Emergency Response & Business Continuity

The Next Generation in Planning

By Scott R. Nicoll and Russell W. Owens

IN BRIEF

- **Tasked with developing response/recovery plans for small-to-midsize businesses, safety professionals must have the knowledge to develop complex and interconnected plans.**
- **SH&E professionals must understand the requirements for the next generation expectations, their effect on business, and how to develop, implement and maintain these new plans.**
- **Today's emergency response and business continuity plans must include procedures necessary to recover critical functions to help get the business back up and running should a future loss occur.**

A safety professional working for a small-to-midsize business (SMB) is often asked to develop emergency response and business continuity (E&BC) plans to protect staff and facilities. These plans predict likely hazardous events and describe how the SMB can protect itself and its employees from any immediate threat.

To be most effective, the next generation of E&BC plans should go beyond simple evacuation plans. These plans should be specific, tailored to the SMB's operations and encompass all facets of the business. Safety professionals charged with this task must be aware of the true responsibility involved. They need to think long term—not just about protecting current operations. Today's E&BC plans should include procedures necessary to recover critical functions to help get the business back up and running should a future loss occur.

Financial Impact/Return on Investment

No matter the business size, response to a disaster and the subsequent effect on business continuity can be daunting. The extent of the effects will vary depending on the characteristics of the disaster, time of year, specific areas of the company affected and duration. In the authors' experience, SMB companies experience a greater proportional effect on their bottom line than larger companies. Therefore, an SMB's failure to prepare for a disaster is the business equivalent of playing Texas Hold'Em—an all-in decision with the future of the SMB riding on the outcome.

Studies have shown that publicly traded companies without a plan or with an inadequate plan reduce their market viability. When market share is lost due to a catastrophic event, it can profoundly affect an SMB's ability to stay in business. Some SMBs may initially recover from the disaster, but reports suggest that "one in four small businesses that close due to a disaster will never reopen. Anecdotally, the statistics are probably higher" (Insurance Institute for Business & Home Safety, 2012).

The days of a simple evacuation plan are over, and safety professionals must consider a disaster's overall effect on the company's long-term health. In a crisis, you do what you have to do, but it is better to do what you planned to do. Put another way, "Planning is vital, but plans are the source of actions" (Kelly, 1989). This is especially true if the company is going to survive the catastrophic event.

In the past, executives have seen the development of E&BC plans as a "document production factory producing reams of paper in three-ring binders" (Mah, 2012) that fill bookshelves and devour budgets with no return on investment (ROI). This view is changing. More and more SMB executives are asking these questions:

- Do these plans make us money?
- Do they save us money?
- Do they benefit our customers?
- Is this only to satisfy a regulatory requirement?

The answers to these questions must show how such plans will positively affect a company's bottom line. To make these plans successful, one must develop strategies and activities that help answer these questions.

How this is achieved varies from business to business and industry to industry. One method asks the safety professional to become involved

Scott R. Nicoll, ABCP, CPP, CFPS, is a senior business continuity specialist and assistant vice president, Chubb Group of Insurance Cos. Nicoll has been with Chubb for 34 years in various loss control roles within its eastern territory, providing disaster recovery and business continuity planning services to clients. He is a principal member of two NFPA committees (1600 and 1620). Nicoll is a professional member of ASSE's New Jersey Chapter.

Russell W. Owens, CSP, ABCP, is senior business continuity specialist, Chubb Group of Insurance Cos., and assistant vice president, Chubb & Son Inc. He provides business continuity planning expertise to clients in the western territory, developing complex response and recovery plans for client companies. He is a member of NFPA, BCSP, RIMS and Disaster Recovery Institute International, and he is a professional member of ASSE's Gulf Coast Chapter.

©ISTOCKPHOTO.COM/THINKSTOCK

with the organization's day-to-day decision making rather than standing on the sidelines until disaster strikes. The volume of an organization's data available to the SMB safety professional should help support the decision-making process. Business continuity should become integral to defining and shaping business decisions to ensure that, even after an adverse event, the company can survive. This is similar to the proactive approach that safety professionals take concerning employee well-being.

