

SECURITY
Awareness in the
90^s

A
Symposium



Co-hosted by

The Defense Personnel Security Research
and Education Center

and

The Department of Defense
Security Institute

December 12-14, 1990
Monterey, California

19950503 058

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

Editor's Note

The contents of these published proceedings are in large part based on original papers presented in advance of the meetings by speakers and moderators. In some cases, particularly for the discussion sessions, the text is based on a transcription from tape recordings. While formal presentations by government employees have been reviewed by their respective public affairs offices, the opinions and statements contained here as provided by both government and nongovernment participants do not necessarily reflect the views of the Department of Defense nor represent officially confirmed facts. In at least one instance a speaker has granted us permission to reproduce copyrighted graphics and diagrams used in a presentation. Further use of material of this nature, of course, would require approval of the speaker. Inquiries about this publication or on how to obtain additional copies may be addressed to the Educational Programs Department, Department of Defense Security Institute, c/o DGSC, Richmond, Virginia 23297-5091

Table of Contents

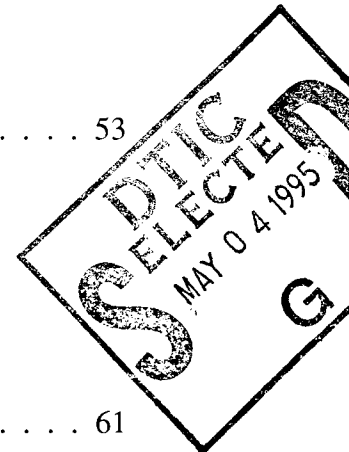
	Page
Preface	1

Changes Shaping The Security Awareness Landscape Of The 1990s

Geopolitical Trends	Maynard C. Anderson 3 Assistant Deputy Under Secretary of Defense (CI&S)	3
Information Security	Steven Garfinkel 17 Director, Information Security Oversight Office	17
Societal Attitudes	Tom W. Smith 19 Research Associate, National Opinion Research Center	19
Discussion	L. Britt Snider 53 General Counsel, Senate Select Committee on Intelligence	53

Strategies For Improving Security Awareness

Marketing Techniques	Robert Bailey 61 Executive Vice-President Director of Marketing Services BBDO	61
Training Approaches	Henry M. Halff 71 Chief Scientist, Halff Resources, Inc.	71
Program Evaluation	Robert O. Brinkerhoff 99 Department of Educational Leadership Western Michigan University	99
Discussion	Richard S. Elster 113 Dean of Instruction Naval Postgraduate School	113



DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

☒	
☐	
Availability Codes	
Dist	Avail and/or Special
A-1	

Planning For The Future

Current Problems	James A. Riedel 121 Program Manager, PERSEREC
	Deborah Russell Collins 131 Security Consultant Collins Consulting Group
	Ernest V. Haag 141 Western Regional Manager HumRRO International, Inc.
	Joseph A. Grau 151 Chief, Information Security Division, DODSI
Strategic Planning	William E. DeGenaro 159 Director of Business Research and Analysis, 3M Corporation
Discussion	R. Everett Gravelle 169 Director, DODSI

Meeting The Challenge

Government View	Brig. Gen. Frank K. Martin 173 Air Force Office of Security Police
	Rusty Capps 183 National DECA Coordinator, FBI
	Willis J. Reilly 191 Deputy Director of Security, CIA
Industry View	Jed Selter 195 Senior Manager, Security and Fire Protection, The Boeing Company
	Lawrence J. Howe 199 Vice-President, Corporate Security Science Applications International Corporation (SAIC)

Catherine A. Dyl	.203
Corporate Security Manager, Bolt Beranek and Newman	

The Executive View And Implications For Practice

Executive View	James A. Abrahamson	.215
	Executive Vice-President, Corporate Development, Hughes Aircraft Company,	
	James E. Freeze	.221
	President, The Freeze Corporation	
Implications	Harry A. Volz	.225
	Director of Security & Transportation Grumman Corporation	
	William B. Bader	.229
	Senior Vice-President, Policy Group SRI International	
	Maynard C. Anderson	.235
	Assistant Deputy Under Secretary of Defense (CI&S)	
Closing Remarks	R. Everett Gravelle	.239
	Director, DODSI	
	Roger P. Denk	.241
	Director, PERSEREC	

The Evaluation Of The Symposium By Participants

Assessment	Suzanne Wood	.243
	Research Associate, PERSEREC	

An introductory note from Mr. Maynard C. Anderson, Assistant Deputy Under Secretary of Defense (Counterintelligence and Security)

It has been observed that the timing of this symposium on security awareness coincides with a significant historical juncture. We are in fact standing at a crossroad and are about to stride out into unknown territory. On one hand we will venture into an era in which the "threat" to our way of life will be perceived in altogether different and complex ways from how it has appeared in the past four decades. On the other hand, we are candidly aware that the resources and technologies made available (or denied) to us to accomplish our tasks will be radically altered. As one attendee put it, "We will have to learn to do less with less, but do it better." I take this to mean that we will have to make every dollar count for more in terms of achieving our awareness objectives, restricting our activities to those things which we know to have a verifiable impact.

But how do we go about this? How can we succeed in our effort to convince employee populations that there is a direct and indisputable connection between national survival and the collective protection of certain types of information—protection from access by those who might use that information against us? This question is the underlying issue of this symposium. In response, two clear themes emerged from this experience. The first is that we have a lot to learn from training and communication professionals who operate *outside* of the security community. And secondly, we have a lot to learn from each other if we can occasionally break through the boundaries that separate government from industry, the Department of Defense from other Federal entities, one military service from another, security specialists from counter-intelligence professionals, practitioners from policy makers—I could go on and on.

We have come away from the meetings with the perception that there is an inventory of skills, methodologies, and psychological tools, freely available to anyone who has ever attempted to win over the hearts and minds of an audience for any purpose. This includes security educators. Consequently, this has been a unique opportunity for re-tooling and re-orienting security educators and policymakers alike—those who are responsible for implementing and for providing guidance to this very essential element of security programs. Because of being both unconventional in format and the first of its type, this has been a "risky" undertaking. But if in retrospect it is judged successful, it may be a major turning point in the way we undertake security education in government and industry.

According to convention, the proceedings of any conference are printed, sometimes well after the event, and distributed to each of the participants or attendees as a sort of historical record. We intend this volume to be much more than that. Our expectation is that it will serve as a vehicle for reaching

a much wider audience of professionals than those who were able to gather in Monterey in December 1990. It will be produced in quantity for broader distribution and, we hope, it will serve as a reference tool for future educators and managers in the decade to follow. We want the proceedings to have a life of their own and this symposium to be remembered even by those who did not attend.

Lastly, I would like to thank the professional and administrative staff of both the Defense Personnel Security Research and Education Center and the Department of Defense Security Institute for their exhaustive efforts to provide this community of educators, managers and policymakers with an educational experience that some have described as a landmark event in our professional lives.

A handwritten signature in black ink, appearing to read 'Maynard C. Anderson', with a long horizontal line extending to the right.

Maynard C. Anderson
Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

Preface

The goal of this symposium is to stimulate thinking on how to improve security awareness. Most of us would agree that security awareness is a crucial element of an effective security program and, even in normal times, the concept of awareness is one that perplexes and challenges us. In these times, the post-Cold War era, the concept takes on added importance. When we first conceived of this symposium we decided that it would not be possible to solve problems or develop recommendations here. Rather, we want to provide each of you with an opportunity to see and hear a variety of individuals from both government and the private sector discussing a common issue.

Some of our colleagues have observed that we in security need to break out of our tired old rut and look to other disciplines for ideas, techniques and tools to help us do our jobs better. And for a substantial part of this symposium that's precisely what we're going to do. Fully one-half of our speakers and panelists are persons whose primary expertise is outside of the realm of security and intelligence. We brought together a diverse group of experts from a variety of disciplines who will help us to look at security awareness from completely different points of reference. Their views, when coupled with some preliminary research findings and insights from our own colleagues in the security and intelligence communities, should help us gain some new perspectives and perhaps a new focus for security awareness.

Changes Shaping the Security Awareness Landscape of the 1990s

Geopolitical Trends

Maynard C. Anderson, Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

Information Security

Steven Garfinkel, Director, Information Security Oversight Office

Societal Attitudes

Tom W. Smith, Research Associate, National Opinion Research Center

Discussion

Moderator, L. Britt Snider, General Counsel, Senate Select Committee on
Intelligence

Mr. Anderson is the Assistant Deputy Under Secretary of Defense for Counterintelligence and Security. He is responsible for the management of DOD investigative, security, and counterintelligence resources funded by the Defense portion of the National Foreign Intelligence Program and Security and Investigative Activities Program. These programs involve over 10,000 personnel and a multi-million dollar budget.

Geopolitical Trends

by Maynard C. Anderson

An anonymous behavioral scientist is reported to have once said that one of every four people is abnormal. So, if four of you are together, and the other three look all right. That behaviorist was probably as credible as the anonymous French bureaucrat who said, "Never do anything for the first time." Thanks to the PERSEREC and the DOD Security Institute, we are doing something for the first time, and it is my pleasure to lead off this morning. My text for the day follows:

"Alexis De Tocqueville did not expect that men could be taught that what is right is also useful." (American Enterprise Institute adjunct scholar Walter Berns in the 1989-1990 Bradley Lecture series, July 10, 1990.) An examination of the history of other nations along with some analysis of the reasons for their past actions and the influence of those actions on their own populations as well as the rest of the world, should lead us to a better understanding on which to base selection of our defensive strategies.

Certainly there is a relationship between politics and geography, and geography sometimes has an equally significant influence on why nations act the way they do. Geography and politics also sometimes have influences on why "people" and individuals act the way they do. Why people act the way they do and what we should do to influence them is one of the reasons we are here. Since there are naturally geopolitical intrusions into our processes for maintaining the integrity of the national security, we need to try to identify and consider those that are most important along with other aspects of international competition. We need to relate those political phenomena, if we can, to personal actions and reactions that they might cause or stimulate.

