How effective incident management retains market share

Courtenay Enright

Received (in revised form): 6th August, 2012

Symantec Corporation, 8001 Irvine Center Drive, Suite 400, Irvine, CA 92618, USA
Tel: +1 650 224 6597; Fax: +1 949 754 4099; E-mail: courtenay_enright@symantec.com

Courtenay Enright *has over 18 years' experience in business continuity and disaster recovery for Fortune 500 firms including Adobe, BellSouth Technologies, Federal Communications Commission, First Data Corporation, Nike, Qualcomm, Robert Half, Intl., Stanford University and Stanford Medical, Starbucks, Washington Mutual and Wells Fargo. She is currently Senior Director of Global Business Continuity Management for Symantec Corporation. Ms Enright has provided assurance oversight for regulatory compliance programmes addressing prevention, response, reporting, training and drills, including the National Preparedness for Response Exercise Program with federal, state and local government agencies, and has represented IT private/public sector cooperative interests within the National Infrastructure Advisory Council to the President of the United States, authoring portions of the Information Technology Sector Appendices and Annex Guidelines. Ms Enright holds a BA from Pepperdine University.*

ABSTRACT

This paper discusses the need for business continuity practitioners to make incident management a focal element of their programme. Particularly during the first few minutes and hours of a business disruption, an established incident management methodology is not only key to achieving a successful, coordinated recovery, but it can play an even more important role in maintaining customer confidence following a disruption or crisis.

Keywords: incident management, crisis, BCM response, ICS (Incident Command System)

INTRODUCTION

What makes a symphony orchestra perform in harmony despite the many different instruments involved and their different levels of contribution? They practise together frequently, using the same sheet of music, and look to one conductor to lead their group.

Using the same process approach for every incident, regardless of scenario, is the most effective approach, because that consistent training builds cognitive retention in an incident management team (IMT). Incident causation is irrelevant — handling the impact on the operation should be the focus of training efforts.

Perhaps the most vivid portrayal of the success of this approach is the widely seen photograph of the passengers of US Airways Flight 1549 standing in single file, in orderly lines on the wings of the Airbus 320 with the Hudson River washing over their shoes (Figure 1). The repetition of hearing the same, standard set of instructions every time passengers fly helps layer

Courtenay Enright

Journal of Business Continuity & Emergency Planning
Vol. 6 No. 1, pp. 13–24

1749–9216

Figure 1 US Airways Flight 1549 after landing on the Hudson River

Source: http://en.wikipedia.org/wiki/US_Airways_Flight_1549

that information, so everyone remembers and understands the expected sequence of actions they will engage in when an incident occurs.

Captain Sullenberger himself said in a news interview:

> 'One way of looking at this might be that for 42 years, I've been making small, regular deposits in this bank of experience: education and training. And on January 15 the balance was sufficient so that I could make a very large withdrawal.'[1]

Over the last decade, most organisations, even those not highly regulated, have reached a reasonable state of maturity with their business continuity plans, having recognised the need to continue operations to support clients and protect the company's financial health and reputation.

Perhaps even more important for maintaining market share is how an organisation handles (or is perceived to handle) a disruption or crisis. Research indicates that:

- customers are more loyal to a company that resolved a crisis quickly; and
- customer loyalty is prompted more by confidence in the brand than by price of the service or product.

Indeed, in *Leading on the Edge of Chaos*, Emmet and Mark Murphy argue that retaining existing customers can actually be more profitable than adding new customers.[2] They go on to suggest that:

- acquiring new customers can cost as much as five times more than satisfying and retaining current customers;
- a 2 per cent increase in customer retention has the same effect as decreasing costs by ten per cent;
- depending on the industry, reducing customer defection rate by 5 per cent can increase profitability by 25 to 125 per cent;

- customer profitability tends to increase over the life of a retained customer.

Business continuity practitioners can play a crucial role in maintaining this customer confidence and supporting their company's revenue stream.

Yet the incident management programme and mechanisms often do not get the same amount of up-front strategy design time as business continuity planning. Just when a company's credibility is at its most vulnerable, and customer confidence is at stake, is the moment for which most organisations are the least prepared.

This does not have to be the case. In a similar way to creating an agenda for a meeting, or a project plan for a department initiative, there are simple measures that can be incorporated into a business continuity planning process to bring order out of chaos.

