

Question :

The BCI is committed to promoting “the art and science” of business continuity management; can you elaborate on that statement and explain the philosophy behind it?

This question can only be explained by looking at the whole Business Continuity Management lifecycle. In order to successfully implement business continuity into an organisation it is true that you must provide appropriate practical technical solutions like IT service continuity, network resilience and work-area recovery. These are the “hard” elements of the process, which we can call a science. However equally important are the “soft” issues like understanding how people might react in a crisis and making BCM fit in with the corporate culture. In fact we are increasingly recognizing that these issues are usually what makes BCM succeed or fail. We tend to think of these challenges more as an art than a science although (as in all art-forms) techniques, rules and skills still apply. In some ways it is really about predictability; when you are dealing with technical processes you can predict outcomes to a high degree, whereas when you are dealing with people and random events that predictability is much reduced. A skilled BCM practitioner must be able to understand the nuances of the organisation he or she is working for. For example when you conduct a Business Impact Analysis you must learn to drill down beyond the basic questions and get to the heart of the business. You need to ask not just how can we replicate what has been lost but can we find a better way of doing it. Teasing answers to such questions takes imagination, tact and people skills of a high order - a good mix of art and science I believe.

Question :

What is the BCI’s relationship with the BSI (British Standards Institute) like; how does it benefit each organisation and businesses in the UK and abroad?

The relationship with the BSI is excellent but to some extent misunderstood by some of the BCM community, particularly outside of the UK.

The primary purpose of the BCI is to develop individuals so that they can become genuine Business Continuity professionals. We believe that only by creating a proper BCM profession can the discipline be given the attention and importance it needs. When an individual gains BCI accreditation and ultimately statutory membership of the Institute, they demonstrate to their company, their manager and any future employees their professional standing and competence.

The role of the BSI is different in that it is a national standards body, involved with every conceivable area of activity of which BCM is just one. In order to develop standards it does, however, need to determine firstly there is a need and secondly there is a viable way in which a standard can be developed. The BSI decided that BCM was one area in which a Management Systems standard was desirable and worked with all industry players to develop one (BS25999 parts 1 and 2). The purpose of a standard of this nature is to ultimately provide accreditation for organisations, not individuals. The BCI played a leading role in the development, providing its chairman and a number of key players on the technical committee but it is a British Standard not a BCI Standard.

However there are obvious synergies, The BSI are very keen on the BCI to professionally accredit their BCM auditors (particularly in Japan) and the BCI believe that part of successfully achieving BS25999 compliance should include the need to employ professionally qualified practitioners in key BCM roles. Much work is ongoing and the BCI and BSI are talking to each other on a range of issues that include publications and joint promotional activities as well as BS25999.

Question :

Does the BCI hold any best practice for managing/controlling conference calls, particularly in a crisis situation?

Incident Communications Protocols

During incidents speed and accuracy of communications is vital since invariably information is scant, incomplete and changeable. This type of crisis communication is different to business as usual when there is more time to prepare, think and respond taking into consideration emotions and human body language. In a crisis you need a style that meets the environment and situation.

Face to face is the preferred method of communications because it can inspire confidence, calm emotions, add humour and communicate all the non-verbal associated messages like leadership, compassion, loyalty, knowledge, mental agility, coolness, command presence and so on. In this case during emergencies there is often a need to rise above the noise and distractions of the event.

The Army use the acronym CLAP for giving orders under fire. This means Clear, Loud, As an order, with Pauses. Fire marshals, evacuation managers and emergency personnel might consider this style for one way information using voice by shouting, PA systems and megaphones.

For a conversation referring to two way communication this shouting style is inappropriate because listening and speaking must take turns to be effective. Face to face is preferred because you can check understanding by nodding, smiling, winking and body language. It should be noted there must be pauses for questions and a check of understanding that the message is understood by the reply. If the voice conversation is over a technical means such as a telephone, 2 way radio then there are protocols to prevent two or more parties speaking at the same time by saying "over" or by punctuating the end of a sentence with OK? Get that? All right? Yes? This allows the other or others to reply and confirm understanding.

Hotlines are good for leaving up to date messages that anyone can access and can be circulated in advance (on a wallet card for example with any entry codes). A simple alternative is to use a mobile phone or landline answer machine with a recorded message then switch it off and circulate the number so many can dial and listen without having to answer each call. At regular intervals this message can be updated. A template is suggested for leaving a hotline message, kept in the battlebox, as a prompt of the kind of information required.

During incidents at weekends, or nights, or when distances are a challenge, or when face to face meetings are inappropriate (such as infectious disease or due to the proximity of danger) then the quickest way to convene a team is virtually on a voice conference bridge or web blog. The loss of observing body language can be a downside. There are some protocols that will assist in effective communications for incident management teams.

Conference bridge numbers are circulated in advance (on a wallet card for example with any entry codes)

A leader of the call is appointed and all comments are approved by that person.

Pre-selection of those people identified to be on the call (and the ability to request more people or downsize as necessary)

Create an agenda so everyone knows what is to be discussed in which order.

