



“Double Down”

Gaming & Wagering Protection Council

July 2011

GWPC Council Members

Chairman

Derk J. Boss, CPP

Vice-Chairman

Anthony V. DiSalvatore,
CPP, PCI, PSP

Newsletter Editor

Jerry Higginson, PCI, CPP

COMMITTEES

Annual Seminar

Alan W. Zajic, CPP

Articles to Security

Management Magazine

Robert A. Prady

Jeff C. Graber

Book Reviews

Charles H. Barry

John Chuvala, CPP

William A. Vicaldo, Jr.

Council Certification

Liaison

John Chuvala, CPP

Guidelines Committee

Tommy J. Burns, CPP

Robert E. Nichols

Program/Workshop

Alan W. Zajic, CPP

Session Reviewer

Chairman's Corner

Greetings All!

I want to catch everyone up with what we've been doing the last few months. I'll start with our webinar on **“Proactive Surveillance Operations”** that Anthony, Farzad and I presented on May 18th. Bob Nichols also assisted. We think it went very well and were told by ASIS headquarters that over one hundred twenty-five people attended. It was very easy to do and ASIS provided an excellent format.

Our next **webinar** is on August 10th and is titled **“Protecting Day Pools and Nightclubs”**. Our presenters are Anthony, Al Zajic and I. We expect a big turnout.

Please let Anthony or myself know if you'd like to be involved in our webinars next year. This is an excellent way for our Council to assist other in our industry!

G2E is coming! We are only a few months away from our premier event of the year. I will be attending and I would like to see a strong Council presence. We have many roles that need to be filled from greeters to speaker introductions. Please contact Al or myself to sign up.

We are still striving to get our webpage established on the Department of Homeland Security's website. Some of us have logons but we need more participation. We are also looking for someone to put it all together. If you can do that, contact me ASAP. I can put you right to work.

Derk

Vice-Chairman

Greetings everyone!

We have had great ideas from our council pertaining to ideas for webinars, articles and projects - with everyone's support the first webinar was a great success and we look forward to achieving more recognition for our council with other webinars in 2011.

We are continuing to coordinate and develop the web project with DHS.

Thanking everyone for their support and ongoing efforts in these and other areas that reflect positively and achieve recognition for our council. Please forward ideas for articles, projects and webinars for 2012.

Anthony



SECURITY Q & A: Crowd Control Quiz Part #1 **by Stephen Van Zweiten**

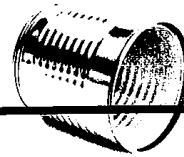
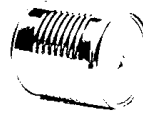
Attached to this newsletter is an article by GWPC Member Stephen Van Zweiten



SECURITY Q&A

Crowd Control Quiz Part 1

By Stephen Van Zweiten



When it comes to security roles and duties, very few are as high risk and as misunderstood by most as crowd control. A highly trained, knowledgeable and competent crowd controller is a valued asset to a business. Some organisations engage security crowd control companies and quite often the person responsible for managing the tendering/engagement process does not fully understand the necessary competencies and skill sets that are required for professional crowd controllers, and the impact they have on their brand and business success. The following questions are designed to test your knowledge and understanding of a number of important aspects of crowd control issues.

1. What is conflict?

- A. A physical confrontation.
- B. A trial of strength between opposed parties and principles.
- C. When both parties raise their voice.
- D. A display of anger and aggression.

2. Frustration if unresolved can often lead to:

- A. Anger.
- B. Irrational behaviour.
- C. Violence.
- D. All of the above.

3. The aim of a crowd controller when dealing with conflict is to:

- A. Enforce the rules no matter what the other party's opinion is.
- B. Gather the information and pass it onto the Manager on duty.
- C. De-escalate the situation and maintain or regain control of the situation.
- D. To do whatever makes the other party happy/content.

4. When crowd controllers use force to maintain control their level of force must be...

- A. Effective enough to gain control of the situation.
- B. Minimal (using a one-plus-one theory).
- C. Necessary force to prevent injury to self/others.
- D. Reasonable.

5. If a crowd controller is threatened with violence which of the following should they do first?

- A. Do nothing until attacked.
- B. Defend themselves.
- C. Assess the threat level.
- D. Negotiate their way out of the threat.

6. What are four things a crowd controller must keep in mind regarding self-defence?

- A. Lawful, reasonable, justifiable, proportionate.
- B. Reasonable, justifiable, proportionate, truthfulness.
- C. Justifiable, lawful, skilful, truthfulness.
- D. Proportionate, reasonable, appearance, gender.

7. How much force is acceptable for a crowd controller to use?

- A. As much force as possible to ensure the situation is controlled quickly.
- B. The minimum force necessary to regain/maintain control taking into account the totality of the circumstances.
- C. Minimal force must be used at all times.
- D. The level of force that the client has stated should be utilised in handling a situation.