There is an incident management methodology, statistically proven to be the most successful approach to mitigating crisis, known as the Incident Command System (ICS). Its success is largely due to the simple axiom that following a standard management process each time, regardless of the scenario faced, reduces potential confusion and need for spontaneous judgment calls during a crisis.

This paper reviews the primary components of that approach and how the same methodology was used to manage five very different types of incident: a monsoon flood, a terrorist bombing, an anthrax quarantine, an extortion attempt, and finally, Japan's recent unprecedented disaster of a tsunami, earthquake and radiation impacts.

In each case, following the principles of ICS helped a company successfully manage the incident and protect its brand and reputation — in some cases the firm even received positive press, increased market share, or increased revenue — by handling the crisis in a manner that maintained its customers' confidence.

INCORPORATING INCIDENT MANAGEMENT CAPABILITY WITH BUSINESS CONTINUITY

Recognition of the need to conduct more deliberate planning in this area becomes evident in the evolution of industry standards, beginning with the publication of British Standard BS25999 Code of Practice and Specifications. Whereas incident management had previously been a stand-alone topic area, independent of the traditional business continuity life cycle of business impact analysis/strategy design/plan documentation/test, more closely associated with emergency response than business continuity, and often managed by an entirely different department from business continuity, BS 25999 wove incident response directly into the life cycle as a normative element in *Clause 8: Developing and implementing a BCM response*.

A natural follow-on from *Clause 7: Determining business continuity strategy*, Clause 8 fills the execution gap that previously existed between having a business function sketch out its recovery strategy (in theory, on paper), then walk through a tabletop of restoring its functionality (again in theory, on paper), without accounting for expected individual and community reactions to stressors during those first few hours of an incident unfolding.

Because actual, physical exercises are viewed as intrusive to actual production, and very time-consuming to coordinate and manage across functions, many business continuity management practitioners find it difficult to get support for, or run, a full-scale exercise that would really test the organisation.

Even if a symphony has had far too little rehearsal time, these components are

designed to provide disciplined management of often unpredictable collective and organisational behaviour. This is what will make or break a successful cross-functional response and mitigate risks more quickly.

The primary ICS planning components focus on establishing:

- common terminology;
- manageable span-of-control;
- objectives-driven response;
- incident action plans;
- comprehensive resource management;
- incident chain-of-command;
- pre-designated communications channels.

FOCUS ON INTERACTION BETWEEN TEAM MEMBERS, NOT THE SCENARIO

Even when organisations exercise the incident management team, it is often with an outward focus on the details of an imaginative scenario versus an internal focus on the personal interaction of the team members.

This is always recognised and documented in company debrief (or post-mortem) discussions after an actual incident, but by then the knowledge is retro-active, and the urgency behind getting that newly-gained information incorporated into company documentation and training quickly fades as the business turns back to the demands of managing daily operations within their functional silos.

The first focus must be on the challenge of managing human behaviour.

In today's market, an organisational landscape can change constantly as new technologies and services are developed, mergers and acquisitions occur, or partner organisations change. This continually has an impact on the composition of a company's incident management team. As with Flight 1549, the combination of passengers, crew and pilots changes with every flight. Less than a handful of staff recognise each other — the frequent flyers. More often, there is a set of fresh new voices on each incident call who have never met each other before. Global organisations are so large and diverse that it is difficult for any one business function lead to know the full operational complexities of sister lines of business in other global regions.

MONSOON FLOOD IN A MAJOR CALL CENTRE

As an example, a new operation in India was experiencing rapid expansion — so much so that product development and support there was beginning to dwarf other global region operations, requiring an update to its existing recovery strategy. A high-level business impact analysis was conducted with the largest functions — technical support and engineering — and a next-level strategy sketched, but before it could even be submitted for local management review, a flash flood submerged the bottom floor of the main campus building.

The back-up network line held, and IT monitoring was alerted immediately to the primary line failure, as local staff were arriving to find their office in the middle of a lake.

The new business continuity solution was just being formed, was completely untested, and not yet relayed to the other global regions that would be needed to support the recovery.

This is a position many companies find themselves in, with a continuity solution in transition, functional teams that have not had an opportunity to test together, or that are not yet familiarised with the current recovery plan. This is where the incident management process becomes that crucial back-stop.

