Have You Overlooked a Key Area of Risk Management?

By Mark Pickett, CPP, Vice President for Wackenhut's Consulting Services

Risk avoidance in today's environment is one of the hottest topics among security managers and risk administrators throughout corporate America. We have seen a focus on increased security planning and prevention tactics. The security industry as a whole has been busy as managers examine every aspect of their security programs to ensure they are as prepared as possible. A major focus of their activities has been on security detection and deterrence principles, and in mirroring the direction of the U.S. Department of Homeland Security, and rightly so. But to a large extent one key area has been overlooked by most companies, that of business continuity planning. This is primarily because organizational lines of responsibility in corporate security do not always include and address the function of business continuity. We often find this responsibility excluded from the security function and contrary to that norm, there is no better place for the

responsibility to reside. Few business functions are as capable or prepared to react to the emergency and crisis situations than the physical security department and the officers trained for the response. There is another organizational issue that may be preventing an integrated approach to business continuity planning. A recent study found that most major companies manage their security responsibilities in a decentralized way, usually through three distinct silos consisting of Physical Security, IT Security, and Risk Management. The end effect is that initiatives requiring well-coordinated planning and training are difficult if not impossible to achieve.

Executive management has an obligation to its employees and stockholders to assure that everything that can reasonably be done to protect the business and ensure its survival is done and security management can proactively assist.

"Managers should have an ongoing focus of the value of business continuity as an element of risk management in their departments".

What can Security Managers do?

Security managers and professional practitioners do, by nature, recognize the importance of being prepared and know how to respond to emergency situations. If the function of business continuity planning is currently part of your overall responsibility, as a security manager, then dust off the program and conduct a quick check of your company's preparedness and responsiveness by examining the Ten Action Steps provided below. If you don't have the responsibility of continuity planning, or your company does not currently have an integrated business continuity plan, then take the initiative. The Ten Action Steps presented below will help you make a case to your senior management for why a plan should be developed and implemented, now.

Why an integrated approach to Business Continuity?

The old approach to business resumption has changed, largely because the corporate environment did not integrate it as a vital business function. Business continuity relates specifically to the continuation and survival of the core function of the enterprise. It is so important that the continuity plan should be a way of doing the business, not just an adjunct to the business. In other words, business models and functional departments within the enterprise must incorporate continuity practices as a normal way of conducting the business of their department. IT departments are the best example of this approach. They cannot afford to loose or have electronic information inaccessible so they integrate continuity practices as part of their normal business functions. However I would venture to say that other vital business departments such as, Legal, Human Resources, etc., would have a difficult time recovering from a crisis if they have not integrated continuity principles into their operations.

Mark Pickett, CPP
Vice President
Wackenhut Consulting Services

Mark Pickett, CPP, is the Vice President of Consulting Services for the Wackenhut Corporation. He is an expert in physical security with over 25 years experience in providing loss prevention control, physical risk assessments, threat and vulnerability analysis, electronic system design and evaluation, systems integration planning, and security operational evaluations. Mr. Pickett is a CPP, Certified Protection Professional, and a member of the American Society for Industrial Security.

[1] The Conference Board, Managing Corporate Security: Patterns of Organization, Executive Action No. 60, July 2003

An integrated approach to business continuity requires organizations to merge the many standalone efforts into a cohesive process that blends strategy, competitive intelligence and event, or response-driven management together. This blended strategy or approach can then facilitate the typical "pro-active" planning principles of detection and deterrence. It can enhance education and awareness programs, and training and response capabilities. A truly integrated continuity plan provides value by reducing multiple plans down to a single format plan that is readily manageable. It provides a consistent framework for operations, whereas separate plans for disaster recovery, emergency response, and crisis management can create confusion, duplication of effort, depletion of resources and possibly cause inaction. An integrated plan provides a consistent response process and framework for operations. It should blend strategy and competitive intelligence into business continuity processes. It will enhance security safeguards against errors and omissions and provide a basis for assuring operational resilience through prepared responses. Most significant, an integrated business continuity plan should enhance clear communications between the continuity facilitation team and external business partners because these partners will become vital to the organization during the recovery process.

Phased Approach to the Planning Process

Phase	Task
Assessment and Business Impact Analysis	•Perform Risk Assessment •Assess Existing Mitigation Programs •Determine Mission Critical Processes •Determine Potential Impacts •Develop Response Recovery Procedures
Strategy Evaluation and Selection	•Define Event Response Strategies •Compare Response Strategies to Timeframes and Resources •Perform Cost Benefit Analysis •Establish Preferred Strategy •Document Selection Rationale
Business Continuity Plan Development and Documentation	•Analysis Existing Plans and Operating Procedures •Prepare Draft Continuity Plan •Prepare Standard Operating Procedures •Finalize Continuity Plan and Supporting Materials •Identify Plan Commitments and Establish Tracking System
Testing and Maintenance	•Design Training Program •Design Testing Protocols •Develop and Facilitate Simulation Exercise •Develop Maintenance Procedures •Establish Audit Plan

Ten Action Steps

Reviewing and then implementing the following ten action steps within the context of your own situation can produce positive results for your organization. They are presented in no order of precedence but you should assess their applicability and prioritize them as it fits your unique situation.