Every business has objectives and plans—whether they are to achieve a profitable year, increased market share, name recognition, ROI or other goals. The E&BC plans should contemplate how to meet these objectives. It is no longer acceptable to just return the business to where it was before the event. Plans must enable the business to grow and meet these objectives despite adverse events. Plans must be regularly updated and refined to reflect changing business conditions and activities.

In the past, E&BC plans often sat outdated and no longer able to meet the new challenges of a changing business climate. Studies have shown that large corporations see a correlation between their ability to recover from a catastrophe and the value of their stock price. In man-made disasters, there can be as much as a 25% variation in stock price (Knight & Pretty, 2001).

Developing Your Plan

NFPA 1600 Standard on Disaster/Emergency Mangagement and Business Continuity Programs is recognized as the National Preparedness Standard. It has formed the basis for many E&BC plans in business and government agencies. To help implement the standard, a companion guidebook was written in 2007 by a group of continuity experts. The book dedicates a chapter to each of the eight phases of plan development (Figure 1, p. 52):

1) program management;
2) risk assessment;
3) prevention and mitigation;
4) resource management;
5) plan development;
6) training;
7) exercise and corrective actions;
8) program revision.

The guide describes the goal of each phase and provides tips for developing a plan for an organization. The book also includes checklists, forms and questionnaires essential to the plan-development process. Among the key documents are the business impact analysis checklist, cost-benefit analysis worksheet and a damage assessment form (see "Things to Consider" sidebar, p. 52).

Building the Team

Developing an E&BC plan requires the efforts of a knowledgeable team. This is not a one-person job due to the complexity of today's SMB. An organization's safety professional may touch on all areas of the business, but most likely will not have in-depth knowledge of each area and its interaction with other segments of the business. Building a team of experts will help ensure access to the knowledge required to develop a robust and detailed plan that encompasses all areas of the company and reflects the symbiotic nature of various areas.

Figure 1
Phases of Developing a Business Continuity Plan

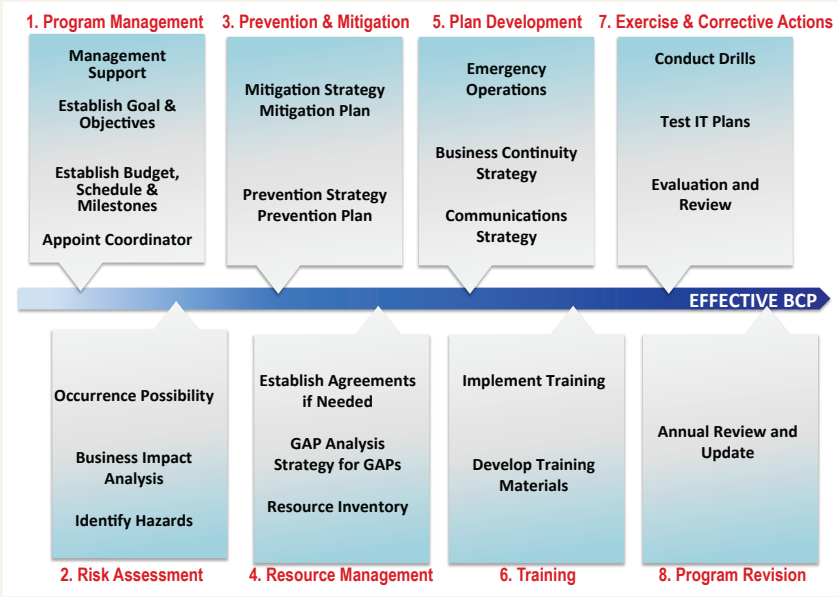


Figure 1 illustrates the eight phases of business continuity plan development.

Before building the E&BC team, the safety professional must have senior management support. Management commitment, direction and support are essential to ultimate success. This support is also crucial in funding the E&BC plans.

The E&BC team should include individuals with expertise in the critical functions within an organization (e.g., finance, manufacturing, human resources, IT, quality control, communications, legal, marketing). The exact makeup of the team will vary based on the operation's size and complexity.

The ideal team should not exceed 10 primary members and may have as few as three (for the smallest companies). Alternates are necessary to fill in for people when they go on vacation, leave the company or change roles.