The one thing that the company was universally educated on was the corporate incident management procedure — one

forum where cross-functional teams would come together to devise their incident management strategy through a structured sequence of information sharing. With just that process being known, and nothing else, eight other global locations were alerted to join an incident management meeting with India. Staff in the Europe, Middle East and Africa region received calls as they were turning in for the evening; other staff in the Asia Pacific and Japan region were awoken in the middle of the night, with India staff having to call in on their cell phones while standing outside.

Conditions that can create challenges to communicating and decision making during normal operational meetings — people from different geographies, organisational disciplines, levels of management, or languages — can be compounded during an emergency meeting and create costly delays to moving to a contingency. These conditions can be mitigated by conducting the incident management team meeting in three distinct phases:

- assessment;
- problem solving;
- action plan.

In training, both business continuity recovery teams and incident management teams are given the same 'meeting ground rules' instruction that an incident commander (the symphony conductor) will facilitate for the assembled team through the same sequence of information exchange during every incident. This sequence is adapted from the ICS 201 Incident Briefing Form.[3]

The approach has multiple benefits, including:

- All participants know the order in which they will be called on to give an assessment, engage in questions and answers (Q&A), and be asked to come up with their function's next actions.
- In a virtual, global conference call, having a planned sequence of conversational exchange is the equivalent of being able to 'eyeball' your team and help them to think and respond rationally.
- By emphasising that no one is expected to come to this discussion with answers, but that working through the sequence of information exchange will help the team arrive at answers, keeps the team from feeling overwhelmed by large-scale incidents by allowing them to isolate each issue and work through it incrementally.
- Emphasising that this format creates a consensus determination for the company helps encourage ideas and proactive strategising, whereas emphasis on personal responsibility or liability tends to make contributors hesitant in taking a firm decision. This is still a matter managing psychology and group dynamics.

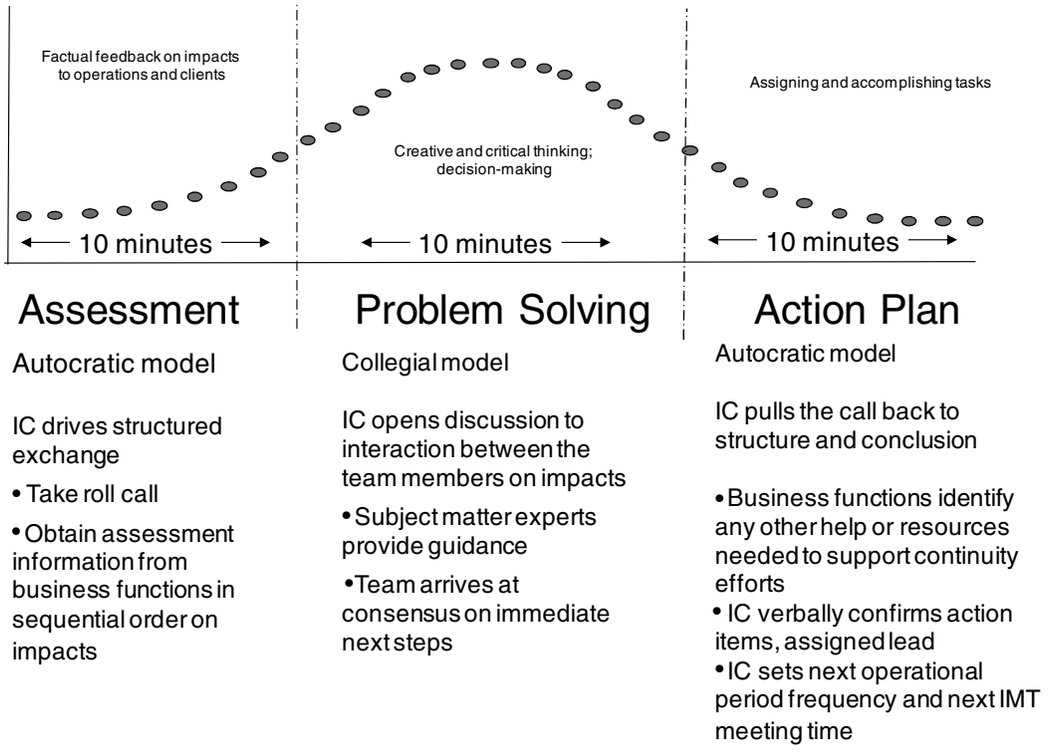
AUTOCRATIC–COLLEGIATE–AUTOCRATIC

The flow of the meeting can be pictured following a bell curve shape similar to that in Figure 2. The team should observe a designated sequence of information sharing for the assessment; and after that there can be a more free-form discussion for answering questions and problem solving. Then the group's focus needs to be tightened back to forming a specific action plan.