Appoint a scribe to take minutes and circulate the minutes as action points.

At the end of each topic a round table is conducted so everyone gets a chance to ask questions or confirm their understanding.

Keep discipline and if there are other issues take them off line.

Prevent distractions by turning off other phones/TV/Radio (a quiet, warm, well lit room rather than standing in the howling wind by a generator and police siren!)

Set future times for further calls (for example on the hour every hour or each day at noon) depending on the frequency required.

Web blogs are good if the technology is available. Communication is in real time, there is an audit trail and contemporaneous record of what is said. There are software systems that have these facilities for incident management.

Text messages (SMS) and pagers are useful and used widely for example the City of London Police have a pager alert system. SMS messages were more reliable over congested networks than mobile voice communications. Text is good for broadcasts (one to many) for cascading information. It can be used for conversations between two but becomes unmanageable if several replies are being sent simultaneously.

Email alerts using mobile devices such as Blackberry, MDA, palm-pilots, mobile handsets and wireless laptops can be used but are not ideal for conversations involving many participants.

If there are group meetings held for the cascade of information issue the facts in hard copy as well as having them presented to avoid speculation, omission or forgetting what was said in the heat of the moment.

Dealing with the media is a different topic not addressed here. This is dealing with internal communications. That said, short wave radios, TVs, web and walk technology is all useful to receive information from news sources. Note : news is not always fact. Note also citizen journalism is real time to most media channels and the speed of response of the press is within minutes if not real time.

There is no substitute for having a rehearsal because human behaviour will influence the style and mode of communications.

There is also a good Powerpoint presentation presented by Jamie Jameson at the 2007 Symposium "Virtual Teams within Business Continuity – a new Norm?"

Question :

An explanation of the terms MTO and RTO. I have seen the glossary for these 2 terms however, it would be helpful to have these explained as there are several interpretations being discussed throughout different areas. The MTO and the RTO seem very similar and I would appreciate your help on this with a definitive, simple explanation.

An example of some of the interpretations are:

MTO:

At what point in time do you need to either recover your lost business processes, or invoke contingency procedures to prevent you from failing to meet your business objectives/targets, or that it is:

This is the period of time by which a business process must be restored.

RTO:

How long can you continue to use your contingency procedures without the services you lost before you fail to meet to business objectives/targets?

or that it is:

The target set for recovering services to allow business processes to be resumed within the MTO

MTO I think has been a RPO RECOVERY POINT OBJECTIVE mixed up with MAO Maximum Acceptable Outage.

RTO is Recovery Time Objective.

I think the easy way to understand these terms is to think of a shop till in a bakers.

If the shop till fails there may be a finite time while cash can be taken for items. If there are codes for bread and codes for cakes the manual system can work for a few days but then there will either be too much cash to count or a danger of losing the integrity of how much is 'cake money' and how much is 'bread money'.

The RT is how long the time is to get the till working. It could be an hour it could be a week. The RT Objective is the pre-identified time in which the recovery should be completed. That is to have a working till.

This can be judged in a business impact analysis (BIA) against other tills or shops or bakery products to see which is more time critical. It may be judged in comparison to any factor such as time, volume, revenue, cost, people, skills, space etc depending on what the appropriate measures are.

The RP is the point at which the transaction is lost so that judgments can be made for synchronisation. Say the till was emptied last night and a new float issued this morning. Bread and cakes have been sold before the till broke. We have the cash for them but might lose the data of what was bread money and what was cake money. If we use a manual system and take cash and sell bread and cakes without using the till but writing down each transaction we will still have a problem once the till is repaired. The till will be out of kilter with the stock and cash.

The problem is how do we reconcile all the transactions after the till broke (including the ones we lost before the manual system got started (bread versus cakes)). We must have some points of known data. This is not a time but a place in a transaction. Last night we reconciled the till, cash, bread and cake stock... that might be an RP. We can add all the manual transactions to the till once it is repaired... that might be an RP. We can count the cash taken before the till broke that might be an RP. We could count all the bread and all the cakes left and that could be an RP.

The RP Objective is the pre-identified place at which all data is synchronised so we can move forward again without fear of losing any transactional integrity.

MAO is a point or time beyond which loss cannot be tolerated. This MAO, if reached, will mean we have to stop and reconcile/recover/invoke other contingencies because further loss cannot be accepted. Sometimes this is set by a contractual obligation, a service level, a regulation or a standard. It would mean your organisation would have to set any RPO or RTO within the MAO to achieve compliance.

Question:

With respect to Business Continuity Planning does the plan cover the employee's families as well ?

A simple answer is "yes" if you want to ensure your plans will work and reflect reality.

A business continuity plan should be viewed as a service level agreement between your organization and key stakeholders when bad things happen. Your employees and their families need to be recognized as key stakeholders ahead of your business interests. Anticipating how your employees will react in an event key provides a more realistic plan.

