The Bill Blackwood
Law Enforcement Management Institute of Texas

==========

Selling Security

==========

An Administrative Research Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

==========

By
Keif A. Dahlman

UT Southwestern Medical Center Police Department
Dallas, Texas
January 2005

ABSTRACT

One of the duties commonly undertaken by law enforcement and security professionals is that of making recommendations as to how to improve security. Such recommendations may be intended for individuals, businesses, college campuses, or even an entire neighborhood community. Regardless of the scope, however, such recommendations often face a common obstacle; getting the recipient(s) to actually implement the recommended security measures.

This research paper will identify various strategies that law enforcement and security professionals can use to encourage or facilitate implementation of their security recommendations, and analyze the relative value and importance of these strategies in achieving this goal. Although certain types of obstacles and strategies are anticipated depending upon the type of person or organization receiving the advice, it is the author's belief that it will be necessary to discover what is most important to the specific recipient before being able to accurately determine the most effective strategy. In addition to a review of existing materials on this topic, the author created and disseminated a survey questionnaire to obtain feedback from a number of respondents regarding what factors are most important to them when it comes to purchasing and/or implementing recommended security measures.

The ultimate purpose of this research paper is to provide law enforcement and security professionals with additional insight into what truly motivates the recipients of their advice, in order to aid them in putting their recommendations in terms that are meaningful to those recipients.

TABLE OF CONTENTS

Page

Abstract

Introduction. 1

Review of Literature 3

Methodology 8

Findings 10

Discussions/Conclusions 12

References 16

Appendix A 17

INTRODUCTION

It is the belief of this author that the single greatest obstacle faced by law enforcement and security professionals who make security recommendations is simply convincing people to put the recommendations into action. The old saying, “You can lead a horse to water, but you can’t make it drink,” is analogous to this situation. Good, solid recommendations made by knowledgeable and experienced law enforcement and security professionals are often eagerly accepted, but much less seldom acted upon. The person(s) in question may be a city council member, a university administrator, a small business owner, or a resident of an apartment complex. The scope of the recommendations may vary dramatically, and may range from something as large as the purchase of a new $500,000 security system for a casino to something as small as making a change in a daily routine. The problem, however, remains the same; the person must be convinced to actually make the change.

It is the author’s purpose to discover exactly what it takes to overcome “mental inertia,” and to motivate a person to implement a security recommendation; this is the central question that the author will attempt to answer in this research paper. The answer expected by the author is that it will be necessary to find out how the person thinks, and what is most important to them. Often the obstacle may boil down to the universal bottom line - money - but this may not always be the case. Some recommendations, particularly those involving simple changes in organizational procedures or personal habits, may involve very little or even no money. In these cases, simple inertia or laziness may be the primary obstacle to change. Time itself may be yet another obstacle. Regardless of the obstacle, however, it is anticipated that

the only way to really convince somebody to make a change is by helping them to see how it benefits them according to their personal perspective of what is important. For a university administrator, it may be a reduction in liability. For a large business owner, it may be improving the financial bottom line by reducing pilferage or theft of trade secrets. For a small business owner, it may be keeping valued patrons feeling safe while on the premises. For a nurse working the night shift, it may be her personal safety while walking through a parking lot.

In addition to reviewing several books and articles on the topic, the author will create a brief survey that will ask questions about what motivates (or fails to motivate) the respondent when deciding whether to spend money or implement changes related to improving security. The targeted audience will optimally include a randomized sampling of people such as homeowners, small and large business owners, university administrators, and city council members. The questions will be designed to discover why the respondent did or did not choose to implement additional security in their home, for their business/campus, or in their city.

It is the intent of the author to help law enforcement and security professionals by gaining additional insight into the decision-making process people use when deciding whether to implement recommended security measures. Hopefully this research will help such professionals to better understand what truly motivates the recipient of their advice, and to put their recommendations in terms that are most meaningful to the person. When people are shown how implementing security recommendations can help them to achieve that which is most important to them, it should greatly increase the chance that they will actually spend the time, money, or effort to implement the

recommendations. The more security measures there are in place, whether in public areas or on private property, the more security there will be for people and property everywhere.

