



Crisis Management and Business Continuity Council

August 2011

Council Chair

James J. Leflar Jr, CPP, CBCP

Vice Chair

Andrea Hollman

Members

Bruce Blythe

Whit Chaiyabhat, CEM, CBCP, PI

Gerald D. Curry

Ernest DelBuono

Anthony V. DiSalvatore CPP, PSP, PCI, CFE, CLSD

Chris Foster, CPP, CBCP, MBCI, ITILV3

Marc E. Glasser, CPP, CEM, CORP, CHS-V, CMAS

Briane M. Grey

Mike Gross, CPP, MEP

Donald E. Knox, CPP, CITRMS

Grant Lecky, PCIP, ABCP, Msysl

James E. Lukaszewski, ABC, APR, Fellow PRSA

John E. McFadden, CPP

Murray D. Mills, CPP

W. Barry Nixon, SPHR

Werner Preining, CPP, CMAS

Allan E. Schwartz, CPP, CHS-III

David A. Spector

Tanya Spencer

Randy Spivey

Samuel J. Stahl, CBCP

Ernest G. Vendrell, CPP, CEM

Keith J. Wagner, CPP

Scott A. Watson, CPP, CFE

Robert M. Weronik, CPP

Richard P. Wright, CPP

Paul Yung

Vehicle Armoring—An Overview

Part 2 of 2

In the last edition of the CMBC Newsletter, Part 1 of "Vehicle Armoring" discussed international standards, armoring material and the armoring process. Part 2 concludes the series with vehicle selection and choosing the vendor.

Vehicle Selection

Selecting the correct vehicle and armoring package results from careful analysis of a number of factors. There are always tradeoffs between armoring and performance, and the correct mix is essential. In a perfect world, all armored vehicles would be level V (for combat zones) and perform like sports cars or off-road vehicles. This, unfortunately, is not realistic, and identifying the proper combination for any given user requires thoughtful analysis.

To determine what type of vehicle is required, initial analysis must focus on the threat level, including the reason why an armored vehicle is necessary. Another fundamental determination is the when, where and how often of proposed movements. A heavily armored sedan is no more useful in a rural setting with a degraded road network

than a lightly armored off-road vehicle used exclusively in a densely populated urban area.

The type of use to which a vehicle will be put is also important. If a vehicle is to be used for transporting many passengers with luggage or briefcases, an SUV is more logical than a sedan. If to be used only for transporting VIPs, a sedan may be the best choice. There are a myriad of options and all merit consideration.

As part of the process, due consideration should also be given to the possible requirement to reinforce brakes, suspension or transmission and to ensure that sufficient horsepower and torque are available in the chosen model.

(Continued on page 2)



(Vehicle Armoring, continued from page 1)

Armoring levels should be determined by an evaluation of the present and potential threat. If assault rifles are common in the zone of operation, a heavier level of armoring with associated movement limitations is probably necessary. If handguns are the major problem, a lighter armoring package that offers more operational flexibility should be considered.

This is an issue that requires analysis; the use of a few AK-47s in a robbery last year does not necessarily call for a higher level of armoring. Modern level IIIA armor will usually stop at least one such round, although not guaranteed, and the second or third round is in all probability coming through the door or window.

Once all the relevant factors have been considered and a judgment made as to which package should be ordered for which vehicle, only then should a vehicle be ordered.

Selecting and Monitoring an Armorer

The process of selecting the proper company to armor a vehicle is the single most important part of the entire process. There are many companies that claim to be first-rate suppliers, and all vendors will state unequivocally that none of their vehicles

has ever suffered a cabin penetration. After all, buyers certainly do not wish to invest with an organization that prominently mentions failures.

Based upon the many different materials used and methods of armoring practiced, some organizations are most definitely better than others.

The process of selecting the proper company to armor a vehicle is the single most important part of the entire process.

The initial step is to identify those companies that could provide the service for a client organization. There are often limitations on what companies can do. Some of the largest and most renowned companies in the world have such backlogs that waiting periods may exceed two years or more, particularly if that company is performing work for the military as well as private clients. Others may be located in countries from which importation is prohibitively expensive, or the client may be located in a place in which importation is a tedious and delay-filled process. If local options are available, they should always be thoroughly examined.

