Transitioning from incident to crisis management to continuity of operations

Received (in revised form): 29th July, 2019

Robert S. Cook*

Independent international consultant, CDEX International

Raelene Anderson**

Manager of enterprise business resilience, Delta Dental

Robert S. Cook

Raelene Anderson

***4411 SW 9th Avenue, Cape Coral, FL 33914, USA. Tel: +1 408 515 4905; E-mail: emconsult911@gmail.com*

****BSI Consulting Group, 5546 Cannes Way, Fair Oaks, CA 95628, USA. Tel: +1 408 515 4905; E-mail: emconsult911@gmail.com*

Journal of Business Continuity & Emergency Planning Vol. 14, No. 1, pp. 46–54

Robert S. Cook *is an independent international consultant with CDEX International and the former Head of Global Emergency Response for a Fortune 500 corporation. Mr Cook is a Certified Business Continuity Planner (CBCP) through Disaster Recovery Institute International and a Certified Emergency Manager (CEM) with the International Association of Emergency Managers. He is also a Homeland Security Exercise and Evaluation Professional (HSSEP) and Incident Command System instructor. He holds two bachelor's degrees from the State University of New York and a master's degree from American Military University. His work has been published in various international publications and he has spoken at multiple national conferences on emergency management, business continuity, crisis management and incident management.*

Raelene Anderson *is the manager of enterprise business resilience for Delta Dental. She has extensive experience in both the public and private sector, having been the Global Director for Applied Materials' Emergency Response and Business Continuity Programs, the Manager of Solectron's Global BCP Program and the Emergency Manager for the City of Sunnyvale California. Ms Anderson is a Master Business Continuity Professional (MBCP) through Disaster Recovery International and a Certified Emergency Manager (CEM) with the International Association of Emergency Managers. Ms Anderson has spoken at multiple national conferences on business continuity and crisis management.*

Abstract

This paper explores the phases of emergency management following an incident through to continuity of operations. It summarises many of the obvious but often missed problems while responding to and recovering from an incident. The authors discuss what they feel is the key step in managing any incident or crisis — setting up the response quickly and correctly from the very beginning. They give insight about how to bring the right people into the room, how to communicate effectively throughout the incident and, most importantly, when to pull in the business continuity personnel so they can begin assessing the situation to ensure a smooth transition between phases and teams.

Keywords: emergency response, crisis management, continuity of operations, all-hazards

INTRODUCTION

When people think about emergencies, they generally think about a municipality dealing with a natural, technological or human-caused disaster. However, corporations also have larger-scale emergencies. This is where emergency management comes in. For

both small business proprietors and multi-billion-dollar, multinational corporations, the rules are the same. Organisations that do not prepare for business disruptions are destined to fail. According to one study, 43 per cent of US companies never reopen after a disaster, while a further 29 per cent close within three years.[1] Additionally, 93 per cent of companies that suffer a significant data loss go out of business within five years. Further, 20 per cent of small to medium-sized businesses suffer some major disaster every five years. Most strikingly, 78 per cent of organisations that lack contingency plans and suffer catastrophic loss collapse within two years. In short, it is not enough simply to call the local emergency number.

An emergency can befall a company at any time. Usually, of course, it happens at the worst time. It is essential to know the critical periods for one's company's and prepare accordingly. As an example, if the 'end of year' or 'end of quarter' is critical due to government or stockholder reporting, it is vital to ensure that the company's response readiness is at its highest. This does not mean the company can take it easy during other non-critical periods; rather, it means that this must be a period of hyper-vigilance. So how does this happen? Simple: through planning.

An emergency is defined as an unplanned event. Naturally, there are many levels to this. However, it is essential to plan at the highest levels for the so-called 'worst case'. While the definition of what constitutes the 'big one' will vary from one company to the next, what unites businesses both large and small is that for all of them, there is an event that keeps them up at night. From a risk point of view, it is important to look at the probable versus the possible, and then prioritise preparedness and response. Certain incidents will always be at the top of the list — for example, a supply chain interruption is always a huge problem, while cyber attacks are a perennial fear. Regional natural disasters are also a concern, but so are obscure events that can take out teams or even leadership.

EMERGENCY RESPONSE

While it is not possible to plan for every eventuality, the preferred method is to respond from an 'all-hazards' approach. In the USA, the emergency operations centre in most hospitals will be lined with endless rows of binders containing volumes of action plans for anything and everything. The problem is, no one — except for their respective authors — has ever read them, and neither will they ever read them. Who, after all, has time to read a novel on 'game' day?