Knowing characteristics of our potential adversaries might assist in determining why they believe exploitation of the United States is necessary as well as how they might go about it and, consequently, enable us to select the best defensive strategies.

Besides a determination of what we must protect, our defense strategies should include a logical explanation of why we protect it, why we share it

with some friends and allies (politics plays a major role here), and why its unauthorized disclosure is in the best interests of neither the nation nor the custodian.

Recent events that have changed the political and geographic structures of nations and alliances, particularly in Europe, will affect the attitudes of the population of the United States that is cleared for access to classified information. Apparent changing internal structures and philosophies of other nations, along with new economic powers like those of the Pacific Rim, certainly challenge us to attempt to determine whether they might change our inclination to act responsibly in support of our national security.

So, despite Leo Tolstoy's dismissal of historians as deaf men answering questions no one has put to them, there seems to be some benefit to paying attention to historical events in the hope that we might find lessons that will help us reach our objectives. In this instance, our main objective is to seek an improvement in the awareness of our constituencies that proper behavior in support of the national interest is necessary.

Syndicated columnist Haynes Johnson recently commented that on 7 September 1945, on the deck of the USS Missouri, the United States stepped onto the international stage. Our nation reconstructed Europe and guaranteed the security of the rest of the world. The United States is still the role model for the world, but, today, there is a dichotomy between that model and the internal problems of our country.

For us, it may be a question of leadership; how do we motivate our citizens to continue to live up to the role of "model to the world" while solving the problems of the country? How do we inspire our citizens to accept responsibility for their actions?

Their actions and reactions have been forcefully shaped and influenced in our brief 200 years of national life. The great events of United States history certainly have included the Revolutionary War, The Civil War, The Great Depression, World Wars I and II, and those European events of 1989. The Eastern European upheaval of 1989 began in Hungary in January, spread to Poland in April, East Germany in September, Bulgaria and Czechoslovakia in November and Romania in December.

Your children and grandchildren will be compelled to remember the year 1989 in their studies of history. It marked the end of the 44-year post-war period and marked the beginning of the Reconstruction of Europe. What killed communism? Sean Wilentz of Princeton, N.J., writing to the editors of *The New Republic* (January 1, 1990) speculates that it was the "workers and intellectuals . . . Ah, the cunning of history—Marx's chosen agents should

overthrow Lenin's tyranny." Of course, some have said that socialism is like Christianity; it has never really been tried.

Some important aspects of the European changes include:

- The demise of Soviet-imposed regimes;
- Steps toward democratization;
- Increased recognition of basic human rights;
- Movement toward free market economies;
- Soviet troop withdrawals; and
- German unification

The fact also remains that there is continued instability and unpredictability in the region, and the Soviet Union remains a military superpower with formidable capabilities.

Overall, from our perspective, espionage against the United States has been the catalyst, in episodic spurts, that has heightened awareness of the danger to the national security. The principal proponent of espionage against the United States has been the Soviet Union, and given its needs for advanced technology as a means to bring it into a more competitive position with the West, its intelligence collection activities will likely continue.

Soviet leaders have seemed to examine motivations of the foreign officials with whom they dealt. We have not always been so perceptive, perhaps. The historical use of power by the Soviet Union has certainly been guided somewhat by its perception of Western personalities.

Gaddis Smith, learned professor of History at Yale University, has recently commented that "...Soviets did seem to be concerned about American personalities. The Americans were not so concerned with the individuals within the Soviet system. I would offer this as characteristic of American attitudes in the 'Classic Period' (of the Cold War) ... To view the Soviet adversary in quite dehumanized terms, as not being people who could engage in a thorough discussion of anything." Professor Smith's observations might account for some of our behavior in reaction to Soviet activities during that post World War II period.

Paul Nitze, on 25 July 1990, gave some credence to Professor Smith's observations when he remembered his efforts in 1950 to articulate the United States policy of containment that lasted into the '80s. Mr. Nitze, speaking to

the concluding banquet of the conference on the origins of the Cold War sponsored by the United States Institute of Peace, said: "As we saw it, Soviet ideology took seriously the Marxist/Leninist view that communist socialism was destined, eventually, to triumph everywhere and that it was their duty to assist that historic process in every practical way. Thus, as we saw it, the contest was not one of competition; it has an absolute quality about it, which, from the Soviet side, did not permit compromise."

Since those early days of the Cold War, much has happened to change attitudes and actions that steered the course of nations. Henry Grunwald, in Time Magazine, October 8, 1990, commenting on the "Second American Century", wrote: "We have learned much about the connection between the abundant life and freedom. We have also learned that communism is really a new form of feudalism, a fixed society. Such a society cannot create abundance. The United States "...played the major role in providing capitalism, widely seen as doomed in the century's first half, to be a vital and successful system. Above all, it helped defeat the two great totalitarian enemies of freedom, nazism and communism."

I believe we must consider the interests, attitudes and actions of the nations of the world with which we deal in conjunction with the behavioral characteristics of the individuals who cause the national profiles to be developed. We have seen that personalities cannot be divorced from history. Future cooperation with both old and new allies will be predicated on their abilities and intent to protect what we are willing to share in our national interest. Our success as a nation will depend on our willingness to properly protect that which we cannot share.

There is not time within this presentation to explore all of the facets of the interpenetration of politics and personalities that might be applicable to the motivation of behavior. Nor have I overlooked the fact that there has been, and continues to be, obvious interest in the personalities of leaders and officials of other nations by the United States in order to deduce possible actions and reactions relative to foreign and international relations.

I do claim, however, that the counterintelligence and security community of the United States has not paid sufficient attention to the traits and characteristics of foreign competitors that might provide us with the means to determine and understand the basis for challenges to counterintelligence and security policies and procedures, particularly in the areas of motivation and awareness. Derivation of better techniques should result from improved knowledge of our own subjects as well as those who seek to influence them in a way inimical to the United States.

Analysis of the personalities of the collectors we confront, along with their targets and techniques, should provide clues that we would find useful. I do

not mean to imply that there is a sinister purpose in all of our international relationships, but we need to understand that every nation and every individual has predominant self-interests. There is a certain cynicism that intrudes into the relationships among nations and their reactions to each other. Mark Russell says that the United States' ally of the week is the country that treats our hostages the best.

Allies and relationships are apt to change remarkably. "While Clausewitz called war a continuation of politics by other means, economics may become a continuation of war by other means. There may be virulent trade wars among the economic big three—Europe, Japan and America (whose sphere should eventually include Canada and Mexico in an American economic community)." (Grunwald)

In examination of its leadership and its bureaucracy, Canada has recently proclaimed that it wants..."a public service that is professional, highly qualified, and imbued with a mission of service to the public." So do we, I hope. In cooperation with Canada, we have considered whether there should be some unique security policies to meet the peculiar needs of our isolated North American nations. Our challenge in this kind of potential new relationship would be to ensure and maintain in our public service in North America, as well as in the supporting industrial communities, a sense of mission to include the proper protection of essential secrets. Robert B. Zoellick, counselor to the State Department, in recent address to the American-European Community Association International's Conference on US/EC Relations and Europe's New Architecture, Annapolis, Maryland, on September 21, 1990, commented:

"I believe that shared ideas and values will become increasingly important as we create the 'alliances', institutions, and regimes that will address the challenges of this new era. Our bond was the hostile threat to our common values ...as the perception of that threat recedes, neither the United States nor Europe can take these associations for granted. New generations may not proceed on the basis of old assumptions."

The United States has realized that, for the last hundred years or so, it has been taken advantage of. There is nothing new, nor unusual, about emerging nations or established nations on their way to becoming emerging powers attempting to take advantage of other nations. Traditionally, the United States has been willing to help. "Lend Lease" is a good example of assistance to a Soviet Union which had already been partly armed and industrialized with the aid of the West by 1941.

Many have speculated that we, as a nation, lacked awareness of the consequences of our actions as well as what our adversaries were about, until we began to see our own discoveries and developments coming back at us in the

form of adversarial systems. The new awareness stimulated technology controls, new regulatory procedures, some statutes controlling information uses and dissemination, and a great deal of discussion about protection vis-a-vis the ability of U.S. industry to compete in the world market. Just as the dust was settling, a new set of circumstances caused another required reevaluation.

In attempting to translate the effects of recent history and current events into implications for the national security that involve people, I believe we can conclude that:

- Cleared people may have false impressions that the need for vigilance has ended;
- A "euphoria of cooperation" may replace the exercise of common sense;
- A misguided sense of rendering assistance may be felt by some.

In response to these postulations, we must reorient the counterintelligence and security countermeasures communities so they do not merely identify hostile adversaries and prevent their access to our information worthy of protection, but they clearly identify what we want to protect and secure it from all who are not authorized to receive it. Security must become a pattern of behavior.

Awareness is the capital of the security process. It involves understanding of the criteria for protection, the need for protection, the options available for protection, and the consequences of the failure to do any of those things correctly. Our challenge is to teach our cleared population what is right and convince them that it is useful. The criterion for protection of information has been the damage caused by its disclosure to persons not authorized access. Another criterion is value—why is the information worth protecting in the first place?

A "value" method of judgment may be easier to work with and may have more validity. If something has worth, there should be a decision made to protect it. The value may fluctuate so that at any time it may be worth more or less than the original value. This is a product of perception as well as reality.

Once something is classified, there is an agreement to pay the price of the classifier's appraisal of value. As value retreats, however, there is no reason to continue to pay the price. It should be easier to make downgrading or declassification decisions on the basis of value fluctuation than on the basis of subjective estimates of potential damages.

The concept and use of the classification guide is based on the premise that classification authorities are willing to assess the value of information. They should do so to the extent possible, for the duration of the program. That is not always possible, realistically, but with a value-oriented discipline, it should be easier.

The application of or matching of value to damage has always been speculative and subjective. We must involve threat (sometimes), counterintelligence analysis, operations security (OPSEC), vulnerability evaluation, foreign availability of material, technological state of the art, military application, all of which serve in some way to help determine something's value. There must be considered the cost of classification in relation to benefit from the information's use.