For example, I can recall during September 11th sitting in an emergency operations centre and receiving an email from the business executive in the early afternoon saying that due to the tragic events that occurred that morning, businesses could close for the day. The problem was that the place was already deserted. Many employees had made their own decisions to go home. They needed time to absorb the event and manage their own feelings. People were overwhelmed by the events that they observed and needed time to connect with their families, friends, neighbours and their local community. Once they were able to reconnect with their families and community, they considered coming back to work.

Clearly, employee families are key stakeholders that businesses must include in their planning assumptions. Ensuring that communications systems have the increased capacity to allow staff to communicate with their families in a timely manner are essential, if you want to keep people from deserting or being absent from work.

In Vancouver Canada public officials have recognized that there is a 70% chance that people will experience the next earthquake while at home. (This is because in a 24 hour day 70% of the day they are at home or in transit to work.) They also recognize that due to the potential overload of demands, possible damage to the transportation infrastructure, (i.e., falling debris and bridge damage) that communities should plan to be on their own for the first 72 hours. (That is - no professional help of police, fire or ambulance service for the first 72-hours.). The local businesses are responding to this and focusing their business continuity efforts on personal preparedness plans with

earthquake kits and supplies based on these planning assumptions. The more prepared staff are, the more likely they are to come to work.

Personal and family preparedness is also a crucial element of pandemic planning that requires social distancing to keep those that may be infected from the public and work colleagues, to ensure continuity. To ensure business continuity, many organizations have developed work-from-home strategies that provide staff with the technology to ensure portability to attend to their ill family members and also work from home. Some of the more robust pandemic plans anticipate the full scope of family demands during a pandemic outbreak that includes stocking of hygienic supplies and support kits as well as child and elder care support initiatives.

The positive benefits of a plan that includes employee families are increased productivity, staff morale and reduced turnover of staff. In turn, the businesses can have the confidence that their plans reflect reality and avoid surprises. Understanding the priorities of employees and their families and anticipating their issues will ensure more robust business continuity plans that will have a greater likelihood of success.

Question:

Where is the general business executive on this issue? How would you characterize the general state of business-continuity/disaster-recovery planning among businesses, especially in the United States?

Much better than 5 years ago but still not getting the top management attention it needs. 9/11 did highlight some issues relating to risk that had not been taken seriously before. For example, a first realisation of the sheer magnitude and geographic scale that could be involved in a disaster. Most organisations assumed that they could plan for a building and perhaps a police cordon area of 500m or so. With most of Manhattan closed down some organisations had over 10 locations simultaneously affected so if any of their plans assumed those facilities to help, they just weren't.

Companies also learned a lot about people issues and how they would handle a crisis. In this situation, even if you are OK physically, you would not be mentally. Your priorities would be home and family not working hundreds of miles away to help recover the systems. Many people never fully recovered from the trauma and this has long-term affects on Business Continuity.

The DR companies like IBM, SunGard etc of course had many more invocations than they could ever have planned for and the whole viability of that industry in dealing with a concentrated terrorist attack came into question, leading many organisations to consider having their own dedicated solutions.

Immediate aftermath communications (or in some cases lack of them) was a key lesson to be learned for many organisations. Do not take the infra-structure for granted, do not assume you will always have telecoms, Internet or even power.

Also the lack of understanding between corporates and public authorities was highlighted and has lead to closer involvement between BC/DR professionals and the Emergency Response community.

These were good lessons and many of them have been applied. Nevertheless much of the planning is still done at operational with only limited tactical planning and virtually no real BCP component in overall Business Strategy.

Question:

Are there particular industries that are doing it particularly well and some that are still hesitant to invest the time and resources? Or is the split more between large and small companies, regardless of industries, for example?

If you split the whole BCM space into Technology Recovery, People Continuity and Crisis/Incident Response you can say that global financial services companies are extremely proficient on the Technology side of things. However we all still have concerns about the effectiveness of the actual Crisis Response and more particularly the HR elements of effective Business Continuity. Without people the most automated operation in the world will still fail, so having the right people doing the right things in the right places at the right time is absolutely vital.

In general regulated industries like banking, utilities and insurance are more involved in BCM than those who have no real statutory duty to undertake it like pharmaceuticals, chemicals, engineering and manufacturing.

However in the US there is no a move towards a voluntary BCM certification programme, in a bill recently approved by the President. Although voluntary this is likely to bring more and more medium to large sized organisations on board.

Of the SME sector, 52% of all businesses affected by 9/11 never opened their doors for business again. Are these small companies any better prepared now? Probably not.

Question:

What is your elevator advice to the business owner that might see the value in BC/DR planning--but still doesn't give it the effort it requires because of immediate profitability concerns?

No modern company can survive a major interruption to its core business processes for an extended time and in some cases no interruption at all is acceptable. Although much of the recovery must be delivered by IT Management, IT do not own the BCM process. They are a key component of delivering the implementation strategy - but ultimately the responsibility lies with the Board. Deciding on the level of risk the company is prepared to take is a Board decision and deciding what systems, services, locations and business processes are vital post-disaster are business decisions. Business Continuity is not just about disasters, it is about designing in resilience to all your key businesses processes.