GUIDELINES FOR EFFECTIVE TIME MANAGEMENT AND DECISION MAKING

In addition to providing structure to the team's interaction, ICS provides a set of guidelines, philosophies and mechanisms

Figure 2 Phases of an incident management team meeting



designed to reduce potential delay or indecision.

This starts by targeting, to have the initial action plan to address an incident issued within a specified timeframe. This is driven in part by the business function's recovery time objectives (RTOs), but increasingly by the expectation of customers for immediate communications. A good target timeframe to issue an action plan is within two hours. This allows a team to move on immediate elements of the response to the incident or recovery of functionality within half an operational day.

Avoid costly delays by taking the time up-front to populate an automated communications tool with company contacts. Such a tool can be set to pull automatically from one's phone directory or other tools, or create customised groupings of contacts by geography, business unit vertical, or topic. In working sessions beforehand, the following should be identified:

- subject matter expertise required for topics (eg an information security threat investigation, an infectious disease scenario, a telecommunications or connectivity outage);
- business function representatives vertically and by geography;
- support teams that have oversight of company policies, guidelines, or processes: business function representatives, facilities, security, IT/network operations centre, HR, communications (internal and PR), and legal;
- an incident commander functioning as an objective meeting facilitator to guide the team through structured information sharing.

By assigning on-call resources in each

global region for each of these areas, at whatever time during a 24-hour period the incident occurs, a pre-populated communications tool can quickly alert the designees needed for the incident management team.

Creating a project plan for chaos

Ideally, the goal of the incident management team's discussion is to execute documented strategies, not begin brainstorming a solution from inception. The ICS principle of doing incident management the same way every time helps in getting to an execution plan much more quickly, even when a team comes together unprepared for the situation.

Other guidelines include:

- *Over-respond with team resources, then drop the ones not needed a few minutes later.* Adding to the team incrementally means information has to be repeated every time new people come into the conversation, and it keeps people in a reactive mode to the incident. Not getting all the right subject-matter experts in the conversation also results in a flawed recovery strategy.

TERRORIST BOMBING IN LONDON

On 7th July, 2005, a series of coordinated bombings in London targeted the public transport system during the morning rush hour.

A mere 48 hours prior to that event, a merger and acquisition deal had just been announced between two companies of roughly the same size, both with operations in the city. Just as financial analysts' speculative gaze had turned onto the newly-minted partnership, these just introduced, separate entities were forced to co-manage a very public crisis.

Two different corporate cultures with two yet-to-be integrated headquarters and sets of reporting chains can be a perfect recipe for conflicting directions, and a power struggle.

As part of the merger preparations, a large volume of new training and company information had just been thrown at staff in both entities. With limited space and attention span spared for business continuity materials, the one procedure that was drilled into staff was the expectation of joining that incident management forum, and following that pre-established sequence of information sharing to achieve consensus on an action plan.

This is why the methodology emphasises so strongly pre-established communication channels. Prior to the merger, each company had different contact information, with customised dialling instructions for each of their phone systems, which did not work at the other company. In the merger training, all employees were pointed to one contact point (accessed by an automated communication tool that was not dependent on either of their custom phone systems) for emergency notification and incident management.

With the immediacy of employee safety at stake, upwards of 60 headquarters and local management staff from each company's HR, physical safety, facilities and business functions piled simultaneously into one call. Everyone knows that the larger the attendance at a meeting, the more unwieldy the conversation can become — particularly virtual meetings, where there are no physical cues as to when to pass the 'conversational ball'.