REVIEW OF LITERATURE

A good amount of literature exists on this topic, but there is not a complete consensus as to there being a single best method for persuading people to invest in security. There is a trend among many recent sources to stress the importance of showing how improved security can help organizations by actually becoming a profit center, rather than merely a necessary expenditure that winds up acting as a financial anchor. For instance, Hearnden and Moore (1999) assert that "The straightforward answer to our question 'Why bother with security?' is 'Because it can help you to improve the bottom line'" (p. 1). They go on to further this concept by explaining that "The successful use of security techniques and technology will usually result in the reduction of business or operational losses, which in turn will convert into an improvement of the final profit or a more effective use of scarce resources" (Hearnden & Moore, 1999, p. 11). In the same work, however, there is also support for the assertion that the best way to sell security is to find out what is most important to the person receiving the recommendations, and to tailor the recommendations to suit the client's needs. "One effective approach is to ask the relevant manager or director to identify what event or events would most seriously jeopardize the achievement of business objectives, for the answers will identify the key risks the organisation (sic) faces" (Hearnden & Moore, 1999, p. 14). It bears mentioning that these two assertions are not

mutually exclusive; in the case of many if not most businesses, the bottom line (making a profit) actually is the thing that is most important. For other types of organizations (i.e. not-for-profits, universities, etc.) or for homeowners, however, this is much less likely to be the case.

In an article in the July 2002 issue of Security Technology & Design magazine, Jim Spencer emphasizes the importance of focusing on providing valuable service and return on cost, instead of on cutting costs, when trying to sell a security program. He states, “Align every cost with the value it produces for your customer…Eliminate costs that produce little value and concentrate your resources on more productive costs” (Spencer, 2002, p. 73). In the same article, he also mentions the need to find out what your client wants; “Find out what your customers value, put a multi-year program together and show them how you will exceed their expectations” (Spencer, 2002, p. 74). Fischer and Janoski (2000) approach the cost-benefit angle from the perspective of creating value by preventing loss that could otherwise occur. “It is sometimes a surprise to security and upper management alike when the criticality of the loss is double or even triple the cost of the item…Management needs to be constantly reminded that protective (preventive) expenses are significantly less than reactive costs incurred after a serious incident occurs” (Fischer & Janoski, 2000, p. 17). Persson and Chandler (1989) discuss four distinct methods for using financial justification to justify security expenditures; simple payback, which is basically the amount of immediate savings over a year; cost-benefit ratio, which displays the ratio of costs to benefits (must be less than 1.0 to be favorable); present worth, which takes into consideration time-sensitive factors such as equipment life and investment potential; and rate of return, which is calculated

in a manner similar to present worth but is expressed in terms of an interest rate, similar to most financial investments (Persson & Chandler, 2000, pp. 3-6). They also talk about the importance of speaking to management in terms they will understand when selling security to them. "You will be most successful if you present your project's financial information using the language and techniques of the financial community. The advantages of doing your project may not be intuitively obvious to someone outside of your work area" (Persson & Chandler, 2000, p. 7).

More support for the idea of presenting security as a profit center can be found in an article by Wayne Siatt in the December 1981 issue of Security World: "Although security as a loss prevention function may still be nebulous to some financial planners, they will respond favorably to most requests if the budget dollars can be shown to have a direct affect on losses" (p. 23). He also specifically mentions the way security can add value by reducing liability and insurance premiums. "The biggest contribution a security department can make is in terms of reducing insurance premiums" (Siatt, 1981, p. 26). Plenty of literature cites the necessity for getting management to start thinking about security as a value-added expense, rather than simply an expense. It is also critical for those selling security to adapt by looking for new ways in which to provide service. "Security has to market (self-promote) itself to 'sell' the value of security and life-safety initiatives. Taking on new duties and responsibilities adds to this value and should be encouraged and sought out" (Fischer & Janoski, 2000, p. 266).

Not all the literature focuses only on selling security as a profit center or a source of savings. It is also important to develop skills in diplomacy and communication, since the ability to establish a good relationship with management can make all the difference

when trying to sell security. "The security manager must have the support of the CEO. The security manager must also be able to communicate down the line with employees, the public, customers, vendors, contractors, and the media" (Fischer & Janoski, 2000, p. 160). Communication skills are often necessary to help managers to better understand not only security proposals, but also the basic security requirements that are appropriate for their situation. According to James Broder (2000), "Most plant managers with whom we have worked do not have the foggiest idea what kind of security they need for adequate protection" (p. 45). In order for any security effort to succeed, it is vital to involve and educate others, both within and outside of one's organization, about the role they play in achieving security. Without this, even the best security proposals will be doomed to failure.