Question:

Is BC/DR becoming a competitive differentiator? For example, do companies ever ask about vendors' plans in RFPs?

Yes this is always key to effective response and recovery. Europe seems to be slightly ahead of the US in this aspect, where proven BCM capability is becoming more and more a core criterion in supplier selection. Outsourcing or off-shoring without absolute confidence in supplier BCM is very risky and most organisations are demanding it.

National and international standards in the BCM field are also making it more possible to demand a coherent and consistent minimum standard of BCM practice from suppliers

The really big issue in BCM now is Supply Chain Continuity. This can be manifested in different ways. For example a disaster in Asia might mean a break in a key part of a US or European supply chain. This might mean loss of business and cash, it may mean loss of market share or reputation, and of course one company's disaster can be a competitor's opportunity. Service delivery failure might well be picked up by the media, leading to loss of confidence from customers, suppliers or investors. In relation to most events there will be key people issues which need managing.

Question:

What are the big regulatory concerns on the table in the area of BC/DR?

Many and varied, particularly in the US but also on an international basis. What does appear to be needed is the emergence of common standards for BCM that can be applied across all business sectors and geographical areas. This is a complex task but one that is getting much attention. Many people look to ISO for a commonly accepted BCM standard and this is starting to emerge. However currently we find that various national BCM standards are wrestling for prime position. The two main contenders have been ANSI/NFPA1600 and the BS25999 standard.

There are also other countries actively moving on a standards agenda that differs from both BS25999 and NFPA1600. In particular much work has been carried out in Australia and Singapore. Standards Australia have produced their Business Continuity handbook HB 221:2003 which although not a formal standard is being informally treated as one in Australasian territories. The Australian Prudential Authority (APRA) has also implemented regulation for the finance sector via their standard APS-232-BCM.

The Singapore directive TR19:2005 on BCM is mainly related to IT Recovery standards and has replaced the earlier and somewhat wider SPRING directive of 2003 which was itself based mainly on the early UK standard PAS56.

ISO have tried to pull together a number of national standards bodies and have recently released ISO PAS 22399 which is designed at incorporating the best from the US, UK, Australia, Japan and Israel standards. A PAS is not a full standard and it might take a number of years before it becomes one. It is currently called "A Specification for Incident Preparedness and Operational Continuity" which does seem to add an unnecessarily further confusion when all the source standards it has consolidated have used the established Business Continuity nomenclature.

In Japan and Korea, firms are already starting to get a preliminary assessment against BS25999 even though it is not officially globally launched until 30th October. In the UK, all of the certification bodies are putting their programmes in place to start accredited firms against the standard immediately after launch. It appears that the US is still ambivalent about the value of this approach, but the rapid international take-up will probably result in US global firms being involved for their overseas operations at least.

The drive towards standards is not only through ISO and its national member organizations. The law has also taken quite an active (if often badly understood) role in BCM in recent years. The most obvious example was Sarbanes-Oxley, which forced firms to re-think their entire internal controls and corporate governance. However more directly related to BCM is the new law titled "Implementing Recommendations of the 9/11 Commission Act of 2007". It is also called HR1 and Public Law 110-53 and is likely to have much impact in the North American business continuity community, even though the program is currently voluntary. Whether this law (which aims to create a certification program for all-hazards business emergency preparedness) will have any impact beyond the US and Canada is questionable, however, as the ISO and other national standards will be well established before any results of this initiative become available.

In addition, and in some ways the most powerful driver are the standards being imposed by regulatory bodies. There are already strong guidelines from the financial regulators in the US and the UK and effectively mandatory rules on BCM in Singapore and Malaysia. Australia's regulator APRA has issued a draft standard that they expect to make fully mandatory. The international nature of this sector of business and the economic power such global firms possess is such that worldwide consistency for financial markets is very important. There is clear evidence that there is a coming together of BCM thinking amongst the various financial regulators, which is likely to be a strong driver for more standardisation. The Basel Committee on Banking Supervision, Joint Forum has issued a 7 high-level principles document for BCM that individual country regulators will look to enforce. The countries represented were: USA, UK, Canada, France, Netherlands, Hong Kong, and Japan, so although not universal it does represent most of the major players in financial markets. These

countries have agreed to adopt these principles in their inspection and accreditation regimes, although the precise details of individual country schemes will vary.

Question:

Does BCI recommend any sort of formula to a business in terms of how much time and money to invest in this planning (e.g., X percent of total revenues)?

No but we have launched a free benchmarking tool that we can use to analyse current trends and comparisons between regions, sectors, business size etc. Information from this might eventually help with this type of metric. However we do recommend that firms follow the stages defined in the BCI Good Practice Guidelines (and also now in BS25999). This starts with "understanding your business" and the outcomes of this are certainly the main drivers to justify strategies, manpower and budgets.