Once potential vendors have been identified, proposals for the determined level of armoring on the selected type of vehicle should be solicited. Vendor proposals often provide a wealth of information about the company and can help a client discard obviously unqualified suitors without further waste of time. Information on the average proposal includes the materials used, time frame, and cost, and will often provide references that can be verified.

Professionalism in presentation is always important, although some of the slickest presentations are used to cover the most inept of organizations. Reviewing proposals helps determine whether or not a vendor is overpriced, whether the materials to be used are adequate to the task, and whether the vendor can fulfill a contract within a reasonable timeframe.

(Continued on page 6)



Council Conducts Crisis Management Training

Across the globe, the top priority of every CEO, corporate manager and building owner is to keep the organization operational and in the black. He/she must anticipate emergencies or crises of any proportions, natural or man-made, and be prepared to react to that emergency.

To assist in that objective, the Crisis Management and Business Continuity (CMBC) Council of ASIS International conducted a four day seminar and workshop in Boston from May 23 to 26, 2011. The seminar, entitled, **“Crisis Management: Introduction to Plan Development with Guided Exercises,”** brought together twelve members of the CMBC Council who conducted educational sessions and group exercises on topics such as the Crisis Management Life Cycle, Performing a Risk Analysis, and the Business Impact Analysis. Additional sessions included crisis leadership, crisis communications, developing the written plan and recovery exercises.

There were 31 domestic and international attendees from various security and emergency management positions of responsibility. To drive home the seminar’s objectives, after each session the attendees were divided into smaller exercise groups to independently develop solutions to various emergency situations. Each team leader presented his team’s solutions, which were then discussed by the students and the instructors.

As stated in the seminar, the first step any stakeholder must take is to conduct a risk/vulnerability assessment, which should identify the probability of all potential emergencies and their impact on life safety, property and the business.

Performing this assessment is critical. The stakeholder should prepare a list of all possible or

potential crises, which may include fires, floods, explosions, telephone outages, workplace violence and terrorist activities.

A crisis management plan, including policies and procedures for an “incident response” must then be written, validated through exercises and issued to employees. The plan is a critical component of an organization’s preparedness strategy.

According to the seminar attendees, the four day event was a huge success. A favorite item was the behind-the-scenes tour of the TD Garden, the city’s major sports venue. The field trip took the learning experience of the classroom to another level, as James Mayall, Director of Public Safety for the Garden, discussed crowd control, building evacuation issues, shelter-in-place procedures and terrorist threats in public venues.



Looking ahead, the CMBC Council is pleased to announce that the seminar and workshop will be held in May 2012 in Chicago, IL. Watch for registration information on ASIS International’s Professional Development website at <https://www.asisonline.org/store/calendar.xml#07>.

Allan Schwartz, CPP, CHS-III is president and CEO of Safeguards International, Inc. As a 30-year veteran in the security industry, he has lectured extensively to various industry and trade groups across the country on a variety of security and risk management issues. He can be reached at safetrak3@aol.com

Enterprise Security Risk Management

Forming a 360° All-around Security Defense

Corporate Security and Enterprise Risk Management

Terrorism, geo-political conflicts, natural disasters, globalization, privacy & information protection, pandemics, increasing client and citizen expectations, and other global forces are reshaping corporate security, creating both challenges and opportunities for the Chief Security Officer (CSO).

Organizations must go beyond managing risks in silos and build an enterprise-wide risk function so that a full spectrum of risks is addressed wisely, systemically, and professionally.



As a business enabler, Corporate Security should be integrated into the overall risk management framework, resulting in deeper penetration into business risks. Why the change? Because the demand has grown for a more holistic approach to corporate security management.

For example, the convergence of IT security must be more closely aligned with physical security and other corporate security functions under the umbrella of Enterprise Risk Management (ERM). Such a convergence is especially necessary for the protection of an organization's brand and reputation as a result of improved risk intelligence sharing, collaborative decision making, and strategic risk focus and oversight from the top.

