Improving your organization's preparedness for disaster requires a highly detailed and objective effort to identify and understand threats to your organization, customers, and the public.

Current events demand a new approach to response/continuity planning. It is no longer prudent or diligent to merely plan for what you know will occur and what the likely consequences will be. Today's preparations must be developed to anticipate and plan for less well known vulnerabilities, including conditions that exist but have not been traditionally threatening.

Vulnerability identification and Risk assessment are challenges that face all industries and functional areas as they prepare and evaluate their emergency response/business continuity plan. All too frequently vulnerability and risk are confused even though they distinct and unique meanings and an intertwined relationship. Vulnerability is 'what' an organization or the general public may be susceptible to, while Risk is the possible consequence attributable to that vulnerability. The development and assessment of emergency response and/or business continuity plans becomes confusing and complex because of the interchange of these terms. A consequence of this interchange is that emergency response/business continuity plans are developed with incomplete or incorrect assumptions, avoidable latent obstacles, and embedded issues that result in conditions that obscure the objective and often compound the event they were designed to mitigate. The inevitable result is an even bigger challenge. The verification and validation of vulnerability and risk inherent within response/continuity plans from:

- Frailties of the supporting infrastructure;
- Adequacy and applicability of policies, practices and procedures as compared to "best practices";
- Mismatches between existing processes and identified requirements;
- Mismatches between existing processes and infrastructure's true, practical ability to withstand threats to business continuity.

Organizations of all kinds conduct supplier certification programs because they are able to obtain a great deal of specific information about their vendor base. Specifically, a survey-based approach to supplier certification can help your organization:

- Choose vendors that present the smallest risk to the supply chain;
- Identify differences among suppliers with respect to business continuity, quality control, and security policies and practices;
- Identify and prioritize the risks associated with current vendor relationships;
- Collect supplier feedback and satisfaction information from internal stakeholders;
- Establish a system of standards for vendors, and set benchmarks for continuous improvement.

Historically, preparation for potential business and public safety vulnerabilities has focused on regional or isolated natural, manmade mischief, and accidental events. Recently, intentional acts (terrorism) have been a higher priority in the list of vulnerabilities that may occur simultaneously at local, regional, and national levels. The threat of terrorism is further compounded by technological evolution and information availability. This combination of recent vulnerabilities and new challenges undermines the historical assumptions and needs employed in planning; historically based plans have become inappropriate, invalid, and potentially reduce response effectiveness.

To maintain validity, Response/Continuity Plans, and the evaluation and assessment process built into these plans, require a proven methodology: fact based, integrated, and at a detail level. Furthermore, the preparation and evaluation processes must be replicable and traceable, providing a foundation for users to understand how the plans were built and revised so that future users can expand on the basis to meet future challenges.

Current events demand a new approach to response/continuity planning. It is no longer prudent or diligent to merely plan for what you know will occur and what the likely consequences will be. Today's preparations must be developed to anticipate and plan for less well known vulnerabilities, including existing but unqualified conditions.

Vulnerabilities should be evaluated and classified for risk severity and probability. The classification of severity and probability requires a 'handshake' between stakeholder processes and the response/continuity plan process. Key interface information must be current and coordinated and the providing organization's response/continuity plan must correspond with stakeholder needs and processes. The 'handshake' or processes integration requires the evaluation of all practices, procedures, and supporting infrastructure to assure stakeholder needs can be satisfied under all circumstances in accordance with expectations.

This approach is further validated by the Department of Homeland Security's recent report which pronounced the need to identify events (vulnerabilities) and prioritize the possibility of the event (risk) occurring at a location where a large adverse impact may result (risk management/risk based planning) to the public and business.

Preparers of response/continuity plans must recognize and understand that the "worst case scenario" is not predictable. It is not an extreme condition of a single vulnerability. Rather, it is an unpredictable combination of vulnerabilities that occur or even the consequences of a limited number of unrelated events. This realization is critical for developing a response/continuity plan that is flexible, adjustable, and 'implementable' "on the fly" to satisfy evolving conditions and emerging challenges.

Evaluating established and implemented response/continuity plans should be performed on a regular basis to continuously verify and validate the effectiveness of the plan within the organization and in communication with stakeholders. For a response/continuity plan to achieve its purpose, people, processes, and products must be properly integrated and prepared. Conducting confidential and proprietary assessments of response/continuity plans consists of three steps:

- Development of Review Plans
- Test the response/continuity plan's thoroughness,
- Web-based Interviews that correspond to and augment face-to-face interviews and web-based tools which provide a mechanism to capture, process, and analyze Review Plan data development,
- Review of functions, assignments, responsibilities, and communications
- Orientation and Training of Staff and Stakeholders
- Results, lessons learned, and corrective action processes in the plans

Thorough evaluations include face-to-face and web-based interviews to supplement and provide perspective for collected data. Interviews are used as a confirmatory process or to assist our understanding. In a fact based approach, interview data alone should never be the basis for an opinion or recommendation. With web-based surveys to provide a confidential and secure library of information, you do not have to wonder how the people in your organization would respond to a threat. Essential to this process is the ability to be able to produce live results and statistical data as information is collected throughout the survey process.

A critical effectiveness assessment employing a series of participant and stakeholder exercises is also included to challenge individual and collective knowledge with the plan. Practical training and the promotion of awareness are ideally accomplished through individual exercises so that needs for improvement can identified at the proper level of detail. These exercises can be performed in a cost effective manner employing face-to-face meetings, web-based exercises, or a combination of both. The objective is to prepare individuals for a Real Time Simulation Exercise. Augmenting and complementing these exercises are two frequently overlooked activities that add significant value to the entire assessment process. They are Lessons Learned and Results Integration and Incorporation.

These activities do not require a large investment on the part of the participants and stakeholders and yield major returns. Through the use of structured end of exercise questions and web-based interviews, information identifying strengths and weaknesses should be monitored continuously. Data collected from the participants and stakeholders is assessed and recommendations for improvement and a timetable for implementation are prepared for the organization.

An effective and 'implementable' plan requires vulnerability and risk evaluation to assure that the plan does not impose additional burdens in responding to anticipated adverse events.

A vulnerability and risk assessment requires a fact based, integrated, and detailed process that is repeatable and traceable. Our experience, using this assessment methodology, provides high confidence the process is solid and repeatable. It provides the foundation from which organizations can expand and build their plans to meet currently unforeseen challenges to ensure safety and stability for both individual businesses as well as public safety. A cost effective and efficient results oriented evaluation process designed to examine the relationship of people, process, and procedures establishes the success equation for verifying and validating Vulnerability and Risk that exist in emergency response/business continuity plans, is absolutely critical in any organization.

Robert Luzzatto is a consultant specializing in helping organizations establish and maintain web-based survey programs.

QUANTANIA
color X numbers