Question :

It seems that, in today's political climate, government should be more involved in BCM and the associated disciplines, particularly with the threat of international terrorism and wide-scale natural disasters. What is the BCI view on this?

Naturally we are in favour of a wider understanding of BCM and its importance to business and the community and government does provide the best vehicle to achieve this awareness building. In the UK, The Civil Contingencies Act (CCA) has put quite a lot of BCM responsibilities on local government primarily through their Emergency Planning arms. This has given additional importance to this area but some think that it largely missed the point of BCM.

BCM is not driven by threats or by specific scenarios whereas Emergency Planning almost entirely is. Putting BCM responsibilities in the public sector within Emergency Planning gives entirely the wrong message. In the same way that for many years BCM had to fight the misconception that it is what you do when your computer fails, now we have to fight the equally invalid view that it is what you do when something "big and bad" happens.

As anyone who knows anything about BCM will tell you, BCM is really only driven by consequence and timeliness. A massive fire to an office block is newsworthy but if no one is hurt and no key business processes interrupted it is not a serious business continuity problem. Conversely a minor problem that interrupts key business processes beyond the acceptable outage time is a serious BCM problem, despite minimal or no physical damage.

Perhaps this message is not exciting enough for governments. Most BCM problems have nothing to do with terrorism or natural disasters and even when such incidents do occur the failures and lesson learned are mainly about dealing with emergencies, not business continuity.

Question:

What country or organisation should we look to as an example of best balancing BCM guidelines and business, and why?

This is not easy to answer definitively because views differ about what is good practice and what is purely done for compliance. One view is that BCM needs to be purely business focused, not technology or incident focused. Most of the big-name organisations that are usually quoted as leaders in BCM are from the financial sector. Naturally non-stop ICT availability is essential to their business viability and as such their investments in BCM are both very costly and heavily technology driven. It is difficult to be certain but much anecdotal evidence does suggest, however, that the "softer" people based issues are given very little attention in some of these global financial conglomerates.

With regard to countries, BCM in its current form has tended to be an English speaking issue for much of its 20 years of existence. Starting in the US as Computer Disaster Recovery and then picked up and

extended as Business Continuity Planning in the UK it settled down globally as BCM in the mid 1990's. Last year at a committee at the European Union in Brussels it was asked if BCM was just "an Anglo-Saxon" thing or did other European countries also take it seriously. The answer was tactful but clear, the rest of Europe had a long way to go in incorporating serious BCM into their business models. Fortunately, things are starting to move in some European areas like Germany, France, Benelux and Switzerland but much more needs to happen in Southern Europe.

In the rest of the world Japan, Korea, India, Singapore, Australia and Canada are all becoming increasingly involved in international BCM activities but the US and the UK still lead the field in this discipline by a considerable margin.

Question :

The BCI has a code of practice and ethics for business continuity practitioners, which presumably gives customers assurance that vendors that are BCI members are reliable and provide quality services. How important is this to the BCI and its members?

Absolutely essential, without this a professional membership organisation has no credibility and therefore no real reason to exist. The BCI is not a trade body, it does not support or lobby for any BCM commercial interests, it purely represents the interests of its professional members.

We believe that any BCM professional needs to demonstrate four aspects of their suitability for membership of the BCI. These are: appropriate experience, knowledge of the subject, proof of currency of that knowledge plus impeccable professional standards in terms of conduct and ethical behaviour.

Companies look to BCI Membership as a guarantee of capability and standards in Business Continuity from people that employ or consultants they hire. As such we check our professional members against these four criteria. Any complaints made against members are fully investigated through a rigorous complaints procedure.

However I do need to emphasise the BCI are involved with certifying vendors. We do not evaluate or recommend vendors that provide BCM services – that is not our role.

Question:

According to a BCI survey looking into the after-effects of the July 7th terrorist attacks in London, 12.5 per cent of the respondents said that the creation of their business continuity plan was directly prompted by that days events. Is this a trend that the BCI still sees, whereby companies tend to only implement a business continuity plan after a major event?

In general , specific high-profile events do prompt organisations to re-visit their BCM provisions. Many surveys (not just from the BCI) show that despite the high profile nature of BCM and the increasing number of threats around the world many organisations still have no or limited BCM in place. This is particularly the case with SME (small and medium-sized enterprises) and if an incident does increase awareness of risk and better appreciation of possible consequences then they are likely to take a fresh look at their business. We would, of course, prefer that the incident did not occur at all but if it does and people learn from it that is at least positive.

It is quite worrying how soon companies forget. Immediately after 9/11, many senior BCM executives in major US corporations said how easy it was to get time on their main Board agenda to discuss improvements in BCM. Six months later it was difficult to get a time slot, 12 months later BCM had slipped off the top management radar again. Keeping top management attention is difficult unless dramatic events are having, so in a way it is easier to implement BCM in traumatic times.