The safety professional's role is to lead this team and manage the project. In leading the team, s/he must provide clear direction and purpose, much of which comes from the built-in senior management team support. This direction is expressed in a mission statement approved by senior management outlining the expected roles and responsibilities of the E&BC team. This information must be communicated to the team and motivate all members to embrace this commitment in addition to their other responsibilities. Few SMB companies have the luxury of a full-time dedicated staff to develop and maintain their E&BC plans.

Assessing Risk

Experience has shown that safety professionals use several different methods to assess risk when building an E&BC plan. Many SMBs use the "I think" method to determine which risk they would or would not include in the overall plan. While this method may work well for some organizations, it does not truly identify the risk and the potential impact to the organization.

Another method is to develop a matrix with severity along one axis and impact along another, then concentrate only on those incidents that demonstrate high impact and severity. A complex numbering system that scores impact probability and resource availability might also be used when developing the plan (Figure 2).

Some SMBs just list past events and develop plans to manage a potential recurrence. However, as business and the world have become more complex, this best-guess approach is inadequate. Investors, owners and key stakeholders want more definitive and quantifiable indications of the risk. One can assess risk more effectively and accurately on an individual-site basis and with an emphasis on statistical probability.

The changing landscape of risk assessment is evident in various journal articles and in resources that focus on terrorist and pandemic events. Most SMBs focus on preparing for fires, weather events and workplace violence. However, as the world changes, businesses must consider new potential threats. The U.S. government has created documents to help employees assess and quantify risk for terrorism, pandemics and other emerging risks. One example is the Risk Management Series offered by the U.S. Department of Homeland Security (DHS), which includes the *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks*.

Sophisticated weather tracking software allows experts to predict a hurricane's movement over a 5-day period. National Hurricane Center estimates that the accuracy of its 48-hour predictions for tropical storm tracking has improved to 95%. For companies located in the storm's path, these systems can identify the most vulnerable sites so

Things to Consider

- **Staff experience.** Does anyone on staff have experience?
- **IT complexity.** Do you need a trusted partner to assist?
- **Management commitment.** Will management support the time required for a long-term project?
- **Budget.** Is budget or funding available for the project?
- **Project scope.** Start with a single plant, then expand to other sites.
- **Learn the topic.** Attend seminars/read articles to understand the basic concepts.
- **Talk to others.** Ask around. Maybe someone was in your shoes a year ago.
- **Regulatory issues.** What specific regulatory or contract issues must be considered?
- **Resources.** What resources are available and what will be required?

they may marshal limited resources. These systems also provide real-time weather alerts. Commercially available weather tracking software such as Weather Defender (**www.weatherdefender.com**) or StormPulse (**www.stormpulse.com**) can identify and follow various weather patterns including tornadoes, high winds, ice storms, hail or severe winter weather, and provide alerts to help businesses better prepare for these events.

Figure 2
Hazard Assessment Matrix

Hazard Assessment Matrix

Hazard	Probability (High 5 ← → Low 1)	Human Impact	Property Impact	Business Impact (High Impact 5 ← → Low Impact 1)	Internal Resources	External Resources (Weak Resources 5 ← → Strong Resources 1)	Total	Hazard Mitigation Actions
							0	
							0	
							0	
							0	

Figure 2 shows an example of a complex numbering system used to score impact probability and resource availability.

Plan Documentation

Today, most E&BC plans are developed using word-processing software and are ultimately printed and stored in a binder. Some SMBs may also use a virtual team room to allow for document sharing and input before creating a final document. This process is cumbersome and may cause confusion during the editing process. In addition, while a plan in a binder may be useful, it is difficult to keep the documents up-to-date as risks and the business evolve, and it may be impossible to access if employees are off site or if an event prevents access to the facility where the plan is kept.

As a result, many companies are moving away from the stand-alone word-processed plan that resides in a three-ring binder. More companies are developing E&BC plans closely tied to operating systems that are already in place within the organization. Most of these systems are server-based and offer direct access to data mining of corporate files to allow for resource allocation, asset tracking and staffing information. These systems offer remote access and real-time information updates based on changing business conditions. Additionally, some programs may tie into external information feeds such as weather alerts and threat assessment software from third-party vendors.