To make it easier, the thought of responding to everything from an all-hazards approach was developed. In an all-hazards approach, an organised structure is used to respond to any and all events.

Getting the right people in the room as soon as possible and creating an organised structure, are critical steps to managing an incident. The right people are the go-to people and subject matter experts. Next, get the wrong people out of the room. These are the people that do not make valuable contributions, but try to manage the incident in a silo, or just take up space. In the USA and many other countries, emergencies on the municipal level are handled using the Incident Command System (ICS). ICS is a flexible command structure that allows for defined roles when acting during an emergency. Many companies have also adopted this model to help manage emergencies.

The right people are assigned to several groups in ICS. The first group is the command group. This is the leader or incident commander, who will direct the team from the beginning to the end.

The second group comprises the subject-matter experts for the situation at hand. These people can range from the company's legal team, to human resources, to facilities, to environmentalists, to IT security and so on. The third group comprises the support people. They will either support the team by completing a task, or they will get the resources needed to mitigate the issue both efficiently and effectively. Exactly who these people will be will depend on the situation.

When using an all-hazards approach and ICS, the incident commander must be the best person to handle the job, not necessarily the one with highest title. Business continuity planners ensure that leaders have a significant number of people with equal knowledge to back them up, should they not be available. This is not the days of old where people spent most of their career with the same company. Today, people change jobs like they change their favourite dining spot. For this reason, continuous training for lines of succession is imperative. Sadly, it is also rare, and most companies seem to expect that someone new can simply jump into the role. These expectations are dangerously unrealistic and, in some cases, can be fatal to the operation.

Imagine, for example, that a facilities-related incident is in progress. In addition to having a strong incident commander to manage the incident, it is vital to have an experienced facilities team in the room. They must know what widget connects to which pipe that will affect which switch and how it connects to the relevant doohickey. An incident commander might have general knowledge; regarding the specifics, however, they are likely to come up short. The best facilities person must therefore be on site to guide the response team through the maze of facility operations. For a cyber event, simply replace the facilities person with an IT person. The structure, however, remains the same. If the issue is affecting multiple areas, then it will require even more subject matter experts to guide the response team through.

The incident commander must prioritise and coordinate these efforts. The focus of the crisis management and business continuity planning (BCP) teams is one of duration and overall effect. This means considering how bad the incident is and how long it will affect operations. While this has a different definition by sector or by company, a definition must nonetheless be established. This is not something randomly chosen. As they say, 'time is money', and for crisis management and BCP, this is no different. When a company is not operating, there is no let-up on the overheads; there will be rent to pay, as well as bills for utilities, machines and systems — that clock never stops. There will likely also be personnel costs, to include salaries, commissions, benefits and other expenses. Then there are IT systems to pay for, to include software applications and a host of other expenses. These are just some of the costs. Now think about what costs are running while the business is stopped or interrupted. While many businesses can compute the daily costs of operations, most companies likely do not have an accurate or even up-to-date number. Compare this figure with the cost of a BCP programme and the likely conclusion is that *not* having a robust BCP programme is costlier than having one. Take a moment to think about that. BCP programmes are much like insurance — something one pays for year after year, hoping it will never be needed. When it *is* needed, however — and every business will need it at some point — it is a massive relief to have it in place.

There are regional differences in the concept of emergency response. In some cases, like Asia or Europe, whoever has the highest title is likely to be in charge. Out

of respect, everyone follows the leader. The question is: what if the leader is not trained to handle emergencies? This is not just a problem for those who need to be led, but a potential curse for the leader too. One example that illustrates this point is when an incident commander was working a chemical leak at a plant in Taiwan some years ago. The site leader came in and demanded everyone who was in the building be sent to the hospital because he feared everyone had been exposed. What he did not understand was that the incident commander — a lower level, but highly trained incident commander — had eliminated that possibility. However, due to the corporate culture, 21 people went to the hospital and were subjected to needless tests.

Just as people expect their leader to lead, so that leader knows he is expected to get his people through the crisis, regardless of his own feelings. In the USA, things are a bit different. ICS is a more flexible system as it requires putting the best people in positions where they can do the best job. This means the big boss might not be the incident commander, but might instead be standing behind, making things happen so that the incident commander can be successful. That big boss is not telling the incident commander what to do or watching over the incident commander as a parent might their child; rather, they are there to provide support. The incident commander still makes the decisions. On the other side, if the incident commander needs guidance or some type of resource, the big boss is right there to assist.