It is important to remind people that BCM is not just for emergencies. It is something you do as a matter of good business practice. When no one questions the need for an appropriate BCM budget and just treats it as a basic cost of doing business, we will have arrived at a proper management discipline. The fact that top executives jump when some serious random incident (like a terrorism bomb) happens shows that we are some way short of meeting that aspiration.

Question:

One recent event in the UK has been a better BCM case study than all others, and that's the Buncefield explosion that took place in Hertfordshire in December 2005 when a petrol storage tank in a business park leaked. Why does this best illustrate the benefits of BCM?

Buncefield was a very good case study for BCM in the sense that it demonstrated a whole range of issues without the undue confusion created by loss of life or serious casualties. I have summarised a selection of these lessons as:

Firstly, it just happened "out of the blue", with no obvious reason, warning or prior experience to suggest it might. I suspect that if you had asked 100 oil industry executives the day before if it could ever happen, they would have laughed and said it was inconceivable. The site was totally safe, met and exceeded all COMAH, EA and HSE requirements and there was no history in Western Europe to indicate an event of such magnitude was possible.

Secondly, it happened at the most inconvenient time, two weeks before Christmas when demand for oil products was at its peak and many organisations were working at full capacity. For retail businesses or companies in warehousing, distribution, transportation or IT supporting retail, this was about the most critical day of the year that it could have happened. Demand was at peak, resource was stretched and resilience was at its lowest level – they were all very vulnerable.

Thirdly, it was those things that many had not planned for that caused the most concern, for example Police and other Emergency Service access restrictions. Lack of access to their own business premises (even if not damaged) caused anger and negativity. For example a transport haulage company felt it could operate easily from home if its Buncefield office was closed. What it didn't realise was that the police would not allow access to this undamaged garage area to remove vehicles. In this case, no lorries meant no cashflow, meant no business.

There are a host of other lessons to be learned and some very impressive recovery stories but we were able to analyse these more clearly because of the very fortunate fact that casualties were very limited and there was no loss of life.

Question:

Of course, both the Buncefield explosion and London attacks are high-profile incidences. Surely there's a case for BCM implementation to deal with more frequently occurring small-scale incidents?

We should not concentrate only on these high-profile media driven incidents. The majority of BCM problems come from escalation of a relatively minor problem (usually resulting from a breakdown in communication at some point) rather than a single "big-bang" incident.

If you look at the BCM life-cycle you will realise that the whole process is designed around understanding your business. What are the risks you face, how do they impact your business and what are you going to do about them. . To keep a sense of reality, some facts are worth noting:

Whilst bombs, fires and floods capture the headlines, almost 90% of business-threatening incidents are 'quiet catastrophes' which go unreported in the media but can have a devastating impact on an organisation's ability to function.

The media are mainly interested in deaths, casualties, management errors and good pictures, not the business consequences of poor planning.

Many of the causes are outside an organisation's control and they are often at the mercy of the emergency services or suppliers who define the timescale of an interruption.

The external perception of how well a company manage a crisis is usually determined less by the technical response and more by the perceived competence of the management.

In other words, anything that creates an unacceptable business interruption is a BCM issue. The important thing is how you manage it.

Question:

Many entrepreneurs adopt the 'it won't happen to me attitude' and think their business is too small to need a business continuity plan. Why should they bother?

Traditionally people have equated BCM with large businesses and expensive IT solutions. In fact BCM for a small business might be very simple but the steps to taken are the same.

Understand Your Business – often this is very easy for an entrepreneurial business to accomplish. The owner/director knows exactly what is vital and what is “nice to have”. BCM is about protecting that which is vital – not recovering your entire operation.

Develop a strategy – this again is for the vital things and might not involve recovery at all. An example could be to buy product in from a competitor and re-badge, another example might be to distribute inventory widely.

Implement plan and responses

Keep the plans up to date

The writing of a large plan is irrelevant, the important thing is to have reviewed your business for single points of failure and critical items and decided how you will address them – rather than making up plans on the hoof.

Question:

What about a sole trader, who works from home and has no employees? Why should they bother with planning for incidents?

Exactly the same as earlier item but maybe even more important – if you are taken ill and you have no staff to take over then you should define who needs to be notified by who (e.g. your clients, suppliers, bank, accountant etc to be called by your wife, son, partner etc.). You must give them all some basic guidance of what you want them to do during your illnesses.

Question:

Many entrepreneurs operating on a low budget believe business continuity planning is an unnecessary expense. How can small company owners keep costs down?

See earlier answers, there are not necessarily much cost in BCP, but obviously depending upon what you find in “Understanding Your Business” you might need to spent money on the implementation of the solution. This might be in IT backup, alternative accommodation or changing some aspects of your normal operations to make it less risky. NEVER buy a solution from a DR provider UNTIL you are fully certain that what they are offering is both NECESSARY and AFFORDABLE. It is no use spending so much on BCP/DR that you put ongoing operations at risk.

BCM is mainly commonsense and good practice – not expensive vendor pre-cooked solutions

Question:

What are key steps small business owners should follow when drawing up a business continuity plan?