After we have established the need for protection comes the equally difficult task of encouraging its custodians to believe in the information's value and behave accordingly. I believe this task will be easier if predicated on value rather than potential damage.

Security education and motivation are often afterthoughts in the security process. Their importance is demonstrated by their necessity throughout the security cycle. Proper behavior is the objective of the personnel security process from beginning to end; in the accountability process during the period of access, and during the "post debrief" period. Motivation of the individual toward responsible behavior is required as long as the person carries in memory the classified information to which there was access. Unauthorized disclosure is not relative to the status of the individual once the individual has been given access. The motivation must have a life as long as that of the motivated person.

The real treasure of the twentieth century is information. Whether it is intelligence, critical technology, or any other category related to the national interest, it is the economic, military or political balance factor that can cause the world to remain stable or tip to one side. It is an amorphous body of material in all sorts of media, in the custody of a great many people, all of whom are different in terms of how they react to motivation.

For example, it is a fact that our military personnel like to talk about their weaponry. The current situation in the Persian Gulf poses interesting problems from a security perspective. The soldiers, airmen and sailors from numerous countries are now participating in joint operations. Language barriers notwithstanding, there must be considerable pressure to compare notes about the effectiveness, performance, range and operational characteristics of the sophisticated weapons they employ. Much of this information is classified. This might be a good test of the effectiveness of our security education and motivation programs.

In attempting to create security awareness, we are working with a system—a system built on a set of managerial concerns, rather than an engineering design. The product of the system is people; the method of production is training. The use of the method and the operation of the system do not occur in a vacuum. They require the understanding and possible manipulation of other management systems to be successful.

Our focus must be on how it works. We evaluate it in terms of measuring impact on mission. Will it produce people with awareness, who, both by example, and word, carry the message and create a "no fault" situation? Is it effective? Could it be done better or in less time? What are the follow-up actions necessary for skill retention and enhancement?

We will continue to attempt to determine the rationale for individual actions of trust and betrayal. Rationalization of behavior is always important to the person engaged in illegal activities. As observed previously, the changes in East-West relations may offer a more plausible rationalization for some persons to commit espionage.

In terms of application of process in making judgments about our population, whether it is for the purpose of determining methods of motivation toward particular behavior or the individual's eligibility for access to classified information which places the person in peril of motivation technique application, there is dispute between advocates of uniform, standard procedures and advocates of subjectivity.

Without consideration for Oscar Wilde's taunt that consistency is the last refuge of the unimaginative, those favoring uniform, standard procedures claim that they will eliminate bias, special treatment and discrimination. Those bent toward subjectivity claim that each situation must be judged on its merits.

"...when faced with the task of making judgments about a singular case, the prediction of human conduct ignores the probabilistic data and operates from the premise that each case is unique. The application of the statistics of prior probabilities to the unique case is irrelevant." (Sarbin, T.R. (1986) "Prediction and Clinical Inference: Forty Years Later." *Journal of Personality Assessment*, 50(3), pp. 362-369, Lawrence Erlbaum.)

Following on with Dr. Sarbin's concept, we might conclude that concrete information that piques emotional interest is more significant than abstract information about other cases in the past.

If those whom we seek to motivate toward particular behavior are viewed as figures in a story, perhaps that narrative can become the organizing principle on which to base the selection of strategies. You will recall earlier refer-

ence to the significance of personalities who lead nations. They might also be figures in this story. Essentially, we seek to determine the actions of the person(s) without concern for any hypothetical actions that might have been expected. The actions then represent the individual's capabilities and intent to perform in accordance with certain requirements. Capabilities are more easily measured by assessment of knowledge, skills, and abilities. But intent is the silent operation of the mind. As the actions and measurements become apparent, I would suggest it is the intent that we must identify, shape and influence.

Creating or devising or selecting awareness techniques rely on evaluation of prior actions, those of individuals, and sometimes those of their organizations. The process takes its shape from history, as well as current appearance and behavior.

There might be little difference between this process and that of adjudication. We are attempting to make judgments about effective techniques on the one hand, and whether someone will perform in a prescribed manner on the other hand. Neither can be done without knowledge of the subject or the subject population. And someone has said, "The imprecision of the science engenders a healthy respect for the unpredictable."

"Awareness" means that an individual understands that there is responsibility to do something. It also means that there must be leadership responsibility in program management. "Lead by example" is another way to say that management makes an impact on the process that creates awareness. Characteristics, beliefs, predisposition, creation of an image, are all factors of significance in the history of organizational administration.

Traditionally, we have concentrated on "awareness" as merely something that is endemic to a subject (a characteristic of) or that affects subjects. It is not likely that we have paid much attention to awareness as a factor in the professional actions of those who decide what it is that will or will not motivate that subject. Just as the case of an adjudicator, we should ask whether that official has knowledge, skills or abilities similar to those of the subject. Does the official share the experiences of the subject? If not, has the official tried to simulate the characteristics of the subject, the circumstances in which the subject lives and works, the pressures that tug and pull on that subject every day?

It would seem reasonable that we should try to find the lowest common denominator in the process in terms of shared experience. Only then can we best provide those in the field, at the end of the pipeline, tools and advice that may be applicable to the motivation of those for whom they are responsible; providing them options that might instill the obligation of accountability in their personnel. We must all determine what will work and why.

For example, to make the best choices of techniques that might influence industrial leaders and their personnel in these changing times, it would seem reasonable to review their attitudes toward employment and see if we can make any connection between those and their attitudes toward the national security.

The October 1990 *Business Month* magazine published results of a *Fax-poll* to which 16,000 corporate executives from 10,000 companies responded by telling what they think and feel about the crucial business issues that affect them every day. The idea was to give readers a voice and then react with stories that reflected and played off their concerns. As a result of the *Fax-poll*, this was learned about business executives:

- They are responsive.
- They are quick to take offense.
- They taught us a crucial lesson about human nature: feeling is far more important than fact.
- They can't abide the thought of defeat.
- They are enraged by things they can't control.
- They aspire to visionary ideals.
- They don't like to deal with some issues, for example, industrial pollution, illiteracy, "dirty work" like layoffs.
- They are sometimes willing to take the easy way out.
- They are not easy to categorize.
- They are willing to be self-critical.

I picked two areas of the *Faxpoll* results to look at a bit more closely. One dealt with ethics and posed the question, "Is business ethics an oxymoron?" One company emerged as a worthy example of good behavior. IDS in Minneapolis is a firm at which all planners must certify that they understand the behavior requirements for dealing with clients. When something goes wrong, it is publicized by the compliance department to every IDS office nationwide along with an analysis of how it could have been prevented. The lesson they've learned is that when everyone knows the rules, it makes them easier to enforce.

The second area I picked dealt with loyalty. The analysis concluded that as times have changed, stability has become a synonym for paralysis: "The irony, or perhaps the word is hypocrisy, inherent in this phenomenon is that nobody preaches corporate loyalty more and practices it less than top management." It was found that corporate loyalty was a virtue only when it was useful. As a consequence, firms that reward loyalty still get it. The organization man hasn't changed much. The former military model is giving way to an egalitarian one.

In an assessment reminiscent of our analyses of espionage cases, the question was asked: How do you form new attachments without the promise of loyalty? The quick answer: "Buy them." The conclusion: People do what they get rewarded for.

Of significance to us particularly, perhaps, is the observation of Peter Drucker in *The New Realities*, that "knowledgeable workers know that their knowledge, even if not very advanced, gives them the freedom to move." As we know from experience, that is most often true if the workers hold high clearances and sensitive accesses.

Do the corporate leaders' attitudes have any meaning in determining security awareness? Does corporate loyalty translate in any meaningful way into national loyalty? Loyalty might be schizophrenic if it requires actions in support of the national security that are not necessarily in the best interests of a corporation. Loyalty to corporate objectives, organization, colleagues, associates, employees, might not mean loyalty to the government exists. In a multinational corporation, loyalties might be even more divided, even though inadvertently and with no intent to do harm.

The determination necessary in situations like these might revolve around whether positive motivation in the form of prosperity, success, civic recognition as a result of achievement of objectives through corporate loyalty, is a stronger motivation than the threat of jail for failure to adhere to security requirements.

Clement Communications, Inc., of Concordville, Pennsylvania, uses the comic strip character Herman as a motivator for its clients. The company claims that Herman's misadventures reduce absenteeism, improve morale, and build teamwork in 23,658 companies. Clement asserts that motivation experts agree that employees will not be preached at, patronized or talked down to; will not be bullied into punctuality, attention to detail, good workmanship; resent heavy-handed approaches to absenteeism, carelessness, waste, poor attitude; and, that appeals to company loyalty and high-toned speeches about teamwork and cooperation are a waste of breath. Other companies agree that a good approach to getting the attention of the worker is humor.

At 3M Corporation, information security is a combination of five elements, the first of which is personal awareness. The others are information management, document controls, computer controls, and physical security. In western Europe, 3M has more than 11,000 employees, 19 companies, 19 primary laboratories, and 23 manufacturing locations. The company has found that effective communication is the greatest challenge transnational corporations will face in the future.

A caution sign should probably be erected here to warn us to be careful of oversimplification. We need to learn what will motivate all of our different people and then apply necessary techniques. And, we need to understand that what works today might not work tomorrow.

Espionage is probably a multifactoral event. Cause and effect is not a simple relationship. It is the interaction of many factors. We don't know whether there is an association between or among factors in cases of espionage that is greater than would occur at random. We don't know if there is a statistical significance to results of our examination of this phenomenon. It is being studied and we hope to find out.

We should not be too quick to dismiss different methods and means. All sorts of techniques are used for motivation. The University of Washington Chapter of Theta Xi Fraternity was expelled from campus and suspended by the national office in January (of 1990) for a hazing incident. Police found pledges with white grease and peanut butter on their bodies, wearing only underwear, in the proximity of stolen sheep that were, according to police, "over-heated and agitated."