This is where ICS addresses span of control — no matter how large the group on the call becomes, with the use of a specific sequence of information sharing, the meeting is kept disciplined, and a cross-functional team can be driven to a consensus action more quickly. As total strangers joined each other, blurting out their names

and titles, or asking startled questions, and with other simultaneous conversations in the background, the sequence was iterated — functions provide assessment information when called on in a specific order; the conversation will be opened up to discussion and Q&A, then the meeting wrapped up with an agreed action plan for immediate-term requirements.

Once it is communicated to staff that there is a roadmap to follow that will culminate in a group decision, this also lessens their initial anxiety about having to come up with the right answer under pressure in an unknown situation. When that level of expectation is set with people, they begin to think and speak more calmly, and manage to the structure.

The incident management mediator

Managing the meeting with discipline is also one of the reasons ICS establishes an incident chain-of-command meeting facilitator and moderator separate from the daily organisational hierarchy: that position functions as an objective third party, with the 'situational authority' to mediate multiple reporting lines. In this case, having a designated incident commander for the process avoided a time-consuming debate over which company or executive should be in charge. Having that mediator also meant that both firms' personnel welfare, recovery requirements and solution contributions were addressed equally and consistently.

If continuity solutions are to be timely and effective, it should be ensured all the brains needed are in the first incident management conversation.

Resources in the IMT have the authority to make a consensus decision for the company

In an urgent or crisis situation, the run-it-up-the-chain approach to obtaining hierarchical approval is reversed. Instead, if someone does not have the authority to make a go/no-go decision, that level of authority needed should be pulled into the IMT call. This brains trust has been established to have the pertinent information and to understand the cross-company impacts of the decisions that will need to be communicated to executive authority. If the decision is sent outside the IMT, critical time is wasted, and there is again the risk of a decision being made in a vacuum that does not address the bigger picture of impacts on an operation and its clients.

Communications during an incident

The other vacuum that can never be allowed to occur is a communications vacuum — whether with internal teams or with the external world

Radio silence or 'no comment' creates a communication vacuum where speculations and suspicion begin to grow. A statement as simple as, 'We are aware of the issue and a core team of engineers are examining the cause. Updates will be provided as available', can buy staff a few more hours to examine the situation fully and decide what they are really able to communicate to the external world.

An example of this is an operation that experienced a protracted anthrax quarantine. At the time, the operation consisted of close to 1,000 employees at a west US hub operation that bridged the workload and data shift for other global regions. The initial lockdown occurred right at the time most people were going to pick up their children from school. The IMT managed communication updates every 15 minutes — from reminders to employees to notify their emergency contact for child pick-up, to notices that vending machines were being opened to provide snacks, to describing the hazmat team's progress outside, and asking employees to respond with their status inside. Employees knew they

could count on a consistent frequency of communication from the company, even when it was not particularly new information, resulting in positive news coverage of the company's incident management by the local news crew stationed outside the building who captured the entire white-knuckle event live on television and in an article that noted:

> 'Employees … said they were so relaxed because they … got regular alerts from the company; those alerts are part of an extensive emergency response plan that includes annual drills.'[4]

That psychology and human behaviour that is being managed will be remembered. Consistent communication keeps people focused and calm, increasing their confidence that the incident is under command and control.

CREATING CUSTOMER CONFIDENCE THROUGH COMMUNICATION

Immediate, generalised holding statements keep the audience with the IMT

Holding statements also keep the IMT from being flooded by curiosity questions while it is trying to handle the incident. With complex and long-term incidents, investigations and remediation efforts may take several days and immediate answers to all of the questions from staff, the media, or the large social network will not be available.

Very general holding statements that the legal department has pre-approved should be on hand, ready to issue immediately. If an organisation establishes itself as an active part of the dialogue, the blogosphere will turn to it more instinctively as a source of information, allowing the company to influence positively the perception of how the crisis is being handled.

In today's internet age, the perception of a brand and reputation — and resulting market share — can be an even greater risk than the actual impact of the disruption to operations. *The Handbook of Crisis Communication* notes:

> 'the Internet has had a significant effect on corporate communication. The speed and ease of communicating via the Internet are changing expectations. Stakeholders have greater expectations of near immediate communication about events.'[5]

If a company is perceived to be unable to handle the crisis, the consequences and customer experience are sadly predictable.

With such heavy dependence on technology, almost no company can avoid a brush with cyber mischief.