The recent advent of cloud computing has also changed the way E&BC plans are documented. Cloud computing is a way of storing information and processing software off site with a third party so that it can be accessed by various means. Storing business continuity plans in the cloud makes them accessible via laptop computers, smartphones and tablets. In addition, access to the business continuity plan and other information is not subject to the events affecting the location that the plan was designed to protect.

However, as with most technology, this approach raises additional concerns such as the security of critical data or the server itself, as well as other Internet vulnerabilities. If power is lost or the Internet is no longer accessible, then cloud-based plans and corporate data are no longer retrievable. Therefore, to be fully protected, SMBs should maintain backup servers and duplicates of data (Hill, 2011).

As with most technology, the use of new software and cloud computing for business continuity plans is a rapidly developing area and must be constantly reviewed to ensure that these tools meet SMB needs. Several resources are available to help compare competing software packages. The cost for many of these new integrated plan-development and tracking systems is often more than the technology employed today and is a factor the SMB must consider.

While new technology provides great possibilities, safety professionals must guard against fill-in-the-blank programs that require little or no true input from the organization. Regardless of which program is chosen, the E&BC team must be involved in the selection process. Rarely will software out of the box directly meet an organization's true needs (2011 Software Surveys, 2011).

Crisis Communications

Business continuity plans rely on various communication methods to disseminate information to a large group of people via telephone, e-mail, text messages and social media. In addition, third-party vendors provide notification services to employees, customers and others if a company must disseminate a message regarding a disaster or emergency. The telephone call tree remains a popular way to get information out. Unfortunately, this method cannot ensure notification of everyone. Current notification systems allow for tracking and verification of the message through various options such as polling and contact reports (Witty, Girard & Goldstein, 2012).

Even as robust and prolific as telephones and mobile devices have become, they have some drawbacks, especially when the power is down or too many people try to access the system at the same time. During events such as Hurricane Katrina and Sept. 11, 2001, mobile carriers were quickly overloaded, leaving people in a communication abyss. Many planners typically use SMS (short message service) texting (Wikipedia, 2012) as a backup since it relies on a different communications infrastructure. Nevertheless, even texting systems can be overloaded as was demonstrated during the 2011 East Coast earthquake (Woyke, 2011).

Without question, efforts to communicate about emergencies with large groups of people will continue to include methods such as call trees, e-mail and radio. Fortunately, new communication tools, such as social media (e.g., Twitter, Facebook, Google+) will enhance the ability to spread the word. The use of social media requires special understanding by both the planner and recipient as to what information can and cannot be disseminated. Social media is less secure than phone calls or e-mail, so information disseminated through social media should be treated like public announcements. The next generation of business continuity plans should include specific policies regarding who should be sharing information, how information should be shared and what type of information can be sent out through the various media (Hill, 2011).

Training & Testing

"No plan of action has any value until proven. Even then, it is of little value until all of the actors have practiced their performance" (Burtles, 2007). Testing has always been a component of any E&BC plan; the challenge continues to be conducting meaningful testing and not just including it in the plan. As the next generation of business continuity planning develops testing will become more necessary because of the plans' increasing complexity and because of regulatory requirements, clients, vendors and stakeholders will mandate testing and certification. Some tests will be mandatory, while others will be recommended, such as the Private-Sector Preparedness recommendation (see Private-Sector Preparedness: A National Perspective sidebar) made by the 9/11 Commission (National Commission on Terrorist Attacks Upon the U.S., 2004). Clients are also requiring more proof that an E&BC plan will actually work. Satisfying client audits will now require more than just checking a box on a form; testing, test results and follow up to improve the E&BC plan will need to be documented.

Once again, as plans become more complex, testing becomes more expensive. More plans will need to be tested using simulations and functional exercises versus orientations and tabletop reviews. By becoming more efficient in what is tested, it may be possible to control expenses without sacrificing results. A company must take advantage of what is learned from testing and implement it back into the plan—despite economic pressures. If companies don't incorporate the lessons learned, they may find themselves faced with the same issues during actual incidents (Figure 3).