See earlier answers and ANALYSE the problem before you BUY any “solution”. You might find that you already have everything in place you need to have good BCM – but maybe you just need to go through it in a disciplined way and get it properly documented, communicated and involve as many staff as possible in a test.

To be sure you get it right first time a specialist BCI qualified consultant would help – but again use sparingly for their expertise – don't just hand BCM over to a consultant to do it. You must own BCM, which means consultants can help but not DO.

Question:

How should entrepreneurs test their plan?

An untested plan is pointless but tests can be done in many ways. For example test your IT backups and recovery procedures not just on your own computers/networks but elsewhere. Test your staff understanding by a scenario walk-through, perhaps have an unannounced out of hours staff/supplier contact test, if you have an alternate building test its suitability and accessibility at a weekend or evening. You do not need to do a full test that puts your business at risk – check bits of it systematically until you are ready for an integrated test.

Question:

Many company owners forget people when it comes to planning for the unexpected. What are the key workforce issues to consider in business continuity planning?

Many and varied.

Firstly they might be killed or injured in the incident so how do you deal with that?

Secondly they might be traumatised by what has happened and unable to work – how do you deal with that?

Thirdly, current personnel might not be able or prepared to move to an alternate temporary location.

Do you incentivise or accept?

Also you might need additional skilled staff quickly – where from and how do you get them to be productive?

Multi-skilling staff, Crisis Leadership skills, Media Training, succession planning, HR involvement in trauma counselling, and just understanding what jobs are essential and what can be delayed are all massive BCM issues.

Question:

How can entrepreneurs create a business continuity management culture within their organisation?

It all depends on them. If they believe it is important it will be. If you consider BCM issues in all decisions at the top, so will everyone else. It purely comes from leadership and the leadership need to understand what BCM is all about – a strategic part of your business success, not a technical/operational recovery issue.

Question:

There are local BCM standards and guidelines in my country – how does the BCI regard these?

Firstly you must comply with any local standards that involved your organisation. Secondly you should also have copies of best international BCM practice, such as the BCI Good Practice Guidelines and BS25999 as they were probably reviewed when your local standards or guidelines were drafted. In addition there is likely to be an ISO Standard for BCM in the next few years & you should keep up to date with this.

The BCI is ideally placed to provide you with BCM information and developments world-wide.

Question:

Is the BCI relevant in the Southern Hemisphere as it seems to be a UK dominant institution?

The BCI is active in 80 countries world wide and is truly international in its stated growth directions. Independent academics tell us that they regard the BCI as unique globally in that the BCI represent main stream management thinking internationally through best practice Business Continuity Management. ISO status is next for BCM and is actively supported by the BCI.

BCI Chapters have been a popular development in Australia, Canada and Nordic countries.

Question:

Is there any legislation that says that my organisation must carry out business continuity management?

The answer officially is NO! There is nothing that says you must do it however reasons for doing it include:

Good corporate governance

good practice and shows key customers, clients etc that you are taking precautions to avoid any business interruption to your and their business

Good corporate image, brand and reputation

Might reduce or encourage favourable insurance premiums

Add value to the organisation, prospective customers may take your business as opposed to another organisation because you have robust BCM measures in place to mitigate against any business interruption and they don't!

Having some sort of BCM in place might be the difference between keeping or losing the business

Many customers/clients now include proof of BCM in business reviews, audits etc

Question:

Are there any plans to turn BS25999 into an ISO standard - similarly as it was done with BS7799.

There is currently an ISO PAS 22399 which has been adopted and is in circulation. Five national documents were used as source material: BS25999 (UK), NFPA1600 (USA), HB221 (Australia), a Japanese continuity standard that was earthquake-based, and an Israeli standard.

It is our view that much of PAS22399 is based on the UK standard, with some very useful additions from the other documents. The British committee had already had the chance to use the other documents as source material, so much of their thinking was already encompassed in BS25999.

The ISO PAS will now circulate for 3 years, unless an ISO committee (or a member nation) decides to either promote it to full standard (which will require committee discussion) or another country applies to promote their standard (in which case they would need to persuade other countries to support their standard over and above the PAS22399 or BS25999)

Question:

Are there any figures on the financial cost of downtime?

No we have no figures for this and do not see how anything meaningful can be provided.

When you talk downtime what are you talking about - loss of a server, a mainframe, a network hub, an entire data centre, telecoms, website etc.

Or are you talking about production (ie manufacturing) downtime, distribution logistics, supplier failure etc etc.

Costs would obvious depend upon a) the criticality of what is down and b) the amount of resilience you have dealing with it and c) the type of business/sector/size you are in.

Question:

Are there any discussions between the Insurance sector and BCM practitioners/BCI regarding the possible impact on the insurance premiums for the companies employing active BCM methodology?

We do not think there is anything formal.

Following a conversation with an insurance expert recently from the Institute of Insurers, he said that for large corporates the Risk Management algorithms used to calculate premiums do include a factor relating to having BCM in place. It improves a corporate risk profile and therefore has an indirect affect on premiums. However there is no obvious 1:1 relationship (it is just part of a large package)

He said there was no inclusion at all of BCM in the calculations used by insurers for SME's (Small & Medium Enterprises) and no short-term likelihood of that being changed.