In early 2012, the media reported how many companies had found themselves targets of:

> 'a month-long reign of terror, [including] hacking the CIA, Fox, Sony and several financial institutions, causing … billions of dollars in damage around the world'.[6]

Faced with an extortion attempt by individuals claiming to have access to old intellectual property, this last example is of a company that positioned itself to manage successfully a brand-affecting incident by following the ICS planning components.

While at first this can be assumed to be a purely a public relations scenario, managed just by a PR team, several business function responses are actually required to mitigate a brand impact.

Companies must divert a number of back-office resources away from daily operations to investigate and analyse

claims of potential theft and unauthorised access, while customer and partner-facing groups can find themselves overwhelmed by the dialogue, questions and concerns from their own colleagues, customers, and the external world.

These same resources must also carve out time to create a forward strategy to move from a reactive to a proactive mode in managing the incident. The resource drain can have a debilitating impact on business initiatives if a structured incident management approach is lacking.

Following the ICS approach of creating and communicating an incident action plan to guide teams' individual and collective tasks for each operational period, the CEO issued a daily status report outlining the company's preventive and protective measures being taken, and provided guidance on customer and partner messaging, to ensure internal teams' alignment on direction.

By issuing communications from the same source and same time each day, and promising updates on significant developments, executive management created a transparent, single source of information, which helped minimise misinformation in social media posts, and encouraged staff to be mindful of the need to communicate with customers in a clear, effective manner.

The firm also conducted direct outreach to customers to remind them of both general security best practices that should be universally observed, and specific remediation measures it recommended customers take as a precaution.

As a result, some of the often obscure components of the information technology environment not usually part of the business-side vocabulary were suddenly a hot topic. Potential for damage to reputation became a two-fold opportunity for suppliers when dialogue around the incident opened new channels of communication with a wider array of decision makers for their clients.

The firm was able to raise more awareness of how those product functionalities and features strengthened the IT environment, and how its subject matter expertise could be leveraged to reduce other operational risk, becoming viewed as more of a trusted adviser than a transactional vendor.

In the following months, law enforcement tracked and apprehended a primary source of that series of cyber attacks, and at the end of April, a Gartner report highlighted those companies in the security market that retained market share lead in the face of advanced persistent threats.[7]

What turned out to be a failed extortion attempt became a public relations win for the target company, because it got out ahead of the incident by addressing the possible consequence instead of counting on the probability that it would not affect clients. By having the mechanisms to take advantage of that window of increased awareness to get messaging out about how its products and solutions were beneficial, the firm actually strengthened its customer relationships and market-share lead.

Be proactive with actions and communications

Whenever in doubt, contingency measures should be implemented sooner rather than later. One of the most common tendencies is for people to wait too long to initiate business continuity. People will always want to wait one more hour for the power to come back on, or for IT to find which server is not cooperating; for a parts repair person to arrive, or to see if the majority of area schools are *really* closing before directing staff to work from home the next day. This is because contingencies are more manual and less convenient, but delaying addressing that contingency always increases the risk and the complexities of the incident.

After some of the worst hurricane seasons for the eastern and gulf coast USA, including Charley, Ivan, Katrina and Wilma, it was seen that waiting means evacuation routes are already taken; staff can get stuck in even worse traffic or travel conditions; or that by waiting for the state of emergency to be officially declared, much of the team's lead time to set up an alternative work environment has been taken away, forcing the team members to make those phone calls and take those steps in the middle of the night.

Consequence versus probability

Finally, the most important driving philosophy should be planning for consequence versus probability. Who could have anticipated the series of devastating events Japan would face on 11th March, 2011? A powerful earthquake, and a tsunami resulting in power impacts and radiation concerns, challenged their nation and all companies doing business there.

While a number of companies closed doors immediately (including one that made the only type of digital tape used by the entire motion-picture industry, creating a single point of failure in that distribution system), while some sent employees to other global regions wholesale, there is an example of one operation that was able to persevere and ultimately expand its presence in the region.[8]

Instead of feeling cut off and powerless to help their island operation on the other side of the globe, where many Japanese staff did not speak the same languages as their corporate headquarters counterparts, the ability of the two entities to align efforts by following ICS planning components allowed them to craft a remarkably successful recovery strategy via a multi-pronged, objectives-driven response.