1. Make your enterprise an unattractive target.

Although it may be contrary to the golden rule of advertising, make your place of business as inconspicuous as you can. Additionally, present an immediate or sudden image of security and protection. Identify appropriate psychological barriers and deterrents that would be effective in saying, "not here you don't".

2. Revise employee screening processes

If your company does not provide an in-depth background search on new-hires then management is placing employees and assets at great risk. Basic due diligence principles validates that you need to know whom you are hiring. At a minimum you should conduct a background check that includes the following.

- Social Security Number Confirmation Trace
- Credit Report for Employment Purposes
- Verification of Activity for Last 7 Years, to include:
- Prior Employment
- Education
- Unemployment of 60 days or more
- Criminal Record History
- Nationwide Wants and Warrants
- Residential Addresses for Last 7 Years
- Statewide Searches (where available)
- State Driving Record History
- Specially Designated Nationals and Block Persons List

3. Validate business, community and government contracts

Know whom your company is doing business with. Conducting due diligence investigations with suppliers, vendors and customers will help reduce issues of fraud and work stoppage. It will also help prevent liability issues through third party criminal activity.

4. Assess business continuity plans

If your company already has a business continuity plan then consider the following.

- Does the plan present an integrated approach by incorporating recovery, emergency response and crisis management issues?
- Is your plan current?
- Has your facilitation team exercised the plan within the last 12 months?
- When was the plan last revised or updated?

[2] Ten Action Steps developed by Geary W. Sikich, a Principal of Logistical Management, Corp. and a strategic alliance partner of The Wackenhut Corporation. By permission.

5. Train and educate your workforce

Practitioners know and understand that the best of plans never work unless the employee base has been properly trained and know how to respond in an appropriate manner. Continuing to educate employees, key managers and plan facilitators will make or break the recovery process. Key players in a response or recovery program cannot perform if they don't understand their role. Train, exercise, train and exercise again.

6. Equip your workforce

Make sure your workforce has the tools necessary to fulfill their role in an emergency recovery situation. Do key facilitators understand the plan objectives and have they been equipped with the authority, means and tools to accomplish their role?

7. Review leases and contracts for risk exposure

Current lease agreements and contracts for operating centers, sales offices, administrative offices and contingency backup locations, should be reviewed to identify potential risk exposure. Are lease arrangements for potential relocation sites current? Considerations should include whether or not contracts may have clauses that provide for business asset losses or security protection provisions. Is, for example, the landlord responsible for providing a certain level of security, and if property loss occurs can he be held liable? Is it stated or implied that the lessee is responsible for rent or payment of utilities if the property is uninhabitable? How do your insurance provisions provide for the gap caused by lease or contract shortfalls?

8. Assess value-chain exposure to supply disruptions

Critical to all organizations is their value chain. The value chain includes all internal and external "touchpoints" to suppliers, customers, outsourcing, strategic partners and other entities that assure your organization's continued success. As with the critical infrastructure assessments, your organization needs to assess the potential effects of a disruption of its value chain to supply disruptions. In conducting the assessment a variety of scenarios need to be developed to assess the short term, intermediate term, and long-term effects of a disruption.

9. Review insurance policies and conduct cost/benefit analysis

As a result of the events that occurred on September 11, 2001 and subsequent events taking place now, a review of insurance policies with respect to coverage, exclusions and exceptions needs to be accomplished. Insurance companies have been and will be impacted by the events of September 11th and events yet to occur. Many organizations will find that a cost benefit analysis will offer an effective aid to decision-making processes, strategy planning and the development of risk reduction solutions.

10. Communicate commitment

Executive management must demonstrate their commitment by being involved in the plan exercise implementation process. Key facilitators and other employees must also know of and understand the importance of this commitment level. Additionally, executive management should clearly understand that plan implementation protects them as well as the company.

In describing the first hours after the terrorist attack of the World Trade Center towers, Rudy Giuliani in his book Leadership, describes how difficult it was for city government to find a back-up command center as part of the recovery process. In fact they dismissed four alternate locations before finding a building that could accommodate the space requirements for their command purposes. He describes how unprepared they were because they never imaged that this kind of devastation could happen to them, not in New York City. Unfortunately, most of corporate America will experience the same issue if they fail to focus on their integrated recovery processes.

It is time to take action. Start now, by planning an appropriate response to a crisis so that your company is ready and able to survive.

The Wackenhut Corporation, founded in 1954, is a leading provider of security and related servicces to major corporations, government agencies, and a wide range of industrial and commercial customers. The U.S.-based subsidiary of Group 4 Falck A/S, Wackenhut is a global provider of consulting and investigation services, which include: Risk Assessments, Crisis Management and Response Services, Ethics and Compliance Services and more. If you would like more information on how we can help you, please contact us at our Palm Beach Gardens Headquarters at 800-275-8310.