The young communist league of the Soviet Union, reported to have lost 10 million members since *perestroika* began, started in January to offer scarce condoms for sale at rallies in the Ukraine as a means of increasing attendance. (Both of these examples are from the compilation of Chuck Shepherd, a faculty member at George Washington University's School of Government and Business Administration, and a fan of unreasonable behavior.)

If as Jonathan Swift proclaimed, "Vision is the art of seeing things invisible," we need a great deal of vision to determine what it is we can do to cause most people to act with responsibility. Motivating people to the proper state of awareness, whether on a global scale, in a small, local facility, or in an Army company clerk's office, requires everyone's best efforts.

I subscribe to the philosophy that four of the most important words in management are, "What do you think?" There is a certain arrogance to a conference like this where a group of senior officials of industry, academia and government gather to determine, discuss and perhaps even decide how to influence people. It is as though we have accepted an obligation to decide what

is good for them. Have we asked them? If there were one recommendation to emerge from the proceedings of this symposium, I would hope it might be that we would all go back and ask the people we work with, "What do you think?"

In security awareness, people are not the problem; the system is the problem. We have a system designed for the fifties and we need a system designed for the nineties. We need to *steer* our subject population to the desired objective. We need an entrepreneurial system to respond to rapid change with flexibility. If you are not operating a program that people like, or in which they will participate, you are out of business.

Our "customers" are captive. But we are dependent on them to preserve our security. That should force us to get close to them. We need to deal with them personally. They need to be recognized for their achievements and accomplishments and potential. We need to figure out how to do that. It is an objective of personnel management as it relates to personnel security.

General George Patton: "Never tell people how to do things. Tell them what you want them to achieve and they will surprise you with their ingenuity." If you want performance, define the mission and spell out the desired results. We will get innovation from our people. It bubbles up.

We cannot treat symptoms any longer. We need prevention strategies. This symposium is the first step in prevention strategy. I recommend:

1. That we give our units control over their programs.
2. That we do customer surveys—Let's go out and see what the people who work for us tell us. Let them choose how they want to be treated.
3. Let's have competitions for best programs and techniques among our organizations, both inter-agency and intra-agency.
4. Let's have effective and continuous reviews of our programs with an objective of program and system improvement.

Mr. Garfinkel has served as the Director of the Information Security Oversight Office (ISOO) since May 1980. He is responsible to the President for the administration of the Government-wide information security program. Prior to assuming his duties as Director, Mr. Garfinkel was counsel with the General Services Administration.

Evaluating Security Education in the 1980s

by Steven Garfinkel

Steven Garfinkel, Director of ISOO, was asked to address the topic of the changing nature of information, the requirements to protect it, and how those subjects impact on efforts to improve security awareness. The following is a precis of his talk.

Garfinkel began his talk by noting (1) that he was uncertain what his topic even meant; and (2) that he was a poor predictor of the future. Accordingly, he had decided to look at security awareness in the '90s by evaluating security education in the '80s. He noted that in the '80s it was considered reasonable to equate security education (the means) with security awareness (the end).

Garfinkel resorted to two self-described gimmicks to examine security education in the '80s: first, he issued a "report card" in several different subjects related to security education; second, he invented several semi-fictional education experts to help him issue the appropriate grades. The subjects for which he issued grades included: (a) the availability of security education and training; (b) the utility of the security education curriculum; (c) the quality of the security education faculty; and (d) the impact of security education on security knowledge and awareness. Garfinkel found a disturbing dichotomy between the overall grades for the first three subjects, which were relatively high, and the last, which was considerably lower. He concluded that we were wrong to equate security education with security awareness. While the absence of a good security education program inevitably resulted in poor security awareness, the presence of a good education program did not necessarily result in good awareness. Obviously, other factors are at work that need to be identified and cultivated.

Dr. Smith is co-principal investigator of the National Data Program for the Social Sciences and director of its General Social Survey. In addition to working at the National Opinion Research Center at the University of Chicago, he has taught at Purdue University and Northwestern University. His research interests focus on the study of social change and he has produced a wide range of publications on trends in public opinion.

Societal Attitudes and Security Awareness

by Tom W. Smith

Introduction

We usually do not think of counter-espionage and intelligence security measures as being affected by the climate of public opinion. Intelligence threats are seen as coming either from foreign agents or troubled individuals beset by personal problems or character flaws. But, as the Oxbridge recruitments in England in the 1930s illustrate, at certain times and places societal conditions can provide a more (or less) hospitable climate for espionage. As societal conditions shift, one must first recognize how the changes may undermine intelligence security and, second, develop procedures to maintain security despite the changes. Security awareness means not only keeping up with the latest technologies for gathering and protecting information, but also understanding how changes in the climate of public opinion may alter our ability to maintain security.

Public opinion can affect security in several ways, through its impact on 1) the pool of potential employees, 2) current employees, 3) security personnel, and 4) legislation and executive regulations. Public opinion on various security-related issues affects 1) the quality and quantity of potential employees, 2) the resolve of current employees to remain both diligent and loyal, 3) the ability of security personnel to carry out their duties, and 4) the passage of legislation and regulations about permissible counter-espionage measures such as wiretaps, employment screening, and background checks. In brief, public opinion impacts on intelligence security in many ways.

Those engaged in security awareness training must know their target audiences in order to get the security message across effectively. In order to know how best to reach your intended audience and to motivate their diligence, you must know what values, concerns, and predispositions they bring with them. Like both teachers and politicians, you must "know your audience" to ensure that your message is received, understood, and acted upon. While your audience is narrower than the general population that I'll be referring to today, it still reflects the general attitudes and values of the

American people, and what I have to report should generally apply to your segment of the American people.

Data and Methods

Information on public opinion about security-related issues was gathered from dozens of surveys from 16 different survey organizations. To assess the current state of opinion and the likely direction of public opinion in the near future, we have employed, whenever possible, trend and cohort analysis.

Trend analysis involves the tracking of recent changes in attitudes. It allows us to clearly compare the present with the past and gives us some limited insight into future conditions.

Cohort analysis compares how attitudes differ across age groups. Age differences can be a function of either aging (maturation) or generational changes across birth cohorts. For example, older men are more likely to be bald than younger men. This is a result of their age, not the impact of the historical period in which they were raised and now live. Older men on the other hand are also more likely to favor traditional roles for women. This is not a function of their biological age, but of the times and culture in which they were raised. That is, each successive generation was raised in a society that was more accepting of modern roles for women, so each succeeding generation of men is less supportive of the traditional viewpoint on women. When age differences are due to cohort effects rather than aging effects, one can usually count on change continuing to slowly shift towards the position of the younger cohorts since 1) cohort turnover means that as the older generation dies off and is replaced by the incoming generation, its attitudes will also "die off" and be replaced by incoming ideas and 2) at least in the short term the attitudes of future generations (*i.e.*, people becoming adults over the next decade) will usually resemble the attitudes of the current generation of young adults more than the attitudes of older adults.

Utilizing the fact that the youth opinions of today tend to become the adult opinions of tomorrow, we have included in our analysis three major youth studies: the Gallup Teen surveys of 13-17 year olds, the Monitoring the Future surveys of high school seniors, and the Cooperative Institutional Research Program's survey of first-year college students.

Finally, we will at least occasionally be able to carry out time series, cohort analysis (*i.e.*, how the attitudes of age groups have changed over time). By examining whether opinion changes at the same rate and in the same direction across different age groups, we can detect recent, generational effects.

Security-Related Attitudes

There are many societal attitudes that touch upon security matters in one way or another. Table 1 lists the main topics which have implications for maintaining security. In the table we list in parentheses the condition for each topic that would tend either directly or indirectly to make it more difficult to maintain security. For example, we would expect counter-espionage to be more difficult as the degree of perceived threat from external sources declined, since both employees and security personnel might become less diligent in maintaining security and more susceptible to recruitment by "harmless" foreign powers. Similarly, an increase in concerns about personal privacy might lead to legislation restricting counter-espionage measures, to a shrinking pool of potential employees who would be willing to subject themselves to security checks and surveillance, or to less cooperation by current employees. In the following section we will examine what current opinion and trends are on each of these topics and how the public's attitudes on these topics impact on intelligence security.

External Threats

With the end of the Cold War the public's regard for the Soviet Union has increased and the perceived threat from the Soviet Union has declined markedly. For example, in 1982 51% strongly disliked (-4 or -5 on a scale from +5 to -5) the Soviet Union, while in 1990 only 15% felt the same way. Likewise, while 67% saw the Soviet Union as a serious or very serious threat in 1986, only 33% see the same degree of threat in 1990. As long as reform proceeds in the Soviet Union, this movement is likely to continue. At least in part, good feelings towards the Soviet Union are likely to grow because the younger cohorts of adult are more favorable towards the Soviet Union than older cohorts. In 1990 only 10% of adults 18-29 strongly disliked the Soviet Union compared to 16% of adults 30 and older. As of late 1989, however, the Soviet Union was still seen as the greatest threat to the United States over the next 10 years, followed by Japan, China, Iran, and Libya.

It is particularly instructive that Iraq did not make this most threatening list. The absence of Iraq underscores two important points. First, public opinion reflects how people perceive matters according to conditions at the time they are questioned. Changing conditions will change opinion. Second, the "surprise" emergence of the Iraqi threat amply validates President Bush's pre-invasion warning that in the near future "uncertainty" is our greatest threat.