Another valuable tool that is useful for garnering support for a proposed security measure is a security survey or risk assessment. The basic aims of a risk assessment should include 1) a determination of the types of risk involved that can affect the people or resources to be protected; 2) the probability of occurrence for each type of risk identified, and 3) quantifying and prioritizing the loss potential for each of the risks (Broder, 2000, pp. 4-5).

One way to make a security proposal more palatable "is to prepare your security plan in stages or increments" (Broder, 2000, p. 39). This can provide the minimal level of security needed right away, without creating an immediate and unnecessarily high cost for more expensive security measures that can be implemented over time. Broder (2000) goes on to list the following eight methods for selling security: 1) Establish a meaningful dialogue with management, and try to gauge their attitude towards security;

2) Deal in principles, not personalities, when gathering information to support your position; 3) Be as professional as possible when it comes to security; 4) Just hit the highlights of the proposal, and keep it concise; 5) Know your limitations, and get outside help iwhen you need it; 6) Encourage management to hire a professional security consultant from outside to get a second opinion; 7) Have your plan ready so you can take advantage of timing when the circumstance arrives; and 8) Develop a public relations program to help sell security throughout the organization (Broder, 2000, pp. 48-49).

Sennewald (1985) makes a similar list specifically intended for those trying to sell security from within an organization. He encourages using new employee orientations as opportunities to sell security, stating that “Not only is there a “captive” audience, but an audience eagerly receptive to information about their new work environment” (p. 242). This advice is intended to apply not only to line employees, but also to incoming middle management. In fact, he says it is even more important to deliver the message to these employees, so that they “are partially convinced of the importance of security when they arrive…There is no question in their minds when they leave the (presentation) that the security function is in the mainstream of the business and has its place in the sun” (Sennewald, 1985, p. 245). He also mentions security tours for employees and managers of all levels, and advertising by means of bulletins, newsletters, or the like (Sennewald, 2000, p. 245). He includes meetings with the various sections or departments and other types of involvement programs to bring employees into personal contact with security “to cement good relationships” (Sennewald, 2000, p. 247). This tends to create personal involvement and interest in

security on the part of employees, which can help to spread support for security throughout the organization.

METHODOLOGY

The purpose of this paper is identify the best methods for overcoming “mental inertia,” and to motivate a person to implement a security recommendation for his/her home, business, campus, or other area of responsibility. The primary method of inquiry used will be a 1-page survey questionnaire, to be disseminated primarily by e-mail (as an MS Word document) but also as a hardcopy in order to reach potential respondents who do not have e-mail. The questionnaire consists of 15 questions about various factors that could impact a decision as to whether or not to purchase and/or implement security measures. The respondents are prompted to rate each factor on a scale from 1 to 5, with 1 meaning the factor in question has no bearing at all on their decision, and 5 meaning the particular factor figures a great deal into their decision. By analyzing the respondents’ replies and calculating an average number for each question, it will be possible to determine which factors matter the most when they are deciding whether to purchase or install security measures. Generally speaking, the findings expected by the author are that there will not be a single best method, and that it will vary from person to person or organization to organization. However, the author expects that the highest ratings will be found for the questions dealing with the following concerns: the cost of implementing recommendations; a history of criminal activity at or near the location; reducing liability concerns; and having a cost-benefit analysis (the latter two primarily for businesses rather than residences).