Beyond the *de facto* recognition of steps needed to support employee health, observe radiation hygiene precautions, and try to augment food and drink supplies that were flying off the shelves of local stores through corporate channels, was an understanding that something broader must be done longer term to support the community and area businesses, to help them weather successive waves of impact.

In addition to donations to area relief organisations, an outreach to the three affected prefectures included donated computers, with free software and technical support associated with their key brands through the following year.

To manage the travel restrictions and rolling brownouts for power conservation, the different business units agreed to a rotating schedule of office usage to support engineering, technical support, and product marketing work cycle at peak times, and capitalised on the schedule of power availability at different offices when each team had to transmit larger files or batches of code.

The country president for that operation then publicised the benefits of this progressive energy conservation model they had developed via the Nikkei newspaper and other media outlet interviews as a way of meeting the Japanese government request for a 15 per cent reduction of electricity consumption — demonstrating thought leadership and increasing customer confidence.

Going into the summer, the firm then also announced a weekend support offering for basic support customers, to help the weekend operation schedule that Japanese manufacturing and other industries had to observe to meet the government's reduced electricity consumption goals.

All these actions culminated in an uptick of customer loyalty and increased market share in an area experiencing a dramatic impact to its GDP. Today, that operation has expanded its footprint in the region as a result.

CONCLUSION

One never loses customers by taking informed precautions. Customers are lost when disruptions to business, particularly those that are public and visible to customers, are not able to be managed.

Focus on incident management methodology is just as crucial to a firm's recovery capability as business continuity planning.

By incorporating planning principles similar to those outlined in ICS, an organisation can be moved from being in a reactive mode and trying to 'catch up' with the incident, to being in a proactive mode, and mitigating the impacts on the organisation more quickly. The following guidelines are fundamental aspects of business continuity:

- Align the company to one sheet of music.
- Practise methodology the same way every time.
- Create quick 'project plans' to manage the immediate term needs.
- Communicate proactively, even if the message is general.

With the immediacy with which information now travels to employees, partners, customers and the external world, incident management also becomes a tool for maintaining market share.

As John F. Kennedy once noted, 'Along with danger, crisis is represented by opportunity.'[9]

REFERENCES

(1) CBS News (2009) 'Capt. Sully worried about airline industry', available at: http://www.cbsnews.com/2100-18563_162-4791429.html (accessed 15th August, 2012).

(2) Murphy, E. C. and Murphy, M. A. (2002) 'Leading on the Edge of Chaos: The 10 Critical Elements for Success in Volatile Times', Prentice Hall, Upper Saddle River, NJ.

(3) FEMA, 'ICS201 Incident briefing form', available at: http://training.fema.gov/EMIWeb/IS/ICSResource/assets/ICSFormsUse.pdf.

(4) Rillos, R. (2008) 'Symantec employees comfortable during scare', available at: http://www.kval.com/news/19152804.html (accessed 8th August, 2012).

(5) Coombs, W. T. and Holladay, S. J. (eds.) (2010) 'The Handbook of Crisis Communication', available at: http://www.blackwellreference.com/public/book?id=g9781405194419_9781405194419 (accessed 8th August, 2012).

(6) Winter, J. (2012) 'EXCLUSIVE: Unmasking the world's most wanted hacker', available at: http://www.foxnews.com/tech/2012/03/06/exclusive-unmasking-worlds-most-wanted-hacker/#ixzz21wrlY49o (accessed 8th August, 2012).

(7) Gartner (2012) 'Gartner says security software market grew 7.5 Percent in 2011), available at: www.gartner.com/it/page.jsp?id=1996415 (accessed 8th August, 2012).

(8) Zacks Equity Research (2012) 'Symantec Beats Estimate in 1Q', *Nasdaq*, 26th July, available at: http://community.nasdaq.com/News/2012-07/symantec-beats-estimate-in-1q-analyst-blog.aspx?storyid=159022#ixzz235ezAk9Y (accessed 20th August, 2012).

(9) Remarks (draft 2) given at the Convocation of the United Negro College Fund, Indianapolis, Indiana, 12th April, 1959, p. 5, available at: http://www.jfklibrary.org/Asset-Viewer/To6xnVCeNUSecmWECy7Fpw.aspx (accessed 20th August, 2012).