Military Preparedness

Support for a strong defense and military preparedness varies inversely with external threat. As the international climate heats up, support grows

Table 1

Trends in Public Opinion Related to Intelligence Security

- A. External Threat (Less)
- B. Military Preparedness
 - 1. Defense Spending (Less)
 - 2. Disarmament (Approve)
 - 3. Military Service/Draft (Opposed)
- C. Support for the Government and the Military (Less)
- D. Personal Values
 - 1. Obedience (Reject)
 - a. Children
 - b. Citizens
 - c. Soldiers
 - 2. Honesty (Reject)
 - a. Children
 - b. School
 - 3. Individual Expression (Approve)
- E. Privacy (Approve)
- F. Counter-espionage Measures (Oppose)
 - 1. Wiretapping
 - 2. Lie Detectors
 - 3. Drug Testing
 - 4. Employee Screening
 - 5. Personal Information and Credit Checks
 - 6. Other
- G. Freedom of Information Act (Approve)
- H. Media Publication (Approve)
- I. Punishments (Lenient)

and when foreign relations improve, support diminishes. Support for defense spending was low in the early 1970s in the immediate aftermath of the Vietnam War. In 1972 only 12% favored more money for the military. Support for more spending slowly grew during the rest of the 1970s until in 1978 29% backed more defense spending. Then the invasion of Afghanistan more than doubled support for defense spending to 60% in 1982. As real defense spending rose in the 1980s and the Soviet threat diminished, support for military expenditures fell until by 1990 it reached an historic low of 11%. (Overall there are few cohort differences on defense spending.)

While support for defense spending has waned in the 1980s, support for disarmament has been strong and growing. In 1990 78% endorsed cuts in nuclear weapons going beyond the currently agreed upon START reductions and 74% favored the elimination of all nuclear weapons. Since the mid-1980s, two-thirds of first-year college students have thought that the United States is not doing enough to promote disarmament, and among high school seniors support for gradual, *unilateral* disarmament climbed from 15% in 1979 to 26% in 1989.

At the same time the willingness of high school seniors to serve in the military in a future war has been tepid with only 18% saying that they would be very likely or sure to volunteer. Commitment to military service has, however, remained virtually unchanged over the last decade. In addition, a military draft has not been popular with high school seniors. In 1989 only 14% favored instituting a military draft, down slightly from 17% in 1981.

Overall, both among the general public and youths, support for military spending is at record lows, while support for disarmament is high. There is also a reluctance among youths to serve in a future war or to support a military draft. Support for military service and defense has not changed notably in recent years however.

Support for the Government and the Military

Support for the government in general and the military in particular is indicated by questions about confidence in the leaders of these institutions, the honesty and morality of the leaders, the job these institutions are doing for the country, the amount of influence that they have, and willingness to work for these institutions. Looking at the executive branch and the presidency, we see somewhat of a roller coaster trend as confidence and other measures have fallen in response to difficulties and scandals and risen as the elections of new presidents rekindled hope. For example, in 1973 (after the Watergate break-in, but before the disclosures) 30% had a great deal of confidence in the executive branch of the federal government. This fell to 14% in 1974-76 after Watergate became widely known, rebounded to 29% in 1977 with President Carter's inauguration, fell to a record low of 12.5% in 1980 during foreign policy and economic troubles, moved back up with President's Reagan's election, fell again to 13% during the 1982-83 recession, edged up to 21% in 1986, slumped back to 17% in 1988 as the Iran-Contra scandal emerged, and then again gained ground to 24% in 1990 after President Bush's election. The two main lessons from this pattern are 1) there has been no long-term, secular trend in government confidence and 2) confidence is mainly a product of performance; scandals, economic hardship, and foreign policy failures drive down support.

When we examine trends among age groups, we learn a valuable third lesson that is masked among the other trends. Among those 18-29, confidence in 1990 is 6 percentage points *higher* in 1990 than in 1973, but among all other age groups confidence in 1990 is 10-15 percentage points *lower* in 1990 than in 1973. This suggests that there is a Reagan generation of younger adults who came of political age during the Reagan Era and who have more confidence in the presidency than those who were or became adults during the time of Watergate and the Carter malaise.

Support for the military does not undergo nearly as much fluctuation as presidential support. Among all adults confidence in the military is a bit lower than the early 1970s, but little changed during the 1980s. The young again show a Reagan generation effect. Among those 18-29 25% had a great deal of confidence in the military in 1973, while 40% did in 1990 (+ 15 percentage points). However, in all older age groups there were slight declines (-1 to -5.5 percentage points) from 1973 to 1990. This pattern of increasing confidence in the military among the young is reflected in the rising percent of high school seniors who see the military as doing a good job (up to 60% in 1989 from 40% in 1980) and the more modest gain in the number who see working for the military as acceptable or desirable (from 22% in 1980 to 26-28% in 1983-1989).

Neither in terms of support for the government nor support for the military are there any signs of political alienation that might indicate a popular unwillingness to back the country, or any decline in patriotism.

Personal Values

Obedience

Since most security breaches involve conscious disloyalty (usually against both an employer and the country), the value of obedience is clearly related to intelligence concerns. We have various questions about obedience: parental obedience as a desirable trait for children, citizens obeying the law and government, and soldiers following orders. Parental obedience is highly ranked as a desired trait in children. Out of 13 traits, obedience ranks third after honesty and having good sense and sound judgement and is well ahead of good manners, trying hard to succeed, neatness, self-control, acting like a boy/girl, getting along well with other children, being responsible, being considerate of others, being interested in how things happen, and studiousness. There has been little change in the ranking of parental obedience in recent years and little difference across age groups under 50 (those over 50 do rank obedience even higher).

In terms of citizen obedience, people are about evenly split between the importance of obeying the law and following their own conscience. For example, in 1990 57% believe there are circumstances under which people should follow their own consciences and break the law, while 43% believed there were no exceptions. High school students are also deeply divided on the matter of obeying the law. In 1989 42% agreed "You can't be a good citizen unless you always obey the law," 36% disagreed, and 23% neither agreed nor disagreed. Most high school seniors (66% in 1989) do agree that you can be a good citizen if you disagree with the government. Thus, the public is supportive of dissent, but divided about whether people should ever

disobey the law. These opinions have shown little change over the last two decades.

On military obedience, in 1975 33% of high school seniors agreed that servicemen should "obey orders without question." This increased to a high of 47% in 1983/84 and has since slipped back to 42% in 1989.

Obedience is and remains an important value to Americans, although loyalty does not extend as far as Stephen Decatur's "our country right or wrong."

Honesty

Honesty has been consistently ranked as the most important trait for children to have. There has been no change over time in its rank and there are no significant differences across age groups.

There is some information on the actual honesty of Americans, although only in regard to cheating at school and the evidence is contradictory. Among teenagers over half indicate ever having cheated on an examination, while about a third of first-year college students report cheating at least occasionally. Among teenagers the trend shows less cheating now than previously, but more cheating is reported by the college students (who also report an increase in copying homework).

Individual Expression

By individual expression, we mean the idea that each person should follow his or her own wishes without worrying about conformity. At least among high school seniors support for individual expression has been growing since the 1970s. In 1975 41% believed that people "should do their own thing even if people think it strange" and in 1989 50% endorsed this idea. Similarly, in 1976 30% agreed or mostly agreed that "I get a real kick out of doing things that are a little dangerous" and in 1989 this was 40%.

Privacy

Personal privacy became an increasing concern of people between 1978 and 1982 (rising from 31% very concerned to 45%), but since 1982 there has been little further increase (46% in 1990). Nor are there any age differences that indicate that incoming generations are more concerned than older generations. In addition, a majority feels that laws to protect privacy need to be strengthened.

Counter-espionage Measures

Wiretapping

Despite the increased concern over privacy, there has not been a decrease in support for intrusive measures such as wiretapping, lie detectors, and drug testing which might be used to detect or deter espionage. When asked about wiretapping in general without any qualification about who is using it or why, only about a quarter of Americans approve. Approval, however, slowly grew from the 1970s to the present. The lack of significant age differences suggests that generational shifts are not driving this trend forward, however. Approval of wiretapping is notably higher when 1) there is court approval and 2) when the target is a known criminal, a spy, or a terrorist. For example, while only 22% approve of wiretapping a suspect without a criminal record, 46% approve if the suspect has a long criminal record.

Lie Detectors

Similarly for lie detectors, people tend to object to the wholesale use of these devices, but approve of their use to help solve a theft or in security matters. For example, in 1986 polygraphing was approved by 26% for all current employees of a company, 46% for all government employees, 75% for employees suspected of stealing, and 81% for the "periodic testing of government employees who have access to classified information." The public is also more inclined to support the use of lie detectors than are most government officials and elites.

Drug Testing

There is widespread support for drug testing of both potential and current employees, both in and outside the government. When it comes to "federal employees involved in national security areas," 93% of the public said they should be "required to take tests for illegal drug use on a regular basis." Only support for the testing of airline pilots, at 94%, was higher.

Employee Screening

People are willing to subject potential employees to a number of pre-employment tests and checks. There is little support (only 12% in 1986) for checks on an applicant's "lifestyle or political associations" and only about a third think that lie detector testing should routinely be used, but a majority approve of written "honesty" tests, and 80% or more support checks on one's criminal record and drug testing. While none of the questions specifically asked about employment screening for jobs involving classified materials, it is likely that approval for screening and testing such applicants would be even higher.

Personal Information and Credit Checks

There is growing concern about credit checks and the disclosure of personal information. In 1990 71% agreed that "Consumers have lost all control over how personal information about them is circulated and used by companies" and only 46% felt that "My privacy rights as a consumer in credit reporting are adequately protected today by law and business practices." In 1978 14% reported that they had decided not to apply for a job, credit, or insurance because they did not want to provide certain information. By 1990 30% reported not applying for this reason. However, people still acknowledge that there are many legitimate reasons for credit checks. In 1990 94% approve of a check when a credit card is applied for and 96% when people want a loan. There is no information unfortunately on credit checks related to security matters.

Other Measures

Other measures that the public favors to reduce spying are investigating why the FBI and intelligence agencies "have been so slow to find and crack down on spies" (favored by 86%), reducing the number of classified documents so fewer people will handle secret material (80%), and "firing managers in government operations who turn out to have spies working for them" (63%).

Freedom of Information Act

Important governmental and military information is available from various published governmental reports, academic research papers, and other public documents. In addition, unpublished and potentially sensitive information may be obtained through the Freedom of Information Act (FOIA). In the early 1980s, the public opposed proposals to curtail access via the FOIA, even to protect intelligence information. By 1990, however, public support for disclosure appears to have waned; 58% agreed that "federal freedom of information laws have gone too far in letting individuals and businesses get government documents."

