

Building-in BC robustness

Developing an efficient business continuity plan involves laying down the right foundations to build a solid strategy including regular testing and monitoring

Business continuity can mean different things to different people and this is one of the major issues for organisations; what can be considered a thorough BC strategy by some can be seen as lacking by others. This is not only the source of significant challenges at industry level (how can end users be confident that businesses in their supply chain have taken the necessary steps to ensure continuity in the event of a disaster?) but how do you address this discrepancy when it exists within the same company? How can an organisation's management team trust that various departments have worked together to make sure that the business is protected should disaster strike?

Back in 2007 ISO, the International Organization for Standardization, published the ISO/PAS 22399:2007 Societal security – Guideline for incident preparedness and operational continuity management. This was the first internationally-ratified benchmark addressing incident preparedness and continuity management for both the public and private sector. According to Dr. Stefan Tangen, Secretary of technical committee ISO/TC 223 'ISO/PAS 22399 represents a major breakthrough in addressing emergency and disaster preparedness, response and continuity. It was unanimously passed by the 50 countries that participate in the committee and provides an international agreed upon benchmark for emergency and disaster management for individual organisations.' In the UK the British Standards Institution has created BS 25999, a Business Continuity Management Code of Practice offering general guidance, and the Specification for Business Continuity Management, listing the requirements that can be objectively and independently audited.

So where should companies start to build a sound BC strategy? Marcie Terman, Business Development Director at DataFort recommends that first and foremost it is imperative that each unit within the organisation lists the core resources needed to continue to operate in a productive manner following equipment failure, a loss of power, data, etc, any tangible point of risk within their department.

"It is important to outline how quickly these resources need to be brought back online to prevent disruption," says Marcie. "Then, based on these criteria, the IT department should draw up the core elements of its business continuity strategy. Although the particulars will differ from company to company, they should all ensure that the Recovery Time Objective or RTO (how long you have to recover the data or system before its absence causes business continuity problems) is equal to or shorter than the Maximum Tolerable Outage or MTO. If the RTO is longer than the MTO then business continuity is not ensured and the business is still at risk. Recovery Point Objective or RPO (how much data the organisation can afford to lose or re-create) is also key; this factor will have a dramatic impact on the data protection strategy



because if your business is involved in any sort of high-volume or intraday trading, currencies or commodities for example, synchronous data replication or mirroring will be your only choice."

Making changes

But all the above planning will fall like a house of cards if the strategy is not seamlessly deployed across the organisation; in fact, in order to ensure continued operations, a business continuity strategy must be managed centrally to maintain focus on congruency between changing systems and the protection of those systems.

"Let us say for instance, that human resources demands to manage its own backup strategy, say through tape backup, because of the regulatory requirements posed by the Data Protection Act," explains Marcie. "However it has no training or method to make sure that those tape backups remain effective, and therefore cracks will develop in the BC strategy and these may result in a breakdown in the level of protection. So, while departmental management is not a good idea, departmental input is key; because your HR →

Testing is a challenging yet fundamental aspect of any BC strategy because it highlights any holes in the plan

(from previous page)

division will be highly aware of changes in legislation that will directly impact the data protection and retention policies. Other departments like finance will have their own very valid concerns too."

Once the core elements of a business continuity strategy are in place, organisations should look at processes that will keep it in step with changes in the business and relevant policies. A sound starting point is to take a good look at the company's business processes and its systems and understand their real risk exposure. For example although generally speaking an organisation located in central London is more at risk of terrorism than one based in a smaller town, the actual risk of terrorism is dwarfed by the risk posed by striking unions that may directly impact the ability of the business to maintain normal operations. Therefore it is important to take an objective stance in order to balance the impact of risk vs. likelihood.

"Companies are rarely static, and to offer ongoing protection, a business continuity strategy should

constantly evolve to match that company's needs," says Marcie Marcie Terman. "This fluidity requires not only intimate knowledge of the business but understanding of both new technologies and relevant legislation. This often makes the use of an outside consultancy more cost-effective than relying on internal staff shifting their focus from business process development to devote time to keeping on top of the latest BC requirements. When you add the cash flow and efficiency benefits that come alongside the adoption of the service-based delivery method for business continuity, this becomes an attractive, low-risk option for many businesses."

Testing times

So you have designed and implemented a BC strategy, you are making sure it changes with your company's needs so now it's time to make sure it works. This is because it is unlikely that the paper version is going to unfold flawlessly in the real world. Testing is a challenging yet fundamental aspect of any BC strategy because it highlights any holes in the plan. Tests should be performed at regular intervals, at least once a year and ideally much more frequently, especially for organisations which are subject to strict regulations such as those in the financial, health and public sectors, where failing to conform to the criteria set out by bodies such as the Financial Services Authority (FSA) can lead to debilitating fines that can put a company out of business.

BC and the manned guarding sector

The recent cold snap has once again brought into question the UK's readiness to react when external events threaten to impact on public and private sector operations

According to Advance Security's Managing Director, Richard Bailey only by working towards the relevant business continuity accreditations can the security sector truly understand the issues facing clients in their quest to deliver 'business as usual' in their respective industries – irrespective of the conditions.

"As representatives of an industry that sells itself on protecting public safety through effective risk management, it is imperative that we are wholly confident in our capabilities to deliver a watertight service amid any crisis. That's why we've long championed the business continuity message," says Richard.

"When the avian flu scare hit three years ago, business leaders were banging the business continuity management (BCM) drum loud and clear. Though the threat was real, the flu pandemic that focused attention so firmly on the discipline of BCM turned out to be somewhat exaggerated; and while it gave us the opportunity to put our client plans to the test, it also had an adverse effect on public perception. Those that had held up business continuity management procedures as a priority measure were seen, by some, as creating unnecessary hype.