Testing must include all individuals involved in E&BC activities, as well as an organization's suppliers. Previously, little or no emphasis was given to SMB vendors/suppliers and their ability to meet the organization's needs. As the economy and business practices have changed, vendors/suppliers have become more intertwined with an organization's ability to respond to disasters.

Emergency Response

Depending on the event, different individuals will be essential to the response. The correct staff will understand the event and take actions to help mitigate the damage and/or prevent loss of life. Various alarms must be present throughout the workplace. These may include fire alarms, water motor gongs, emergency exit buzzers, elevator alarms and car alarms. Does the staff know how to respond to each alarm? The plan should identify the various alarms and actions needed to investigate the reason for the alarm. A company must also ensure that everyone throughout the site can hear the alarm. For instance, water motor gongs are notorious for only being heard outside, because inside noise from machinery masks the sound of the alarm.

Exit diagrams are needed to direct staff to a safe location either inside the building

Private-Sector Preparedness: A National Perspective

Responsibility for preparedness for a national calamity does not rest with the federal, state or local governments. Neither is it the sole responsibility of the Department of Homeland Security (DHS). This was pointed out in the 9/11 Commission Report. One of the findings and recommendations from this commission was that a voluntary National Preparedness Standard be endorsed. The 9/11 Commission also determined that preparedness in both the private and public sectors should include 1) a plan for evacuation; 2) adequate communications capabilities; and 3) a plan for continuity of operations. The recommendation reads as follows:

> *We endorse the American National Standards Institute's [ANSI's] recommended standard for private preparedness. We were encouraged by Secretary Tom Ridge's praise of the standard and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company's compliance with ANSI standards in assessing its insurability and creditworthiness. We believe that compliance with the standard should define the standard for care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in a post-9/11 world. It is ignored at a tremendous potential cost in lives, money and national security.*

In 2007, at the direction of Congress, DHS set in place a voluntary program to serve as a resource for private and nonprofit organizations that are establishing comprehensive business continuity plans. As part of the PS-Prep program, it offers the opportunity for these organizations to develop and maintain certification to nationally recognized standards. More information about PS-Prep is available from **www.fema.gov/ps-preptm-voluntary-private-sector-preparedness**.

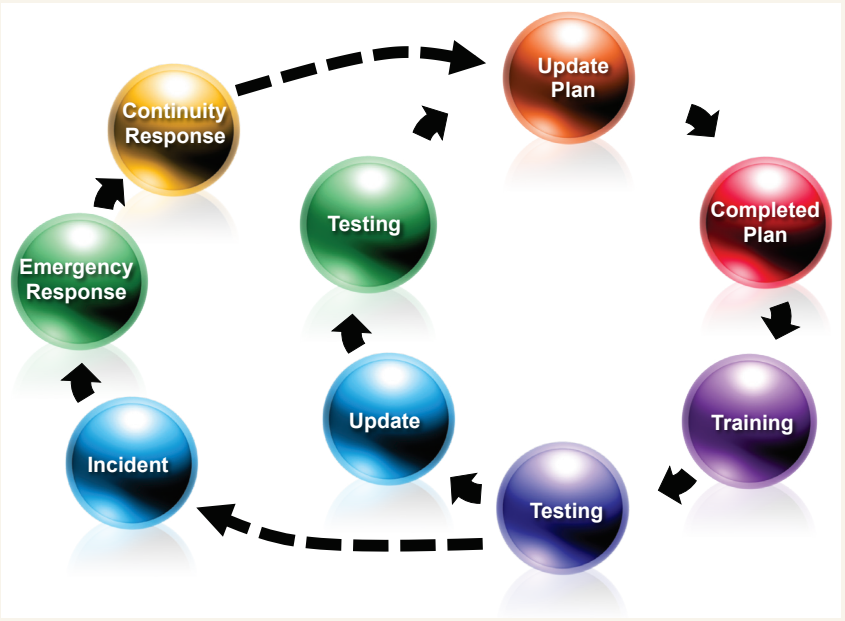
during a tornado or to the exterior of the building during a fire. These diagrams should include color-coded primary and secondary exit routes, the location of fire extinguishers, areas of refuge within the building and gathering points outside the building.