Media Publication

One of the most serious potential conflicts in our democracy is between the press and government over the publication of classified material. In deciding whether the press should be able to publish classified government documents or whether the government should be able to maintain its secrets, the public considers whether national security is involved. Large majorities favor the publication of confidential papers that "reveal incompetence or dishonesty by public officials (73%)" or are about "economic plans" (61%). Conversely, majorities oppose the publication of "defense plans" (83%). When

it comes to "top secret materials" that do not "endanger national security," the public splits down the middle, 42% favoring publication, 47% opposed, and 11% undecided.

Punishments

A key indicator of a society's resolve on a matter is its willingness to punish transgressors. Spying and treason are clearly seen as very serious offenses by the American public. While support for capital punishment is highest for murder, there is about as much support for executing spies and traitors as for rapists and hijackers and more support than for executing drug dealers. Support for the death penalty appears to have risen from the 1970s to the mid-1980s, but then declined slightly. As of 1988 42% support the death penalty for "Spying for a foreign nation during peacetime." This decline came about in part because the younger generation is less supportive of the death penalty than older generations are.

What about the punishment of actual spies in actual cases? The only information available concerns the conviction in 1987 of Jonathan Pollard for spying for Israel. On one hand, this case illustrates that people are concerned about what country is behind the espionage and consequently how much threat there is to the United States. When people were asked whether they were more bothered "to learn that Israel spied against the United States or to learn that once again Russia was caught spying against the United States" 46% selected Russia, 26% Israel, 15% both, and 13% unsure. However, the lower concern over Israeli spying did not materially improve the public's attitude toward Pollard. When asked if Pollard's spying made them feel angry, embarrassed, or sympathetic, 48% said angry, 12% embarrassed, 7% sympathetic, 7% something else, and 27% uncertain. Asked to evaluate Pollard's sentence to life in prison, 9% thought it too lenient, 57% correct, 16% too harsh, and 17% undecided. Thus, of those who had an opinion on the matter, 82% felt that life imprisonment (or more) was an appropriate punishment.

Summary

The task of intelligence security is complicated by American public opinion. Certain attitudes and trends indicate that maintaining vigilance against espionage may become increasingly difficult, but other opinions and changes show support for counter-espionage measures.

Of all the changes during the 1980s that are likely to continue into the 1990s, the one that is most likely to undermine counter-espionage efforts is the perception of diminished threat from the Soviet Union and the resulting decline in support for military preparedness. It is hard to keep up your guard if you do not perceive an immediate, serious threat.

On the other hand there is no growing disillusionment with either the presidency or the military. In fact, the incoming adult generation tends to have more confidence in governmental and military leaders and be more approving of the job they are doing than older adult cohorts. There also are no signs of widespread political or social alienation or a weakening of patriotism.

Our inspection of personal values also shows a mixed pattern. Obedience and honesty are highly rated values and there is no clear evidence that these moral values are eroding. Expressive individualism has been increasing however. This growth in self-centeredness might undermine conformist security programs.

Similarly, more concern about personal privacy could inhibit the use of intrusive security measures. For now at least, this has not materialized. People are often supportive of such counter-espionage measures as wiretapping, lie detectors, drug testing, employment screening, background checks, and other measures. While the public generally finds such intrusions objectionable, they generally accept them as justifiable when national security is involved.

This same distinction is important when considering intelligence leaks via the media (and the Freedom of Information Act). People support freedom of the press and do not want the government to be able to stifle whistleblowers or to block the publication of most governmental information. But again, people make a distinction when national security information is involved. In fact, the public appears to be more willing to prevent the publication of defense materials than are the courts.

When it comes to the act of espionage itself, people consider it a serious crime. There is substantial (but not majority) support for the death penalty and this support has remained strong over the last decade. In addition, the Pollard case in 1987 suggests that it is the act of disloyalty itself and not who one spies for, or why, that primarily determines attitudes towards punishment. Few Americans sympathized with Pollard and a solid majority backed the imposition of a life sentence.

Conclusion

Given the changed nature of perceived threat in the post-Cold War world, counter-espionage efforts need to adjust in several ways. First, rather than seeing threat in terms of communism and/or the Soviet Union, one should emphasize that threat could come from changing and unexpected quarters. It may be from old rivals, new enemies, duplicitous allies, foreign terrorists, domestic radicals, or industrial spies. The very circumstance of uncertainty necessitates greater rather than lesser vigilance in security matters.

Second, one may need to deemphasize "threat" as the main rationale for maintaining security. Loyalty, obedience, and honesty could be given greater weight as reasons that secrets must be kept. In addition, professionalism and competence might be given more importance.

Third, security personnel must be aware that people are leery of threats to privacy, compromises of freedom of the press, and other challenges to civil liberties. Currently when balancing these concerns against military and foreign policy matters, most people are willing to give great weight to national security. But the public's attitudes result from a delicate balancing of these often competing interests, and ignoring or abusing civil liberties could help to tip the scale against the use of intrusive measures to protect national security.

Finally, just as you need to be responsive to changes in the technology of spying, you need to monitor, understand, and adjust to changes in public opinion. The trends we have followed and tried to project into the future will eventually shift in unanticipated ways as unexpected events unfold. In addition, new issues will emerge that may impinge on security matters in ways that we do not now foresee. To understand societal trends you need good raw intelligence in the form of surveys asking the right questions and good intelligence analysis to interpret the survey data. Understanding the climate of opinion will allow you to tailor your programs to best meet the security challenges of the 1990s.

Studies

ABC/WP:	ABC/Washington Post
AP/MG:	Associated Press/Media General
Canada:	Institute for Social Research, York University
CBS/NYT:	CBS/New York Times
CF:	College Freshmen, Cooperative Institutional Research Program, University of California, Los Angeles
Gallup:	Gallup Organization
Gallup-Teens:	Gallup Organization, Teen Survey
Harris:	Louis Harris and Associates
LAT:	Los Angeles Times
MFT:	Monitoring the Future, Institute for Social Research, University of Michigan
MORI:	Minnesota Opinion Research Institute
MOR:	Market Opinion Research
MS:	Market Strategies
NORC/GSS:	General Social Survey, National Opinion Research Center, University of Chicago
ORC:	Opinion Research Corporation
PAF:	Public Agenda Foundation
Roper:	Roper Organization
YANK:	Various Yankelovich organizations

The following tables have been selected from the comprehensive inventory provided by Dr. Smith for inclusion in these proceedings:

I. Trends in Attitudes

External Threat

CBS/NYT: Do you believe the military threat from the Soviet Union is constantly growing and presents a real, immediate danger to the United States, or not?

	Yes, Danger	No, Danger	DK	
4/1983	57%	37	6	(1489)
9/1983	63%	30	7	(1587)
1/1985	52%	39	9	(1525)
2/1985	54%	42	5	(1533)
9/1985	53%	39	9	(1277)
10/1987	31%	67	2	(1002)
5/1989	26%	65	9	(1073)

Note: 10/87 done by Marttila and Kiley

Various: How much of a threat would you say the Soviet Union is to the United States these days<197>a very serious threat, a serious threat, a minor threat, or not a threat at all?

	Very Serious	Serious	Minor	Not a Threat At All	DK	
3/1986	20%	47	25	6	2	(1148)
4/1986	13%	40	33	12	2	(1505)
5/1986	9%	37	40	12	2	(1506)
11/1987	15%	45	31	8	-	(1000)
1/1988	16%	41	32	8	-	(1000)
4/1988	17%	36	32	12	-	(1000)
5/1988	11%	37	39	12	2	(1500)
6/1988	18%	42	29	8	3	(1006)
12/1988	9%	35	44	10	2	(1000)
6/1989	9%	31	45	14	-	(1546)
2/1990	7%	26	49	16	-	(1000)

ABC/WP=1986-1987,5/88,6/89

MOR=1/88,4/88,12/88

YANK=6/88

MS=2/90

LAT: In your opinion, which of the following countries represent the greatest threat to the United States over the next ten years?

12/89	%
Soviet Union	24
Japan	16
China	14
Iran	8
Libya	4
Germany	2
Lebanon	2
South Africa	1
Other	11
DK	18
	(2095)

Government and the Military

NORC/GSS: I am going to name some institutions in this country. As far as the people running these institutions are concerned, would you say you have a great deal of confidence, only some confidence, or hardly any confidence at all in them?

Executive Branch of the Federal Government

	Great Deal	Only Some	Hardly Any	
1973	29.9%	51.4	18.7	(1469)
1983	13.3%	56.2	30.5	(1545)
1990	24.2%	51.9	23.9	(869)

Military

	Great Deal	Only Some	Hardly Any	
1973	32.6%	50.9	16.5	(1457)
1983	30.2%	56.4	13.4	(1548)
1990	33.6%	52.6	13.9	(873)

MFT: Now we'd like you to make some ratings of how honest and moral people are who run the following organizations. To what extent are there problems of dishonesty and immorality in the leadership of _____?

Large Corporations

	Not At All	Slight	Moderate	Consider- able	Great	No Opinion	
1975	2.4%	9.2	28.1	32.8	13.1	14.5	(2879)
1982	3.2%	17.7	35.0	23.0	7.0	14.2	(3330)
1989	3.3%	17.3	33.6	22.3	6.5	17.0	(2661)

The President and his Administration

1975	6.0%	14.0	19.4	24.3	25.4	10.8	(2867)
1982	4.5%	22.8	30.5	20.1	10.4	11.7	(3297)
1989	4.5%	20.8	27.2	23.0	9.6	14.9	(2643)

The U.S. Military

1975	7.6%	24.4	24.7	17.3	8.6	17.3	(2865)
1982	7.1%	27.7	25.8	14.8	8.5	16.1	(3280)
1989	7.0%	21.4	26.4	16.2	9.4	19.7	(2636)

MFT: Now we'd like you to make some ratings of how good or bad a job you feel each of the following organizations is doing for the country as a whole. For each one, mark the circle that best describes how you feel. How good or bad a job is being done for the country as a whole by _____?