Former Deloitte Global CEO Bill Parrett provides new insights into this enterprise-wide risk function, corporate security, and risk management. In his book, "*The Sentinel CEO: Perspectives on Security, Risk, and Leadership in a Post-9/11 World* (2007)", Mr. Parrett gives his views that following 9/11, the security of physical assets and the response to major security events such as pandemics, terrorism, and cyber crime are top of

mind for business executives today. ERM has become an increasingly visible and important management solution, especially for the newer and more complex risks.

Mr. Parrett also recognizes the ascension of the CSO not only as a new senior level position on the corporate organizational chart, but as a key decision maker in the top management of many companies and an indispensable ally of the CEO.

The "FIBER-reinforced" Corporate Security Model

In light of the myriad of more challenging security threats faced by the CSO, a practical corporate security model is necessary for the protection of the five key assets – **Facilities, Information, Business, Employees, and Reputation**. The protection of these resources is bolstered by physical, personnel and information security mechanisms as well as crisis management and business continuity strategies.

Fiber is essentially the cell walls that provide the architecture or skeleton of a plant. It gives the plant the strength, support, and resilience against strong wind and harsh weather. One of its major purposes is also to provide a tough protective armor around the embryo of the future plant.

According to this "FIBER" model, security is a value-added service with an emphasis on combined security and safeguards for *proactive prevention* rather than reactive enforcement. All security programs are based upon threat & risk assessments and security recommendations tailored to individual and facility requirements. Security becomes everybody's business. The vigilance and involvement of every employee is needed under the leadership and guidance of a professional and competent security organization.

(Continued on page 5)

(Risk Management, continued from page 4)

The FIBER-reinforced corporate security model further emphasizes that for risk assessment purposes, the consequence analysis should estimate the potential impacts on all five primary assets. Recent high profile international crises and blunders continue to show that reputation risk can pose the greatest threat to an organization's stability and value, and result in drastic implications for the companies involved (i.e., the BP oil spill and Toyota recall). Obviously, reputation risk has not been fully integrated into their risk assessments.

Enterprise Security Risk Management

Enterprise security risk management (ESRM) exists to ensure that risks traditionally associated with security, but not always covered by ERM, are properly considered and treated. For ESRM to be successful, Corporate Security must collaborate seamlessly with other control functions such as Compliance and Internal Audit to enhance the organization's security posture.

In the course of implementation, Corporate Security should also build effective interfaces with other key support functions such as Human Resources, Communications, Legal, Information Technology, Safety, and Facilities Management. Not only does the CSO need to understand the security threats and risks to the organization and its people, but he or she should also take an active role in understanding the nature of business operations, environments, and events to analyze any potential reputational risk.

An organization should focus on the following baselines to maximize the value of security and at the same time proactively pursue total security risk mitigation:

- Physical Security
- Information Security
- Personnel Security
- Crisis Management
- Business Continuity

In addition, there should be a systematic approach to acquiring and analyzing the risk intelligence

necessary to support senior leaders of the organization both in the protection of assets and in the allocation of security resources.

A corporate security risk assessment methodology should be adopted to analyze threats and vulnerabilities, assess risks to the organization, and develop recommendations for enterprise-wide risk mitigation. Senior management should also engage with the CSO's security agenda to set their risk appetite in navigating the risk landscape.

Paul Yung is the National Corporate Security Leader with Deloitte, based in the Hong Kong office. He has over twenty years of senior management experience in the development, implementation and review of emergency response, crisis management, business continuity, physical security, personnel security, and the handling/oversight of corporate investigations. He can be reached at pyung@deloitte.com

References

- "The Sentinel CEO: Perspectives on Security, Risk, and Leadership in a Post-9/11 World", William Parrett, Wiley, 2007.
- "The Convergence of Physical and Information Security in the Context of Enterprise Risk Management", The Alliance for Enterprise Security Risk Management, 2007
- "Enterprise Security Risk Management: How Great Risks Lead to Great Deeds", ASIS, The CSO Roundtable, 2010



(Vehicle Armoring, continued from page 2)

Visits to each potential vendor's plant should be conducted. These visits are the most important step in selecting a vendor. No reputable armoring company will refuse a potential client the opportunity to carefully inspect the work being done at their plant, and full advantage should be taken of this fact. Vehicles in the armoring process should be carefully inspected. The optimum situation is to visit a plant in which multiple vehicles at different stages of completion are available to be inspected.