Available Resources

Developing an E&BC plan that reflects today's complex business operations and the global business world is a challenging task. But, various resources are available to help safety professionals develop these plans. Industry group websites, such as Continuity Insights or the *Disaster Recovery Journal* (DRJ), offer tools that guide risk assessment and business-impact analysis. Federal Emergency Management Agency offers specific guidance for protecting large and small businesses. This includes preparation tips for windstorms, wildfires and earthquakes; recommended contents of a disaster supply kit; and flood analysis. Find these tips at **www.ready.gov**.

The Institute for Business and Home Safety (IBHS) provides an online risk-assessment tool for E&BC planners. IBHS also provides plan document templates (**http://disastersafety.org**). Consensus standards such as NFPA 1600 and 1620 and ASIS/BSI Business Continuity Management Standards provide a set of criteria for these plans. Copies of the NFPA and ASIS standards are available as a free download at **http://goo.gl/ojumQ**. Training seminars are offered by DRJ and Disaster Recovery Institute International to hone the skills needed to develop these plans. **PS**

Figure 3
Testing & Update Cycle



Note. *Adapted from The next generation of SMB emergency response and business continuity planning, by S. Nicoll & R. Owens, 2011,* Proceedings of ASSE's Safety 2012, *Denver, CO.*

Figure 3 illustrates the cycle used to test and update plans in order to become more efficient, which saves time and expenses.

References

2011 Software Surveys. (2011, Fall). *Disaster Recovery Journal, 24*(4), 74-80. Retrieved from **www.drjournal-digital.com/drjournal/fall2011?pg=14#pg76**

Burtles, J. (2007). *Principles and practices of business continuity: Tools and techniques*. Brookfield, CT: Rothstein Associates Inc.

Hill, B. (2011). 5 trends in preparedness: 2012 forecast [webinar]. Retrieved from **www2.preparis.com/l/2492/2011-11-18/BPVG0**

Hookway, J. & Poon, A. (2011, March 18). Crisis tests supply chain's weak links. *The Wall Street Journal*. Retrieved from **http://online.wsj.com/article/SB10001424052748703818204576206170102048018.html**

Insurance Institute for Business & Home Safety. (2012). Every business should consider a risk and vulnerability assessment. Retrieved from **http://disastersafety.org/commercial_maintenance/commercial-vulnerability-assessment_ibhs**

Kelly, R.B. (1989). *Industrial emergency preparedness*. New York, NY: Van Nostrand Reinhold.

Knight, R.F. & Pretty, D.J. (2001). *Reputation and value: The case of corporate catastrophes*. London, U.K.: Oxford Metrica.

Mah, K. (2012, Winter). Change or perish! Business continuity management as an operational competitive edge. *Disaster Recovery Journal*, 25(1), 42-43. Retrieved from **www.drjournal-digital.com/drjournal/winter2012#pg44**

National Commission on Terrorist Attacks Upon the U.S. (2004). The 9/11 commission report. Washington, DC: Author.

Nicoll, S. & Owens, R. (2011). The next generation of SMB emergency response and business continuity planning. *Proceedings of ASSE's Safety 2012, Denver, CO.*

Short Message Service. (2012). Wikipedia. Retrieved from **http://en.wikipedia.org/wiki/SMS**

Stronach, R.I. & Raisch, W.G. (2007). Introduction to emergency management and business continuity. In D.L. Schmidt (Ed.), *Implementing NFPA 1600 National Preparedness Standard* (p. 2). Quincy, MA: NFPA.

Witty, R.J., Girard, J. & Goldstein, C.H. (2012). Magic quadrant for U.S. emergency/mass notification services. Retrieved from **www.gartner.com/technology/reprints.do?id=1-19Q6C7Z&ct=120316&st=sb**

Woyke, E. (2011, Aug. 23). East Coast quake a reminder of cell network reality. *Forbes*. Retrieved from **www.forbes.com/sites/elizabethwoyke/2011/08/23/east-coast-quake-a-reminder-of-cell-network-reality**