A key advantage of the ICS system is that it provides enough flexibility to allow people to think individually when something does not go according to plan. By contrast, a more rigid structure can prevent individuals from taking immediate action. At the same time, however, freelancing cannot be allowed. If responders are left to do as they want, the incident commander loses control. Whether flexible or rigid, the incident commander must be the most knowledgeable and the best at leading. Almost everyone with the ability to be an incident commander has a proven record of incident management and has built a reputation of respect.

THE DONENESS CRITERIA

One of the most important lessons in emergency response is understanding the so-called 'doneness' criteria. How do we know when any phase of the response is done? This is no arbitrary question — indeed, it requires considerable thought. The answer is important because it guides when to transition from one phase to the next. In its simplest form, there are three basic phases: the incident phase, the crisis management phase and the business continuity or recovery phase. The big question is when to move from one phase to another. Depending on the type and impact of the incident, these lines can become even more difficult to define, making it even harder to know when to transition. This can take some real thought and some real leadership.

The incident phase is easily visible: something happens that requires attention. It can be something small or something that will affect the entire company's operation. This phase requires personnel resources who are normally tasked with some other job to stop what they are doing and focus on the emergency. While this is a simple definition, the action of response is not. The reason for this is simple. Most companies do not actually prepare for an emergency. This is specific to training for actual response. An example is a natural disaster, such as an earthquake. While facilities teams are well versed in keeping a facility up and running during normal operations, they may well have no

idea what to expect or how to respond to massive destruction, as in most cases they are not trained for such events. While business continuity teams write plans on how they might respond, many companies do not actually provide training, and certainly do not practise response activities. This failure can have long-reaching effects. At the same time, however, there is an expectation that during extraordinary events, ordinary people will be able to do extraordinary things and somehow deliver smooth results.

In a recent training, we discussed a natural disaster requiring the complete evacuation of several thousand employees from the site. The discussion covered everything, from getting people into their cars, to sheltering people who had no way home, to notifications, to letting employees know about their pay and when to come back to work. While discussing this, the human resources person's face began to drop. The horror in her eyes was plain. She looked up and said, 'We are not prepared for this'. Of course not — this is an extraordinary event. Most companies simply pray and hope that nothing will happen. This might constitute a plan of sorts, but a good plan it is not.

How does one know when the emergency phase is complete? If one takes this down to the simplest example of a water leak, the emergency phase is over when the water stops flowing. The impact of the leak is still evident; however, the water has stopped and the emergency team is done. Doneness is not always so clear-cut. In a cyber incident, for example, it might take days or even weeks to know when the intrusion is completely under control. In this case, doneness might be an evolving notion, but still must be determined. Likewise, identifying doneness when dealing with concurrent incidents can be complicated, but it nevertheless remains essential.

The incident commander (and possibly senior management) should clearly define when the emergency phase is complete. This must be clearly articulated to all everyone participating in the emergency. There must be alignment with all groups involved. As with all things corporate, for things to work properly, the important thing is not necessarily for people to agree with the decision, but rather for everyone to be on the 'same page'. In many cases, responsibility cannot be turned over to the next group until the emergency phase is complete. In short, the exact point of doneness is essential to know.

The doneness criteria determine when to transition from emergency to crisis and from crisis to BCP. What this should not imply, however, is a hard stop between one phase and the next. While some governmental agencies will not begin the next phase until the previous one is completed, the handover should be blended. In other words, at some point during the emergency phase, the crisis management team should be brought in to gain full understanding of what is happening. The same can be said of the BCP team. In order to understand the full extent of the incident, all teams need to see it in a tangible way — simply put, explaining the situation is no substitute for demonstrating its full impact. In this way, they can fully appreciate the impact of what is before them. This will help them develop plans on how they will handle their phase.

THE CRISIS MANAGEMENT TEAM

Before cleanup and repairs can begin, the company must work toward understanding the short-term impact on the company, that is, what is going to happen over the next 48 hours. This is where the crisis management team (CMT) comes in. In many respects, this is the worst time: this is when the immediate needs and required

responses come to light. If not handled properly, this will 'end' most companies. The reason for this (beyond them being ill-prepared to handle the situation), is that they fail to understand the gravity of the incident, the complexities of the incident and the immediate effect.

The key factor, so frequently overlooked, is how to communicate with the company's people. Thirty years ago, companies were actually in better shape in this regard, for the simple reason that there were landlines and telephone booths everywhere. In almost all cases, they worked, no matter what. Even those little pagers worked because they too relied on the landline system.

Today's communication technology relies on the internet, Wi-Fi, satellite Wi-Fi and so forth — everything is digital, and none of it is designed for disaster, especially a natural disaster. So, if there is an electrical outage, or cell towers go down or get overloaded, what happens next? The result is the same the world over: there is almost zero communication.