To our knowledge there is no formal report on this. The conclusion is that reducing insurance premiums will never be guaranteed by BCM - but in fact the insurers might well insist on BCM being in place before they will insure some risky businesses at all.

Question :

Has the BCI issued any guidance on where individuals that make up part of an organisations crisis management team should keep their copies of the business continuity plan i.e. should BCPs be kept in the office, at home, in a car? What is considered best practice?

There is no specific guidance in the GPG on the location of the plans. However, given the nature of incidents, immediate accessibility is imperative at all times - so keeping them only in the office is clearly not appropriate. (One company in the City lost all copies of their plans in the Bishopsgate Bomb as they had called them all in for updating). However you do not need all the information straight away so a small 'emergency' checklist in a wallet may be sufficient for the first few hours, giving you time to access the full document which could be kept on the site, but also additional copies at other locations including home and the nominated alternate location for the team. Ease of maintenance and security of the information (which may be confidential) should also be considered - the latter may rule out certain locations - such as a car.

Question :

Could you please describe what BCI is and what it means to the BC professional?

The BCI is first and foremost a professional institute made up of individual members, all of whom are Business Continuity practitioners.

It also has a wider mission in that it looks to promote best practice in BCM throughout the world, through training, education, professional certification and partnership with industries, governments and standard bodies and regulators.

It helps the BC professional gain much better recognition for his/her skills, experience and contribution to their organisation's success.

Question :

What is BCI's relationship with other organisations, such as Disaster Recovery Institute International (DRII) and the British Standards Institute (BSI)?

We have a good friendly relationship with all organisations that share our aims for improving the awareness and quality of BCM globally.

This certainly includes our friends at the DRII, with whom we have co-operated for over a decade on defining what BCM is and what a practitioner needs to know.

The BSI is a different relationship. We have helped them build the new standard BS25999 and we encourage organisations to adopt it when appropriate. However, there are other standards in other countries, like NFPA 1600 or the ISO PAS 22399 and we are happy to work with them as and when the opportunity arises.

Question :

Do you believe that there should be international standardisation for the business continuity profession and why or why not? If so, what would it take to make this a reality?

Yes of course we do and we feel that it is one of our primary goals. However, standardisation does not necessarily mean uniformity – it means clear definitions, frameworks and principles that organisations and practitioners should comply with. We view this concept more as principle based rather than mandatory rule based.

I guess this is already happening to some extent. I am sure there will eventually be a generally accepted ISO BCM standard and once you have that the whole question of what makes BCM a profession and what a professional needs to know becomes much clearer.

At the BCI we believe our professional qualification which is held by 4000 people across 85 countries is the closest we have to that acceptance today.

Question :

Disaster Recovery, Business Continuity, Business Resiliency, Risk Management, Emergency Management, Crisis Management – these are all terms used throughout our industry. How do you describe the nuances between them and how do you see them working together?

Yes, this is a real problem for BCM acceptance in this proliferation of terminology. No wonder outsiders get confused!

To me, Business Continuity Management is about resilience and recovery so certainly your terms Disaster Recovery and Business Resiliency are part of BCM.

Emergency Management has typically been used to describe large-scale incidents (mainly affecting the general public) which public authorities have primary responsibility.

Crisis Management has usually been seen as an incident needing a specialised and immediate response, like dealing with a hostage situation, a major food recall program etc. This usually has a major external comms component.

In BCM we tend to call both emergency and crisis (incidents) and it is the realisation of an incident from any source that generally triggers BCM.

Risk Management is an over-arching subject covering a very wide range of issues – one form of risk treatment is BCM but there are many risks that fall outside of BCM's remit.

Question :

A question that is often asked of us is how to get executive management hooked into the idea of business continuity, without having to survive an actual crisis. In your experience and from your vantage point, what has been the most successful way to get executive management on board with BCM?

It is a challenging question with no single answer. Some points I like to stress are:

- Try and use carrots not sticks

- Don't let it get delegated to compliance
 - Positive ideas get people excited by BCM
 - Link BCM to winning more business by demonstrating competence, resilience and quality
 - BCM helps keep customers happy by always delivering on time
- BCM protects your brand from supply chain failures

Remember to always FOCUS on the commercial issues and show how BCM can help.

These are all BCM issues but often top management do not realise it! So TELL THEM!

Question :

Where do you see the business continuity industry headed over the next ten years? Will it change or we do just more of the same?

The question is more where will business go – because BCM is only a response to protecting your business.

More globalisation, more off-shoring, more outsourcing mean different challenges.

The traditional IT/DR might still be around but BCM is more likely to be about managing global supply chains, increasing resilience to interruptions thousands of miles from your customer base.

Bringing Enterprise Risk Management and BCM closer together will, I think, be a big challenge but a vital one.