Large Corporations

	Very Poor	Poor	Fair	Good	Very Good	No Opinion	
1975	8.5%	17.4	35.0	22.4	4.5	12.3	(2904)
1983	2.7%	9.6	33.6	31.1	7.6	15.4	(3332)
1989	2.6%	6.5	27.5	34.8	10.3	18.3	(2817)

The President and his Administration

	Very Poor	Poor	Fair	Good	Very Good	No Opinion	
1975	14.1%	18.3	36.8	16.6	3.3	10.9	(2903)
1976	11.0%	16.6	38.7	19.7	4.1	9.9	(2973)
1977	5.4%	8.1	31.5	31.2	10.2	13.5	(3106)
1978	10.1%	15.8	37.8	21.4	4.8	10.2	(3737)
1979	12.1%	20.0	37.7	17.4	3.7	9.1	(3261)
1980	16.9%	21.8	34.3	15.3	3.9	7.8	(3261)
1981	7.0%	9.4	28.7	30.8	12.0	12.2	(3609)
1982	14.7%	17.1	31.4	21.1	7.5	8.2	(3645)
1983	12.6%	16.4	31.2	22.8	8.3	8.7	(3335)
1984	7.8%	10.6	28.3	30.6	13.3	9.5	(3238)
1985	7.9%	10.1	27.0	29.3	16.6	9.2	(3238)
1986	5.8%	7.8	23.1	32.6	21.8	8.8	(3128)
1987	9.8%	13.9	30.6	25.4	9.8	10.4	(3323)
1988	8.7%	13.1	31.6	25.8	9.5	11.4	(3334)
1989	6.0%	10.2	32.1	27.4	9.0	15.3	(2812)

The U.S. Military

1975	4.9%	5.4	26.3	34.4	17.8	11.2	(2911)
1976	3.5%	5.5	24.3	34.8	19.6	12.3	(2978)
1977	3.2%	4.8	24.4	35.6	17.5	14.6	(3104)
1978	2.7%	4.4	25.0	34.6	18.6	14.8	(3728)
1979	4.2%	7.7	28.7	31.9	13.7	13.7	(3259)
1980	6.1%	11.4	28.5	29.1	11.2	13.7	(3247)
1981	4.9%	10.5	29.3	29.8	13.3	12.2	(3604)
1982	4.1%	6.4	25.7	34.2	16.6	12.9	(3638)
1983	3.2%	4.7	23.5	36.7	19.6	12.3	(3327)
1984	2.4%	3.2	22.2	36.6	24.8	11.2	(3238)
1985	2.3%	3.1	22.0	37.5	22.7	12.3	(3235)
1986	2.2%	2.1	15.8	37.2	29.2	13.4	(3115)
1987	2.3%	3.0	17.7	38.2	24.0	14.9	(3317)
1988	3.0%	2.8	19.3	37.8	23.1	14.0	(3329)
1989	2.8%	3.1	20.3	36.9	23.2	13.7	(2811)

Personal Values

Obedience

MFT: *These next questions ask your opinion about a number of topics. How much do you agree or disagree with each statement below?*

I feel that you can't be a good citizen unless you always obey the law.

	Disagree	Mostly Disagree	Neither	Agree	Mostly Agree	
1976	17.8%	16.7	17.2	35.1	13.1	(3011)
1977	19.2%	16.5	19.2	33.9	11.2	(3174)
1978	20.2%	16.8	17.0	34.2	11.7	(3762)
1979	17.6%	18.3	19.9	33.5	10.8	(3350)
1980	16.8%	16.3	19.1	35.8	12.0	(3282)
1981	17.7%	17.2	19.6	33.6	12.0	(3594)
1982	16.6%	17.8	18.3	34.5	12.9	(3657)
1983	19.0%	16.1	19.2	33.3	12.4	(3419)
1984	17.1%	18.4	19.5	33.1	11.9	(3277)
1985	19.2%	18.2	19.7	31.7	10.9	(3281)
1986	19.6%	18.3	21.1	30.4	10.5	(3150)
1987	20.1%	20.0	22.3	29.0	8.6	(3340)
1988	18.2%	19.1	21.1	30.7	10.9	(3366)
1989	18.2%	17.3	22.7	32.6	9.2	(2844)

I feel a good citizen should go along with whatever the government does even if he disagrees with it.

1976	42.0%	24.1	16.0	13.0	5.0	(3007)
1977	41.2%	22.9	16.1	14.3	5.5	(3171)
1978	43.2%	24.0	15.9	12.7	4.2	(3761)
1979	42.2%	24.9	15.5	12.8	4.5	(3350)
1980	36.6%	24.3	17.8	16.1	5.2	(3275)
1981	37.0%	24.8	15.8	16.5	5.9	(3593)
1982	37.6%	26.1	17.2	14.0	5.2	(3648)
1983	38.9%	24.8	17.9	13.0	5.4	(3419)
1984	39.6%	25.3	17.2	12.5	5.4	(3279)
1985	40.8%	23.8	17.3	13.3	4.7	(3278)
1986	39.0%	24.9	18.3	13.5	4.3	(3150)
1987	44.1%	25.5	16.3	10.6	3.5	(3341)
1988	40.9%	25.9	18.7	10.3	4.3	(3357)
1989	40.3%	25.3	19.1	11.5	3.8	(2841)

MFT: Servicemen should obey orders without question.

	Disagree	Mostly Disagree	Neither	Mostly Agree	Agree	
1975	16.5%	23.0	27.8	22.0	10.6	(2618)
1976	20.0%	22.1	18.7	26.4	12.9	(2972)
1977	19.6%	21.8	18.2	25.9	14.5	(3137)
1978	18.0%	21.2	20.4	26.7	13.7	(3717)
1979	17.3%	21.2	20.4	28.1	13.1	(3278)
1980	15.7%	18.2	22.1	28.7	15.4	(3259)
1981	14.0%	18.4	20.1	30.5	17.0	(3590)
1982	14.7%	18.2	21.7	29.1	16.3	(3612)
1983	13.1%	18.0	21.7	30.1	17.1	(3386)
1984	13.1%	18.8	21.2	29.6	17.4	(3254)
1985	14.7%	17.6	22.6	30.2	14.9	(3268)
1986	13.5%	18.9	22.2	28.6	16.8	(3109)
1987	13.5%	19.8	23.9	27.5	15.2	(3301)
1988	12.6%	19.2	25.4	27.3	15.5	(3295)
1989	14.2%	19.2	25.0	26.5	15.1	(2839)

Honesty

NORC/GSS: Which three qualities listed on this card would you say are the most desirable for a child to have? Which one of these three is the most desirable of all? All of the qualities listed on this card may be desirable, but could you tell me which three you consider least important? And which one of these is the least important of all?

	Most Desirable	Three Most Desirable	Not Chosen	Three Least Desirable	Least Desirable	
That he/the child is honest						
1973	35.9%	28.9	33.3	1.0	0.9	(1500)
1975	38.9%	31.4	28.1	1.4	0.2	(1481)
1976	38.2%	29.3	31.4	0.8	0.3	(1490)
1978	38.2%	30.9	29.5	1.0	0.3	(1520)
1980	40.1%	27.0	31.1	1.0	0.6	(489)
1980	33.1%	30.4	35.7	0.8	0.0	(487)
1983	36.0%	32.0	30.5	1.3	0.3	(1579)
1984	30.9%	28.9	38.5	1.3	0.4	(1438)
1986	24.7%	26.8	47.1	1.3	0.1	(716)

Gallup-Teens: At your school, how common is cheating on tests or exams? Would you say there is a great deal, a fair amount, or not very much cheating?

	Great Deal	Fair Amount	Not Very Much	DK	
1959	22%	60	18	-	(na)
1978	30%	42	26	2	(na)
1981	37%	39	24	-	(na)
1986	22%	44	30	4	(na)
1989	44%	34	22	-	(500)

Gallup-Teens: Have you, yourself, ever cheated on a test or exam?

	Yes, Have Cheated	
1978	62%	(na)
1981	66%	(na)
1986	59%	(na)
1989	54%	(500)

Individual Expression

MFT: How much do you agree or disagree with each of the following statements? People should do their own thing even if other people think it's strange.

	Disagree	Mostly Disagree	Neither	Mostly Agree	Agree	
1975	2.7%	3.9	11.1	41.3	41.0	(2761)
1983	2.7%	5.1	11.8	37.4	43.0	(3084)
1989	2.7%	5.5	10.4	31.8	49.7	(2643)

I get a real kick out of doing things that are a little dangerous.

1976	24.2%	21.2	24.8	20.5	9.3	(2721)
1983	23.0%	19.8	26.3	20.2	10.6	(3078)
1989	17.7%	15.1	27.2	24.9	15.0	(2647)

Privacy

Harris & NORC/GSS: How concerned are you about threats to your personal privacy in America today? Would you say you are very concerned, somewhat concerned, only a little concerned, or not concerned at all?

	Very Concerned	Somewhat Concerned	Only a Little Concerned	Not Concerned at All	DK	
1978	31%	33	17	19	1	(1256)
1982	45%	29	14	11	1	(1513)
1982	45%	29	14	11	1	(1504) ¹
1983	47%	30	15	8	0	(1506)
1990	46%	33	na	na	na	(2254)

¹NORC/GSS

Cambridge: Do you think we need new laws to protect personal privacy, or are existing laws adequate?

	Need New Laws	Existing Laws Adequate	DK	
1988	48%	37	15	(1471)
1989	50%	37	13	(1448)

Counterespionage

Wiretapping

GSS: Everything considered, would you say that in general you approve or disapprove of wiretapping?

	Approve	Disapprove	DK	
1974	17%	80	4	(1484)
1975	16%	80	4	(1490)
1977	18%	78	3	(1530)
1978	19%	78	3	(1532)
1982	19%	77	4	(1506)
1983	19%	78	4	(1599)
1985	23%	74	3	(1534)
1986	22%	74	4	(1470)
1988	20%	74	6	(983)
1989	26%	69	5	(1000)
1990	22%	72	6	(925)

NORC/GSS: Suppose the police get an anonymous tip that a man with a long criminal record is planning to break into a warehouse. Please circle a number for each question to show if you think police should be allowed without a court order to tap his phone?