Like all great military operations, those with superior communications win every time. Battling an emergency is no different. Poor communications on any level will result in huge problems. For example, a system might come back online and start affecting some other system that has not recovered, but that information cannot be passed on. If someone flips a switch and incident commander does not know, this too can have negative effects. Without proper and reliable communication, the proverbial left hand cannot know what the right hand is doing.

Media communications falls under the same umbrella. How many times has a major corporation handled a personal information hack poorly and public perception (not to mention stock value) plummeted? This falls under the CMT's remit, and if they are not prepared for *any* crisis, then this is a huge problem. To reiterate for the millionth time, it is impossible to prepare for *all* incidents; however, handling crisis management from an all-hazards approach works. There is no time to deal with this on 'game' day; it is essential to prepare in advance.

With respect to media communications, a common problem is having the wrong person speak for the company. Much like choosing an incident commander with appropriate crisis management experience, the CMT must also pick a person who has the ability to speak in front of a group. Too many times, really smart people perform poorly when in front of camera or large group. This is not only painful to watch but can be troublesome for their company. Public perception of the company's ability to handle a crisis may well lie in the hands of this person. Like most skills, dealing with crisis is a learned skill. To think that a chief executive or a public official is automatically versed in crisis because of their title is a huge mistake.

During a crisis, all participants must have a grasp of their roles. Much like with emergency response, someone must be in charge of crisis management. This person should be predetermined, and ideally not the same person as the incident commander in the emergency phase. For this part, the leader of the CMT should be someone senior with broad powers to coordinate the actual crisis. Much like the incident commander, the leader of the CMT must have significant training and work well under severe pressure. This pressure will likely come from all ends. It will not only come from the senior management, but also from those who are looking for guidance, if not instruction, during those initial 24 hours.

These stresses include, but are not limited to: how to move people; how to communicate with sites outside the disaster area; how to speak to customers;

and how to keep everyone calm. While this provides some things to contemplate, ideally sooner than later, it is again vital to understand when this phase is complete. What are the 'doneness' criteria? This is critical in order to pass the baton to BCP to get the company back up and running. While this can be done simultaneous to CMT, it is important to ensure there is no overlap in the work being done, and perhaps more importantly, no one is working to conflicting agendas.

As in the emergency phase, the key question is who decides when the CMT job is done? This phase requires strong leadership as each group will look at things from a different perspective. Human resources will look at it when everyone is home and they are able to communicate with the employees. Corporate communications will think in terms of when the stock stops tumbling. Facilities will think it is done when the water stops. Being part of the CMT means no longer representing a single group — it means representing an entire company. It is therefore important for everyone to agree when the crisis phase is over. If the setup of the CMT is regionalised, the chief executive will want an answer. If there is an 'executive' CMT, as is usually the case during a large disaster, the board of directors will surely want an answer. In either case, specific doneness criteria should be expected.

A critical point is ensuring everyone is on the same proverbial page. Too often, sectored management teams fail to act in concert. This might be for a host of reasons, but the main two are generally, a failure of leadership to maintain control of the objectives, and secondly, when someone believes their area or group is more important than another. However, in a crisis, individuality does not matter. The only thing that matters is to get all of the objectives completed so the company can operate. It is critical to remember that all groups, regardless of importance are interrelated and therefore interdependent. Only once this is understood is it possible for everyone to work together to repair what was broken.

THE BCP TEAM

Finally, it is time to get the company back and running in whole or in part. This is the part where it might be necessary to keep the company running while clean-up and repairs are completed. This is the part where the finance team is assessing what the company has lost and how much it will cost to get the company to pre-incident conditions. Some might even use this opportunity, and possibly insurance money, to make improvements. In either case, this takes time, careful calculation, and a tremendous amount of leadership. In the recovery phase, two things will be happening simultaneously. The first is keeping the business running; the second is making it whole again. The first of these is relatively easy. Everyone works with what they have, and the business continues. This is of course unless the facility has no redundancies or is completely wiped out. Otherwise, people can work from another site or their homes, purchase goods from competitors to hold them over, or simply understand the mechanics needed to start full production. Much of this depends on what the business continuity plan says should happen in a worst-case scenario. If there is no plan, most likely the business is dead. As mentioned previously, 43 per cent of US companies never reopen after a disaster and 29 per cent more close within three years.