8. Which of the following is not a standard consideration that affects a crowd controller's use of force?

- A. Relative size, stature and strength of the other party.
- B. Distance from subject.
- C. Injury, exhaustion and fitness level of the crowd controller.
- D. The estimated response time for police arrival and assistance.

9. When negotiating during a conflict situation the most important key attitude a crowd controller needs to possess is:

- A. Empathy for person/persons involved.
- B. Security must always be seen to be right.
- C. An attitude of fairness towards all parties involved in conflict.
- D. I have a job to do and this is not personal.

10. What are some of the reasons people become violent?

- A. Emotional or physical problems.
- B. Illness or injury.

- C. Anger or frustration.
- D. Stress.
- E. Substance abuse (including alcohol).
- F. All of the above.

1. Answer: B According to the Oxford Dictionary, conflict is a trial of strength between opposed parties and principles.
2. Answer: D When a person becomes frustrated their behaviour can change quickly if crowd controllers are not highly skilled, the situation can (and in most cases, does) get out of hand. This has direct and indirect costs to the business.

3. Answer: C The aim with all confrontational management is to maintain and regain control of any situation. Try to de-escalate the situation and negotiate a win-win outcome if possible.

4. Answer: D Almost all jurisdiction throughout the world use the term "reasonable force" to assess the actions of an individual. This takes into account a variety of factors.

5. Answer: C When threatened with violence, a crowd controller must assess the threat level. A risk-based approach is required. A crowd controller does not have to wait to be hit first, before they are allowed to defend themselves.

6. Answer: A If a security crowd controller acts within the law, uses reasonable force, can justify their action given the circumstances and demonstrate parity/disparity with other persons involved, they will have nothing to fear.

7. Answer: B Force can be used for a variety of reasons, such as defending others, defending property, self-defence and effecting an arrest. In all circumstances, objective reason and taking into account the totality of the circumstances.

8. Answer: D A, B and C are all aspects that need to be considered at the time a crowd controller wishes to use force.

9. Answer: A Empathy (to put yourself in someone else's shoes) is arguably the greatest attribute a crowd controller can possess.

10. Answer: F All of the above are factors and reasons why people can become violent. A competent and knowledgeable crowd controller can identify a change in behaviour with persons known to them and effectively deal with the issues at hand.

Stephen Van Zweiten is managing director of Exact Security.

By Stephen van Zwieten

Asset protection is a higher priority for business today than at any time since World War II. Never before have there been so many private companies offering security services and today the security industry is a major employer in every developed country. The 9/11 terrorist attacks in the USA was the catalyst for exponential growth in an industry that had already been growing rapidly for many years. The evolution of security has been dramatic in terms of the essential integration of the latest technology and highly trained people.

This article explores an aspect of security which is largely ignored: the holistic approach to security. This approach calls for security planning to take into account the needs of the entire business. Customer relations and sales opportunities are every bit as important as asset protection under holistic principles. A more holistic view of security promises the next evolutionary stage of security: becoming a valuable contributor to business profit centres.

The recent global financial crisis, natural disasters, worldwide economic difficulties and plummeting profits in many business sectors have contributed to much greater analysis of costs and benefits relating to security. In a perfect world the costs of security could completely disappear, but now that security is an essential part of most businesses it is time to look at the cost from a different angle.

Security professionals today face the growing challenges of rapid environmental change, accelerating technological solutions, demands for higher and higher standards and more professional security strategies. Adding to the challenge is the need to recognise that security is a global concern and it is no longer sufficient to rely only on local, state or even national security knowledge.

The Holistic Approach

The holistic approach requires the security professional to take a much broader view and to think more about the client's return on investment needs. There are tangible and intangible benefits to consider in the return on investment formula and the security professional needs to have an in depth knowledge of all of them. It is that sort of knowledge that allows security to focus

on what is important to the client's bottom line and offer continuous improvement and flexibility.

The holistic approach requires a profound understanding of the client's business – how it operates, what outcomes it is striving to achieve, and what strategic plan is being followed. Gaining this sort of knowledge is time consuming and costly for the security provider and can seem difficult to justify. However, the potential gains in most cases would easily outweigh the extra time and effort.

Armed with such a depth of understanding of the business, security can work on its own strategies. These must include all the ways in which it can positively influence revenue and other costs. Asset protection is important but is largely about prevention and goes into full operation only when needed. In contrast, the overall strategy should be proactive and in operation at all times. These strategies require security to identify where it can assist all departments and teams to achieve their business outcomes.

Many businesses have more than one firm providing security services. This occurs for many different reasons. The most common reason is the belief that the business is spreading its security risk. While there might be an element of truth here, it is more likely that they are simply increasing their company's security costs, creating different and confusing standards of service, and setting up operations in silo fashion.