Some of the checks necessary on a vehicle in the armoring process include:

- Ensure that no gaps are left in the armoring at points where accelerator pedal, electrical cables and other items enter the passenger compartment.
- All welding must be seam welding; no spot welding is acceptable.
- Front, side and rear window posts must be covered with armoring material in such a manner as to leave no gaps between posts and window edges.
- All window glass must be installed replacing OEM glass; no hanging of ballistic glass panels inside the vehicle is acceptable.
- Window glass should be of a thickness appropriate to the armoring level (19-25mm for B4 and 36-45mm for B6).
- Points at which ceiling and side, or floor and side armoring meet must be seam welded or covered with additional protection.



- Rear cargo door armoring and side armoring must be installed inside the doors and panels, not strapped on the inside of the vehicle.
- If a prefabricated armoring kit is used, no trimming of edges or pieces is permissible (vehicle models have been standardized since Henry Ford).
- The roof should be completely armored, not just the first foot or so above the driver's head.
- Door hinges and hydraulic closures should be reinforced to support the additional weight of armoring.
- Radios and other additional equipment should be installed as part of the armoring process, not retrofitted afterwards.
- Offsets behind door handles and locks must cover sufficient area to deflect oblique impacts.
- Glass should not be accepted that distorts driver or passenger vision or is much thicker than commonly accepted norms.
- Opaque armoring material should be either ballistic steel or fiber-based, no stainless or common steel.
- No riveting should be permitted except on floor protection, and then only in zones where IEDs are not a threat.
- Battery and radiator protection must be installed to prevent overheating or interference with mechanical functions.
- If used, run-flat devices should be installed in all tires including the spare, although new tire

(Continued on page 7)

(Vehicle Armoring, continued from page 6)

technologies are diminishing the requirement for separate run-flat devices.

- Weapons firing ports should be prohibited, particularly in the driver position.
- Finish work must be perfect; all leather or fabric should appear to be original and no damages noted.
- Vehicle paint job must be seamless and equal to original factory work.
- All systems (i.e., air conditioning, heating, radio, turn signals, etc.) and gauges must be tested and repaired or replaced as necessary before vehicle is accepted.
- Doors, cargo hatches and windows should close smoothly, completely and seamlessly. No sagging, grinding, scratching or misalignment is acceptable.

Once a vendor has been chosen and armoring has begun, vehicles should be regularly inspected and photographed throughout the entire process. At each step (disassembly, armoring, reassembly), carefully check the quality of the work. When work on the vehicle is finished, a test drive should be taken to ensure that everything functions correctly and there are no problems.

After the vehicle is received by the customer, warranty services provided by the armorer must be performed regularly. Additionally, since armoring a vehicle normally voids a factory warranty, arrangements must be made to ensure that maintenance is available and that technicians are capable of performing such work.

The process of armoring a vehicle can be complex, involved and time consuming. With the information provided here, however, that process will be easier for the security professional. Because in the end, providing a well-made vehicle to a client truly is a life saving act.

Richard Wright, CPP, manages all aspects of security for twenty-six Country Offices in Latin America and the Caribbean for one of the largest multilateral lending institutions in the Western Hemisphere. He can be reached at wrightsecurity@gmail.com

Council News



The Crisis Management and Business Continuity Council is developing a new organizational structure to align all of its activities with the mission and goals of the Council.

This new structure will allow us to focus our efforts on the continual improvement of our annual Crisis Management Workshop, the development of various publications, liaison interaction with other organizations, the development of Professional Standards, and various Council planning documents.

The Council takes its responsibility as the crisis management and business continuity Subject Matter Experts for ASIS International seriously, and we will continue to provide solid advice and assistance to our colleagues on matters involving organizational resilience, crisis management, emergency preparedness and business continuity.

The Crisis Management & Business Continuity Council newsletter was produced by council member David Spector. Contact him at (781) 981-2402 or dspector@LL.mit.edu