The second part is so complex it requires an incredible amount of leadership. The reason for this is that every single department head will be screaming that their group is the most important and that resources should go to them as

a priority. This is where the chief executive comes in. The chief executive will make the decisions on prioritising what gets resources first. It could be a machine that makes the products, or it could be a roof, so the machines will work. Each situation is different because each disaster is different. The chief executive and chief financial officer will decide priorities. The BCP team is expected to coordinate and execute. This is why BCP professionals should write plans from an all-hazards approach. If properly trained and executed, the procedure becomes the focus, not the disaster, because while every disaster is different, with different effects, the response is the same.

What is amazing is how often the BCP team will get beaten up every single day until completion. Not only is BCP the 'fix' team, but also the complaint department as well. If recovery falls a week behind due to scheduling or some other delay, the chief executive and the people who need that part of the 'fix' done will be lining up to yell. Here is the good news: seasoned BCP persons will know this is coming. While this knowledge does not make the day any easier, it does at least provide insight into what is coming. The best thing to do is to be realistic and prepare for bumps. BCP managers who aim too high had better dust off their resumés because they will not survive. However, those who are realistic and make the people counting on them understand the potential 'bumps' will likely get a promotion when the dust settles.

Like with all teams described above, there are some rules. Rule number one: you did not create the problem, but you are there to solve it. The second rule is: understand what you are dealing with and meet that problem head on. There is no dressing it up and hoping it will get better on its own. It must be dealt with. The final rule for now (as there are surely many others), is: find your courage. In all phases it takes more than skill and finesse — it takes courage. It takes courage to meet the problem head on as stated, but it takes even more courage to tell people things they do not want to hear at the worst moment of their lives and career. You will tell them 'no', and if there is one thing everyone hates to hear — even at the best of times — it is 'no'. When that person is the boss, it can be even scarier. BCP has to deal with unrealistic deadlines that cannot be controlled. Most likely, they are just reporting the facts while some other group is grappling with the issue. It might be a facility opening later than anticipated, costing the company more 'burn' rate, or a part for the money-making tool on back order for an unknown length of time. Either way, BCP will bear the brunt of discontent. BCP deals with interruption. The common mistake is failing to prepare for interruptions to those interruptions. Remember Mr Murphy: if it can go wrong, it will, and at the worst possible time.

How does one know when the BCP team is done? Again, this is not when everyone is back to normal. The word 'normal' oversimplifies things and a corporate disruption is anything but that. If there is a list of objectives, one could conclude that when the list is exhausted, the work is done. However, when entire factories get destroyed and take years to rebuild, is the BCP team still in play or does responsibility get transferred to project management? This requires a clear answer. This is why the 'doneness' criteria are so important.

MESSAGING

Messaging is important — really important. It is vital that *all* teams are fully briefed on the 'message'. It is unacceptable to have the incident commander saying

one thing, people in the field saying something they 'think' they heard, and the CMT people telling customers there was a small leak while the BCP team is telling them they cannot get their product because the factory was washed away. When the sales people are saying all is well when patently it is not, it does not instil confidence in the company. There must be one message and only one message. Failure to stick to a single truth will result in any number of inaccurate stories appearing on social media. This can be a disaster for the company and fatal for reputation and stock value.

In this age of transparency, companies must balance what they say and when. If one looks to the public sector, one sees examples of governmental agencies saying things designed to keep the public calm rather than be open about the extent of the incident. The same thing happens in the private sector. How many times following a cyber attack do companies report a relatively low number? Then, days later, that number grows and grows. They seem to be spoon-feeding everyone what the company feels they can take without a panic. The problem is, some companies never recover from this type of behaviour.

The point is, honesty in the face of adversity requires not only transparency, but courage as well. When companies peddle a lie, it will *always* come back and bite them. Whether dealing with customers, employees, vendors, the media or anyone else, it is essential to provide full facts or they will fill in the blanks — and that can destroy a company's reputation. Throughout all phases, the message must only change if there is new information. Furthermore, the message should be consistent and managed and delivered by a single person.

TRANSITIONING BACK

Transitioning is an important part of the closeout of the disaster. Always, the important thing is to learn, whether that be from personal experience or someone else's experience. Experience is an excellent teacher, but it can be costly in both time and money. For this reason, it is much better is to gain understanding from those who have lived through previous incidents and have insights to share. There is a big difference between thinking you are ready and actually being ready.

The other learning point is not to let your guard down. If a disaster befell your company, especially a natural disaster, and you lived through it but did not harden your assets, you must be prepared to walk this road again. This happens surprisingly often: people build a house, the disaster hits, they rebuild, and get wiped out again. This is why it is important to do better than recover to pre-incident conditions — and improving on last time requires planning.

Reference

(1) Hanwacker, L. (2015) 'Businesses need to plan for worst', *Southwest Florida Business Today*, November, p. 8.