But most importantly, they are eliminating the opportunity of having a security provider playing an active role in their business plan – seeking opportunities to enhance sales, improve customer relations and company image, build important relationships and other issues important to business planning. There are many relationships that can be enhanced by security – police, other regulatory authorities, local government, neighbours and the local community are examples.

The holistic security provider knows the client's business sufficiently to see opportunities unique to that business. Sometimes a suggested change might even be against the interests of the security provider, but that is not the point. The holistic approach demands priority in achieving the business plans of the client. In one case a client was advised that a change in operations would result in a reduction in security costs of nearly

\$4,000 per week – not so good for the security company's short-term profit, but appropriate in the spirit of this approach.

One very good example of this holistic approach came from Penrith Panthers Licensed Club. In 2005, the security team analysed the club's mix of business and costs. The club was achieving record bar sales and record attendances every Friday and Saturday night at its three night clubs. The entertainment and bar managers were happy but the gaming manager was not so happy. Setting new records for bars and entertainment departments had a negative impact on gaming revenue: security costs were climbing to cope with the higher risk, younger demographic replacing the lower risk, older demographic.

The traditional responsibilities of security were being handled to a standard that brought the team recognition by regulators and their peers as being the benchmark within the industry. Many of the senior managers at Panthers were comfortable with the mix of business and resisted change. Security could have easily looked after its own interests by continuing to provide the large team to satisfy the needs of the club.

Regardless of the potential loss of security hours and security wages of \$1.2 million, security put together a business plan and presented it to senior management. The plan involved closing the nightclubs. The loss of revenue from bars (\$8.6 million per annum) and entertainment would be more than offset by huge savings in security, advertising and marketing, and by increases in gaming revenue.

The plan was adopted and the immediate impact on the business confirmed the plan's predictions but there were even greater benefits that were more difficult to quantify. There was a dramatic reduction in crime, anti-social behaviour and vandalism. Slowly but surely, the lower risk clientele started to return to the club, resulting in an increase in gaming and catering revenues. Over a period of two years, this change resulted in the club achieving a substantial increase in profits.

Another good example came from the efforts of Panthers' sales staff to bid for an important and prestigious event. By involving security in meetings of the sales teams, a shared understanding of the problems was achieved. This allowed security to suggest how it could add value to proposals and enhance the sales team's effort: potential function clients could be



offered special services that would satisfy their unique needs.

The Corvette Club called for bids for its national event. It was well known that the Corvette Club executive had a strong preference to hold the function in the ACT. Panthers Club function staff were almost resigned to the fact that they would not get this sale. However, sharing the problems with security paid off. Security was able to offer a number of suggestions to make the Panthers Club bid more attractive and that made the difference.

The event was held over the Easter weekend, which was traditionally a quiet time for the club. The Corvette Club booked one hundred rooms over four nights, equating to four hundred room nights. Hundreds of additional customers in function rooms, restaurants, bars and gaming areas increased revenue by hundreds of thousands of dollars.

Both of these cases point to the high value of moving security from the list of necessary costs to the list of operations that contribute directly to profitability.

The security profession and security professionals need to adopt an enterprise-wide risk approach in the business. It is important to identify silos, gaps and duplications that may exist in the business. Technology changes at a rapid pace, so it is very important to future-proof the security system. If the security provider and the supplier of technology are the same company, the holistic approach can be further enhanced. Some businesses have different security providers for crowd control, electronic security, security consultancy, patrols and alarm responses, and security training.

There are a number of benefits of using one provider; a better balance between cost and quality is just one of them. The opportunity to take on a more holistic approach is another. Liaising with one client manager who can see the holistic view of security can lead to more cost effective security strategies to mitigate risk.

A clear understanding of the business in which they operate, allows security professionals to achieve a holistic approach to security, providing the appropriate level of asset protection for the

business and much, much more.

However, the holistic approach has to be a shared ideal. It can be recommended and promoted by the security provider, but cannot be implemented without the goodwill of the client. The greater the cooperation between security and client, the greater will be the benefits. A partnership relationship between security and client is the ideal way to maximise benefits, opportunities and client profit. ■

Stephen Van Zwieten CCP is an operational expert with over 30 years of experience in security and surveillance strategy and management. Currently Vice President and Board member of SPAAL (Security Providers of Australia Associated Limited), Steve has also served as the founding Chairman of the Australasian Security and Gaming Council from 1996-2004 in addition to serving as the Senior Regional Vice President of ASIS International for Australasia 2002-2009 and Chairman of the NSW Chapter. Steve is currently the Managing Director of Exact Security.



1625 Prince Street
Alexandria, VA 22314-2818
USA
703-518-1447
Fax: 703-518-1517
Email: councils@asisonline.org