"Now, following last winter's big freeze and the ongoing impact of similarly icy conditions currently affecting the country, business continuity is back on the agenda. From snow chaos through to G20 protests and the London tube strikes, the security sector has a duty to deliver an uncompromised level of service at all times. What's more, with the recent spending review leading to talk of public sector strikes, there is a very real risk of public services being affected; transport, policing, even waste collection – with perhaps the additional problem of picket lines to cross.

"If the threatened strikes take place the private security industry will be leaned upon to ensure the security of UK private and public infrastructure. Not a problem for the majority of security providers; but for those without adequate BCM systems it will be difficult to guarantee that their officers will be on duty, on time as required – despite the problems they might face in getting to the front line. The potential impact on the perception of the security sector as a whole could be extremely negative.

"Arguably such events are by and large beyond the security industry's control, but in order to protect clients' assets and ultimately ensure public safety the security sector must have the provisions in place to cope. If we can't show evidence of proactive business continuity management, how can we expect our clients to follow suit?

"It's time we took it upon ourselves as an industry to ignite a supply chain reaction by showing a demonstrable commitment to business continuity management (BCM) and seeking a similar stance from our suppliers. Only by investing the necessary time and resource into getting our own houses in order first can we add real value for our clients and confidently deliver in a crisis," concludes Richard.

"In order to virtually eliminate the chances of the plan failing to work an in-depth test should be carried out at least once a year"

"In order to virtually eliminate the chances of the plan failing to work an in-depth test should be carried out at least once a year; this would not only ensure that everything works at the technology level (including any new elements of the IT environment) but it also helps new staff become familiar with the various steps needed to keep the business protected," says Marcie. "But testing and the resulting changes can take time so in order to minimise disruption it should be performed at times when the organisation is less busy, for example over the holidays."

Businesses aiming for a watertight strategy should have detailed documentation of the plan and policies so that it can be shared between relevant staff and passed from incumbent to new employees. They could also make a full time employee responsible for the company's BC strategy, someone who knows its every aspect inside out, from data security and recovery, to communications networks and SLAs. For a belt and braces approach, if budget allows, a secondary backup system could be deployed where an additional data centre or site with mixed storage media would provide an extra layer of protection depending on the scale of the disaster.

"When the survival of your company is at stake, it would be foolish not to put a strategy in place that could make all the difference; the key is in striking the right balance between risk and protection," concludes Marcie.

Standards in business continuity

Monthly business continuity comment by Lyndon Bird FBCI, Technical Director, Business Continuity Institute

Although there is very little debate about the need for a more consistent and professional approach towards Business Continuity Management, there are considerable differences of opinion about the value of a formal standard of the type routinely accepted for quality, environment, or health and safety. Although the British Standard BS25999 has been around now for several years, the number of companies who have submitted to the full rigours of acquiring formal certification is not very extensive: We are still talking a few hundred organisations, rather than the tens of thousands some might have imagined when it was launched.

While this relatively low level of certification is undeniable - and some question whether the BCM profession has failed to make a compelling case for standards or the standards themselves have failed to deliver sufficient business benefits - record numbers of firms have enthusiastically bought and studied the BS25999 Code of Practice; so the more fruitful discussion is about how companies 'align' with or 'self-certify' against such guidelines, or even a more detailed programme such as the BCI's Good Practice Guidelines, and how this compliance can be adequately assessed or proven, short of formal certification.

Another key consideration in the standards discussion is end-user appetite for new BCM standards: it would certainly be a reasonable observation to say that there is greater enthusiasm for new BCM standards among standards bodies than potential end-users. As well as BS25999 there are national BCM standards from two ANSI approved US standards writers (NFPA and ASIS) as well as from Singapore, Malaysia and, fairly recently, from Australia/New Zealand. At ISO-level, ISO22301 (specification) and ISO22313 (guidance) are due out over the next twelve months. To add further complication, ISO are also working on an Operational Resilience standard which might well overlap with their BCM offerings.


A seasoned and well respected BCM professional has observed that: "Given the development of many new standards within the field of business continuity, there is a danger that some of the benefits of developing an industry 'code' or standard are eroded. The very definition of the term 'standard' as a level of quality or excellence that is accepted as the norm or by which actual attainments are judged, is at risk as the diversification of standards increases."

In the United Kingdom, the development and continual improvement of the British Standard is under the control of the BCM/1 committee - a group of industry experts representing organisations like the BCI. In spite of this control, there has been much proliferation in the form of Publicly Available Specifications (PAS) and Published Documents (PD). While PDs add valuable detailed explanation to the standard, PAS's are written by a typically smaller group of interests that do not need to seek the wide consensus of a full standard. The PAS approach can therefore cause confusion when it is at odds with an official standard over key issues and concepts.

Despite these challenges, standards for BCM are here to stay, and the probability is that the release of ISO 22301 will bring - at last - some standardisation to BCM standards.

Get Your Fire Training From The Professionals

- All levels covered from entry level to specialist
- New courses added for 2011
- Most comprehensive technical fire safety training available
- Wide range of locations nationwide
- More than 30,000 professionals trained - CIBSE CPD approved



Fire Industry Association
Training for a safer future

For details and dates go to www.fia.uk.com




Looking for a more intelligent way to control and monitor keys and equipment?

Cutting operational costs and reducing administration time, significantly, Traka's intelligent access management systems can be configured for a wide range of applications, and tailored to suit the way you want to work.



If you'd like to know more about Traka, call 01234 712345 or visit traka.com