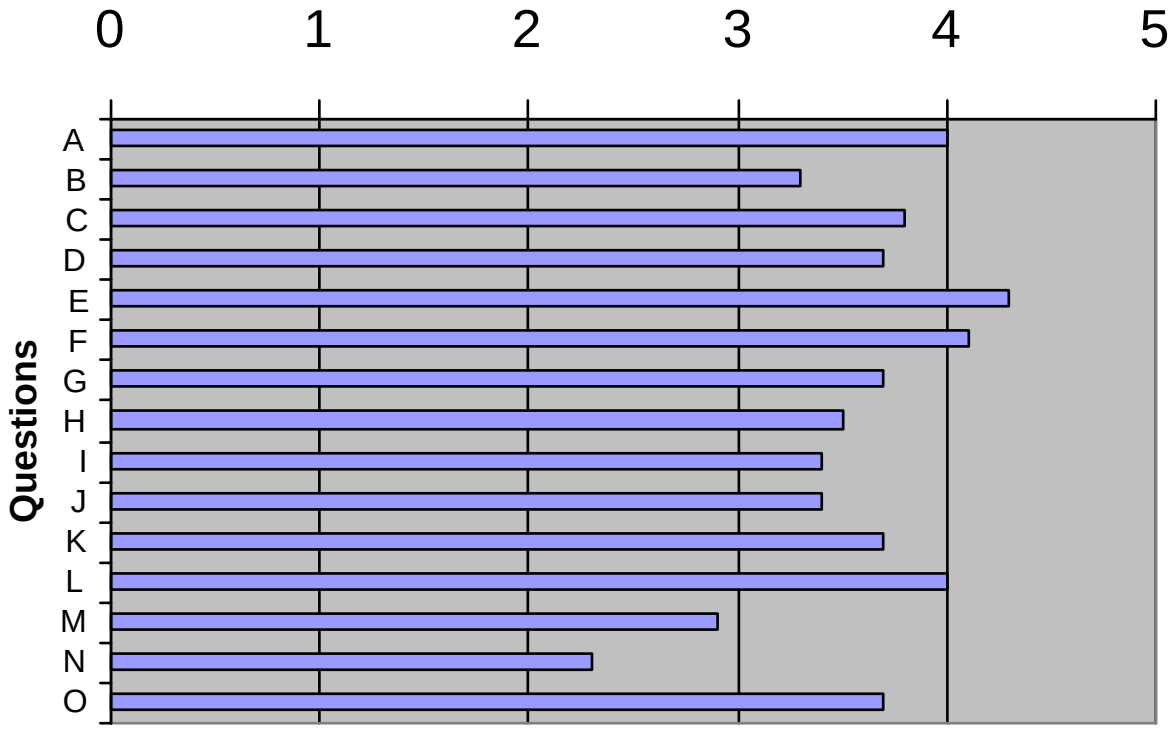
Several methods were used to find target populations for the survey, and the goal was to obtain responses from a combination of business owners, homeowners, and university campus administrators. The author sent the survey to the administrators at the university where he is employed, but to date no completed surveys have been returned from this source. The author made numerous attempts by both telephone and e-mail to contact the Stemmons Corridor Business Association (SCBA), which is a not-for-profit organization composed of numerous businesses in the portion of Dallas known as the Stemmons Corridor (which includes the author's workplace) for assistance, but unfortunately there was no response from the organization. The author contacted the Texas Municipal League (TML), but they were unable to assist with this survey. Through the American Society for Industrial Security the author was able to contact an executive with Wells Fargo, who had his staff complete and return four surveys. The author's father, a CPA, sent the survey to three of his clients, from whom two surveys were completed and returned. The survey was also sent out to all the members (approximately twelve homeowners and business owners) of the Oak Hollow/Sheffield Village Neighborhood Association, which is the local neighborhood association where the author resides. Of these, three surveys were completed and returned. The survey was sent to several other individuals, work associates and acquaintances, with negative results. Finally, the author disseminated the survey to all of the other sixteen students in the October 2005 LEMIT Module II, and fifteen of these were completed and returned. Due to the relatively small total number of returned surveys (twenty-four), the author intends to continue the effort to obtain more responses after Module II, to increase the validity of the findings.

FINDINGS

After receiving all of the completed surveys that were returned by respondents, the author was able to calculate which factors were rated as most important when deciding whether to purchase or implement security measures. These findings are reflected in Figure 1, and the complete survey questions are included as an appendix.

