continuity management should be IT-led.

However, if it is to be effective, business continuity management must be a board level responsibility and business continuity planning needs to be business-led. These statements are supported by BS 25999, the Business Continuity Management British Standard, which was launched in 2006 by BSI British Standards.

Business Continuity Management - Bridging the divide

BS 25999 (2) states that:

Business continuity management is a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- ◆ proactively improves an organisation's resilience against the disruption of its ability to achieve its key objectives;
- ◆ provides a rehearsed method of restoring an organisation's ability to supply its key products and services to an agreed level within an agreed time after a disruption; and
- ◆ delivers a proven capability to manage a business disruption and protect the organisation's reputation and brand.

BS 25999 also states that 'top management' participation 'is key to ensuring that the BCM process is correctly introduced, adequately supported and established as part of the organisation's culture.'

So, best practice is clear on this issue, but why do so many organisations fail in this area? Partly this is because it is a 'work in progress'. The call for board level involvement in business continuity management is a recent one and for some organisations this requirement has simply not filtered through yet. However, for others there are more serious systemic reasons. In some organisations the IT department operates almost as a closed-shop. It doesn't appreciate the business and operational needs of the wider organisation and the rest of the organisation sees IT as a non-understandable realm of science fiction, which communicates in a different 'tech-speak' language.

These caricatures may be exaggerated, but they exist. And from a business continuity point of view it can cause serious difficulties in both the development and management of business continuity programmes.

Examples include the following:

- For the development of a BCMS, the business representatives who are responsible for this need to decide upon two key metrics: the recovery time objectives (RTOs) and the recovery point objectives (RPOs). These are the time frames within which critical systems are restored to a working capability and the point in time to which systems and data should be restored following an incident. Since critical systems will inevitably include IT, the IT department will need to be actively involved in providing information for the determination of RTOs and RPOs. The business needs to be able to clearly articulate what information it requires and the IT department needs to understand what it is being asked for and must provide the information clearly and accurately.

- Another area where the business-IT gap can cause major problems, and even complete failure of the business continuity management system, is in the business impact analysis (BIA) phase. Here the owners of the business continuity process need to understand exactly what is mission critical in terms of all business processes and systems; including those which reside within IT. What frequently occurs is that the BIA includes top level systems, but lacks granularity. This happens because the business does not appreciate the complex dependencies and interdependencies which exist in the IT systems and therefore it fails to ask IT the necessary questions to encourage it to drill down within systems to highlight critical sub-components and to achieve an appropriate level of granularity.

How to bridge the divide?

It is clear that for a business continuity management system to be successfully developed, some way must be found to bridge the gap between the IT and business focussed aspects of organisations. The following measures will help:

An Appropriate Sponsor

What is clearly needed is an 'ambassador': a person who can understand both 'sides' of the divide; someone who can speak both the language of the business and that of the technician; and can understand the needs and requirements of both. Many organisations find that this is where the help of an external consultant can be extremely useful. Kavanagh, in particular, offers specialist help in this area.

External consultants can also bring in lessons and experience from working with other organisations ensuring that simple mistakes are not repeated and that the 'wheel is not being reinvented', thus preventing the resulting waste of effort and resources.

Best Practice and Standards

Standards are a very useful set of tools to help bridge the business-IT gap. They are developed to capture best practice and to help ensure that all the important elements of a process are documented.

In terms of business continuity management in the UK, there are two key standards:

BS 25999 Parts One and Two

BS 25999 has already been mentioned in this white paper, but its importance cannot be understated. It is not only a British Standard but is the *de facto* global standard for the development and management of business continuity programmes.

Business Continuity Management - Bridging the divide

BS 25999, the Business Continuity Management Standard, is split into two parts. Part one provides the best practice information (the Code of Practice) and part two describes the specifications of a business continuity management system.

Organisations can choose to use BS 25999 informally as best practice guidance, or they can go a step further and be formally certified as being compliant with the standard.

By following BS 25999 an organisation can ensure that it is 'doing things the right way' and that no corners are being cut.

BS 25777

British Standards recognised that BS 25999 was mainly written for the business and realised that a more technical guide was required to meet the specific needs of technology recovery. A companion standard was therefore developed to fill this gap. This is BS 25777, the Information and Communications Technology Continuity Management Code of Practice.

Using BS 25999 and BS 25777 together helps both the wider business and the IT department understand their specific roles within the business continuity programme and helps cover all the bases.

Testing and Exercising

Another very useful toolset for bringing business and IT together is testing and exercising. Every business continuity management system needs to be tested to ensure that it is fit for purpose and to highlight any weak areas. The BCMS also needs to be exercised so that everyone involved in incident response and disaster recovery can practice and understand their roles. This ensures that they can respond quickly and efficiently in a real crisis.

Testing and exercising is helpful as it can be used to bring people together who do not usually meet for business purposes and this alone can help to break down barriers. However, having to jointly participate in a test or exercise and the subsequent debrief can help highlight areas of misunderstanding that need clarifying. A failed test should not be seen as something negative, but instead as a positive opportunity to improve the BCMS.

A test or exercise is only as good as its facilitator. However good the underlying business continuity management system is, a poor facilitator will result in a substandard outcome. Again this is where the experience of external consultants can help.

Conclusion

The best and most effective business continuity management system is developed through taking a holistic approach. However this does not come naturally to many organisations, where a divide often exists between the IT department and the rest of the business. Given that IT is such a central part of many business continuity plans there is a strong temptation to delegate business continuity to the IT department. This should be actively avoided. Business continuity must be led by the business, but the business needs to be able to communicate with the IT department and understand its technical language and highly complex infrastructure. To fail to achieve this will inevitably result in a sub-standard, potentially worthless, business continuity management system.

The authors

Tony Stranack

Tony Stranack joined Kavanagh in 2006. He holds a BSc in Computer Technology, and has 20 years experience of working in the IT industry. Before joining Kavanagh, Tony worked at EMC for 12 years, where he ran the UK Business Continuity Practice.

Tony brings to Kavanagh and its clients a unique depth of knowledge of IT including substantial experience of practices and processes within the operational environment. Tony has been trained to auditor level in the BS 25999 standard and he has a wealth of practical experience in business continuity management.

Charlie Cornish

Charlie Cornish joined Kavanagh in 2007. He holds an MA in Engineering from Cambridge University and has 19 years of experience in Information Technology and Programme Management. Before joining Kavanagh, Charlie was IT Director for Aspect Software, a leading provider of contact centre solutions. Previously Charlie worked for other blue chip organisations including Vodafone and Thorn EMI.

Charlie has a breadth of experience delivering tactical and strategic customer-focussed IT services and support to global organisations, in both the infrastructure and applications arenas and is trained as a BS 25999 lead auditor.

Kavanagh and BSI

Kavanagh has been awarded membership of BSI's Associate Consultant Programme (ACP) for the Business Continuity standard BS 25999 and advises clients wishing to achieve full BS 25999 certification or simply follow BS 25999 as best practice.

www.kavanagh.co.uk

Business Continuity Management - Bridging the divide

References

- (1) 'A Decade of Living Dangerously: The Business Continuity Management Report'
Patrick Woodman and Dr. Vidal Kumar, The Chartered Management Institute, March 2009
- (2) BS 25999-1:2006 BRITISH STANDARD Business continuity management, Part 1: Code of practice. BSI British Standards