According to the survey results, the single factor with the highest impact on people's decision-making process was Question E, which received a 4.3 on the 5-point scale. This item referred to the apparent knowledge and/or credibility of the person making the security recommendations. The second highest rating of 4.1 was given for

Figure 1 - Survey Response Averages



Question F, which asked the respondents about the importance of reducing liability concerns. Questions A and L tied for the third highest rating, with both receiving a 4.0. Question A asked about the importance of the cost of security equipment and installation, and Question L attempted to gauge the importance of the history of crimes actually having occurred at the respondent's business or home. Question C was rated as the fifth most important reason, receiving a rating of 3.8. This question dealt with the importance of receiving information about how other businesses or homes in the vicinity have been impacted by particular types of crimes. Four categories - Questions D, G, K and O – all received a rating of 3.7, which was just above the mean rating of 3.6. Question D was similar to Question C, but it specifically targeted the effect of learning about examples of similar security measures being implemented at other businesses or homes that are similar to that of the respondent. The purpose of Question G, which was targeted primarily at business owners or university administrators, was to determine the importance of receiving a cost-benefit analysis showing the expected benefits of making the recommended changes, versus the potential losses of failing to implement the security measures. Question K, which was related to Questions C and L, was designed to measure the perceived importance of knowing the general crime statistics in the surrounding vicinity. Question O, like Question G, was targeted primarily for business owners or university administrators, and it asked about the importance of the positive effect on public relations and perceptions of employees and/or customers by being seen as proactively addressing the issue of crime.

Responses to Question H came in slightly below the mean at 3.5. Question H assessed the importance of having a written security survey or risk assessment detailing existing security strengths and weaknesses, and making specific recommendations. Questions I and J came in only slightly lower, both receiving ratings of 3.4. Question I addressed the use of photographs to illustrate security weaknesses, and Question J was closely related to Question H, but it focused on a particular aspect of the written security survey, namely the use of multiple levels of security recommendations to provide options (i.e. maximum, intermediate, and minimum). Question B, which received a rating of 3.3, referred to the level of difficulty involved in implementing changes in procedures to increase security.

At the lowest end of the spectrum, the survey indicated two factors that were rated the least important by the surveyed respondents. Question M received a rating of 2.9, and it asked the respondent about the effect of media attention to terrorism and other criminal activity. Question N came in at the very bottom of the list, with a rating of only 2.3. As with some of the others, this question was intended primarily for business owners and university administrators, and it was designed to gauge the concern that added security will create the perception that the business or organization is a high risk or dangerous location.

CONCLUSIONS

Since the author believes that the single greatest obstacle faced by law enforcement and security professionals who make security recommendations is that of convincing people to put the recommendations into action, the purpose of this research

paper is to determine the most effective methods for motivating a person to implement such recommendations when they are made for his or her home, business, or other area of responsibility. Although the author's hypothesis is generally that there will be no single best method, and that the best method will vary from person to person and from one organization to the next, he does propose that the highest ratings will be accorded to the following factors: the cost of implementing recommendations; a history of criminal activity at or near the location; reducing liability concerns; and having a cost-benefit analysis (the latter two factors primarily for businesses rather than residences).

When tested against the data collected from the survey, the author's hypothesis proved quite accurate overall, with one noteworthy and interesting exception. The hypothesis fared well in that three of the four factors estimated to be most important were rated among the top four rated questions from the survey results, and the fourth was still rated in the top half of the questions, above the mean rating of 3.6. The factor of reducing liability concerns (Question F) was rated as the second highest at 4.1, and the factors pertaining to cost and to crime history at the respondent's location (Questions A and L, respectively), were both rated at 4.0, making them tied as the third highest rated factors. The question asking about the value of a cost-benefit analysis (Question G) was rated at 3.7, still coming in above the mean. The most surprising data, and the one result which was totally unanticipated by the author, was that the most weight of all was given to the factor of the apparent knowledge and/or credibility of the person making the security recommendations.

There are two noteworthy limitations on this study that are deserving of mention. One limitation is that the total number of returned surveys (24) is relatively low, and a

much larger number would help to better confirm the validity of the findings. A second consideration is that the people who were surveyed were probably not perfectly representative of the entire target population, since only six respondents were known to be responding as business owners or on behalf of a business, three respondents were known to be responding as homeowners, and the other fifteen were all police officers from the LEMIT class. The officers in this group were presumably responding from the perspective of a homeowner, though some may actually have owned or operated businesses and therefore been able to respond from that perspective; this factor was not measured in the survey. It is also possible that their profession had an influence upon their responses, though the author noted that there was a large degree of variance in the responses by this group, which seems to contradict this notion.

Admittedly, the survey instrument may have addressed too broad a field by attempting to simultaneously target homeowners, business owners, and university administrators or other organizational leaders. As noted previously, some of the questions were not really applicable to homes, and were intended primarily for businesses or other organizations. For the purpose of any future research along this line, the author would recommend obtaining separate survey samples from each of these categories, though this would necessitate some redesign of the survey in order to suit each category. The survey would need to be altered by either deleting the questions that do not apply, or by altering the wording of those questions enough to make them appropriate for each category without significantly altering the basic meaning of the question. It may be desirable to create new questions specifically tailored towards the homeowners, though this would negatively impact the ability to

draw direct comparisons between the surveys from the other categories. Nevertheless, the homeowner survey could be treated as a separate research category unto itself, and would therefore still have value in its own right.

It is the author's hope that this study will prove useful to other law enforcement or security professionals who as part of their job make security recommendations to any individuals or organizations. When considering how to best utilize their time or how best to present data when making such recommendations, this research is intended to help give an indication as to what format to use or which factors would be best to include when presenting recommendations, as well as which factors may not be as effective. This study's findings also indicate that it is clearly important to be viewed as a knowledgeable and credible professional when it comes to having one's security recommendations taken seriously, so law enforcement and security professionals are urged by the author to never underestimate the extent to which this perception influences the outcome of their recommendations.

REFERENCES

Broder, J. (2000). *Risk Analysis and the Security Survey* (2nd ed.). Burlington, Massachusetts: Butterworth-Heinemann.

Fischer, R. J., & Janoski, R. (2000). *Loss Prevention and Security Procedures: Practical Applications for Contemporary Problems.* Boston, Massachusetts: Butterworth-Heinemann.

Hearnden, K., & Moore, A. (1999). *The Handbook of Business Security: A Practical Guide to Managing the Security Risk* (2nd ed.). Dover, NH: Kogan Page Limited.

Persson, E. A., & Chandler, L. L. (1989, May). Getting Your Bucks in a Row. *Security Management, 33* (5), 40-47.

Sennewald, C. (1985). *Effective Security Management* (2nd ed.). Boston, Massachusetts: Butterworth-Heinemann.

Siatt, W. (1981, December). Blending Basic Elements for Budget Solutions. *Security World, 18* (12), 20-26.

Spencer, J. (2002, July). Maximizing ROC (Return on Cost). *Security Technology & Design, 12* (7), 72-75.

APPENDIX A: SURVEY

Please use the following standard when rating each of the following aspects of the survey question.

1 = not at all 2 = very little 3 = somewhat 4 = quite a bit 5 = a great deal

Question: When deciding whether or not to purchase and/or implement security measures such as high security locks/padlocks, CCTV cameras, procedural controls, access control systems, duress/panic alarms, etc., how much do (or would) the following factors figure into your decisions?

A. The cost of security equipment and installation: _____

B. The level of difficulty involved in implementing changes in procedures: _____

C. Having information about how other businesses/organizations in your area have been impacted by particular crimes or risks: _____

D. Learning about examples of similar security measures being implemented at other businesses/organizations similar to yours in type and size: _____

E. The apparent knowledge and/or credibility of the person making the security recommendations: _____

F. Reducing liability concerns (e.g. preventing workplace violence, the burglary of customer's/employees' vehicles, etc.): _____

G. Having a cost-benefit analysis showing the expected benefits for implementing security versus the potential losses resulting from the failure to implement recommended security measures: _____

H. Being given a written security survey/risk assessment detailing security strengths and weaknesses and making specific recommendations: _____

I. The use of photographs to illustrate security weaknesses: _____

J. The use of multiple levels of security recommendations to provide options, such as minimum, intermediate, and maximum recommendations: _____

K. Knowledge of general crime statistics in the vicinity of your business/organization: _____

L. History of crimes having occurred at your business/organization: _____

M. Media attention to terrorism and other criminal activity: _____

N. Concern that added security will create the perception that your business/organization is a high risk or dangerous location: _____

O. Positive affect on public relations and perceptions of employees and/or customers by being seen as proactively addressing the issue of crime: _____