	Definitely Allowed	Probably Allowed	Probably Not Allowed	Definitely Not Allowed	
1985	23.5%	22.8	24.9	28.8	(631)
1990	20.4%	28.5	26.9	24.2	(1113)

NORC/GSS: Now, suppose the tip is about a man without a criminal record. Please circle a number for each question to show if you think police be allowed without a court order to tap his phone?

	Definitely Allowed	Probably Allowed	Probably Not Allowed	Definitely Not Allowed	
1985	8.1%	13.9	26.4	51.7	(633)

Lie Detectors

Harris: If someone works in a government agency that uses classified information and there is a leak to the press, do you think it is or is not all right to make all those employees who handle the information take a lie detector test to learn who leaked the information?

	1978				
	Yes, Take Test	No, Don't Take Test	It Depends	Not Sure	
Public	58%	29	10	3	(1511)
Govt Officials					
Congress	27%	65	6	1	(77)
Law Enforcement	67%	24	7	2	(42)
Regulatory	17%	72	9	2	(53)

Harris: I will read you some practices that have been used by business organizations for different reasons. For each one I would like you to tell me whether they should or should not be forbidden by law. Please think of most jobs in business and government and not jobs that require security clearances or special moral qualities.

1978

	Forbidden	Allowed	DK	
Asking a job applicant to take a lie detector test.	62%	31	7	(1513)
Requiring an employee to take a lie detector test when there is suspicion of theft in his department.	43%	48	9	(1513)

AP/MG: How about if you were applying for a job and the prospective employer asked you to take a lie detector test? Would you object to taking it, or not?

1986

Would object	30%
Not object	65%
DK	5%
	(1512)

AP/MG: Some people say that lie detector tests are needed in certain circumstances to make sure people in sensitive positions are honest. Other people say that lie detectors are not always accurate and should not be used. Still others say that mandatory lie detector tests are an invasion of a person's right to privacy. I will read a list of circumstances in which lie detectors might be used. For each one, please tell me whether, in your opinion, lie detector tests should or should not be used.

1986

	Should	Should Not	DK	
For periodic testing of government employees who have access to classified information	81%	15	4	(1512)
For testing of employees suspected of stealing from work	75%	21	4	(1512)
For testing in court of people accused of crimes	72%	22	6	(1512)
For testing in court of witnesses	63%	30	7	(1512)
For periodic testing of all government employees	46%	49	5	(1512)
For testing of prospective new employees by companies that are considering hiring them	37%	55	8	(1512)
For testing of all current employees by their companies	27%	66	7	(1512)

Harris: As you know, the number of people caught spying in the U.S. has increased greatly over the past few years. As a way of trying to control the growth of spying in this country, would you favor or oppose...

1986				
	Favor	Oppose	DK	
Making most government employees who handle secret information regularly take lie detector tests	75%	24	1	(1254)

Drug Testing

Harris: In the following situations, do you consider it reasonable or unreasonable for employers to require someone with your job to take a scientific test for drug use?

1990				
	Reasonable	Unreasonable	DK	
In the application process, before being hired	83%	17	1	(2254)
If supervisors feel an employee's behavior shows signs of the effects of using drugs	65%	34	1	(2254)
In a randomized drug testing program for all employees	66%	33	1	(2254)

Gallup: The following is a list of some programs and proposals that are being discussed in this country today. For each one, please tell me whether you strongly favor, favor, oppose, or strongly oppose ____?

1987					
	Strongly Favor	Favor	Oppose	Strongly Oppose	DK
Mandatory drug tests for government employees	24%	41	22	8	6 (4244)

ABC/WP: I'm going to name some groups which some people have suggested should be required to take tests for illegal drug use on a regular basis. After each, please tell me whether you think they should be tested or not?

1989				
	Tested	Not Tested	DK	
Airline pilots	94%	6	0	(750)
Federal employees involved in national security areas	93%	6	1	(750)
Police officers	93%	7	0	(750)
Professional Athletes	88%	16	1	(750)
Members of Congress	87%	12	1	(750)
High school students	67%	31	1	(750)

Employee Screening

Harris: If someone is applying for a job, do you feel it would be appropriate for a prospective employer to (READ EACH ITEM), or not?

	1990				
	Appropriate	Not Appropriate	Depends on Job	DK	
Check to find out whether the applicant has a criminal record	80%	14	5	-	(1511)
Ask that the applicant take a written honesty test	55%	40	4	2	(1511)
Check into the applicant's lifestyle or political associations	12%	85	3	-	(1511)

Personal Information and Credit Checks

Harris: Do you agree or disagree with the following statements?

	1990	
Consumers have lost all control over how personal information about them is circulated and used by companies.	Agree	71%
	Disagree	27%
	Neither/DK	3%
	1990	
My privacy rights as a consumer in credit reporting are adequately protected today by law and business practices.	Agree	46%
	Disagree	51%
	Neither/DK	3%
		(2254)

Harris: Have you ever decided not to apply for something like a job, credit, or insurance, because you did not want to provide certain kinds of information?

	Yes, Decided Not to Apply	No, Did Not	DK	
1978	14%	85	1	(1496)
1990	30%	69	1	(2254)

Harris: When people (want to borrow money/apply for a credit card), do you think that the company (giving them credit/issuing the credit card) should be able to check on their credit records, or not?

	1990	
	Should be able	
Borrow Money	96%	
Credit Card	94%	
	(2254)	

Other Measures

Harris: *As you know, the number of people caught spying in the U.S. has increased greatly over the past few years. As a way of trying to control the growth of spying in this country, would you favor or oppose...*

	1986			
	Favor	Oppose	DK	
Conducting an investigation of the FBI (Federal Bureau of Investigation) and other intelligence agencies to find out why they have been so slow to find and crack down on spies	86%	12	2	(1254)
Cutting down the number of government documents classified as secret and top secret, so that the number of people with access to such secret material in government is sharply reduced	80%	17	3	(1254)
Firing managers in government operations who turn out to have spies working for them	63%	34	4	(1254)

Freedom of Information Act

Harris: *[Favor or Oppose] Cutting back on the access people have to government records about themselves and public officials under the Freedom of Information Act.*

	Favor	Oppose	DK	
1981	33%	63	4	(1252)

Roper: *The Reagan Administration thinks a number of government regulations and restrictions have gone too far. Here are some things they propose changing. (CARD SHOWN RESPONDENT) For each one, would you tell me whether you are in favor of it or opposed to it? First, changing the Freedom of Information Act so that the FBI, the CIA, and the Justice Department can keep all the information in their files secret.*

	Favor	Oppose	DK	
1982	36%	53	11	(2000)

Harris: *Do you agree or disagree that...federal freedom of information laws have gone too far in letting individuals and businesses get government documents.*

	Agree	Disagree	Neither	DK	
1990	58%	37	1	4	(2254)

Media Publication

Gallup: As a general rule, do you think the press is too quick to print classified information whether or not it might hurt the nation's security?

	1971
Yes	57%
No	30%
DK	14%
	(339)

ORC: Do you think the press should publish top secret government material once it comes into their hands, or should it be withheld until the government decides publication will not harm national security?

	1971
Should publish	14%
Should be withheld	76%
DK	10%
	(607)

ORC: Do you think "freedom of the press" includes the freedom of a paper to print stolen top secret government documents, or not?

	1971
Yes	15%
No	74%
DK	11%
	(607)

Harris: Now let me read you some statements that have been made about the case of the Pentagon Papers on the Vietnam War. For each, tell me if you tend to agree or disagree.

	1971			
	Agree	Disagree	DK	
In a democracy such as ours, it is necessary to tell the people the truth about how we got into the war in Vietnam, even if it means printing top secret documents, as long as they are not about today's situation there	53%	30	18	(1600)
One way to cover up past mistakes such as in Vietnam is to put "top secret" on all the documents and keep them locked up	40%	46	14	(1600)
Whenever a newspaper obtains a copy of a "top secret" government document, it should go to the government in order to get permission to print it	61%	24	15	(1600)
It is always wrong for a newspaper to print any document that has "top secret" stamped on it, even if it deals with the past and not the present	47%	38	15	(1600)

Harris: I will read you a few suggestions that people have made. For each, tell me if you would favor strongly, favor somewhat, oppose somewhat, or oppose strongly such a step be taken. The government should have the right to prosecute anyone who publishes materials that it classifies as secret.

1978

	Favor Strongly	Favor Somewhat	Oppose Somewhat	Oppose Strongly	Not Sure	
Public	48%	22	12	11	6	(1512)
Govt Officials						
Congress	19%	36	13	27	4	(77)
Law Enforcement	60%	14	19	2	5	(42)
Regulatory	25%	21	21	34	0	(53)

PAF: Freedom of expression means different things to different people, now I'm interested in what it means to you. I'll read you some statements about the right of freedom of expression, about what it protects and how far it goes. For each one, tell me whether you agree if this is a freedom of expression right or not. If you're not sure, just say so.

1979

	Agree	Disagree	DK	
A newspaper has a right to print top secret materials as long as it doesn't endanger national security	42%	47	11	(1000)

NORC/GSS: Suppose a newspaper got hold of confidential government papers about defense plans and wanted to publish them. Should the newspaper be allowed to publish them or should the government have the power to prevent publication?

	Allow to Publish	Prevent Publication	
1985	16.8%	83.2	(587)

Now suppose the confidential government papers were about economic plans. Should the newspaper be allowed to publish the papers or should the government have the power to prevent publication?

	Allow to Publish	Prevent Publication	
1985	61.3%	38.7	(586)

Gallup: Which of the following, if any, would you favor as a way of reducing news leaks that might affect national security?

	1986 ¹
Have a special unit in the White House to investigate leaks	34%
Requiring all senior officials to take lie detector tests on a regular basis	20%
Allow the Justice Department to block publication of information it feels threatens national security	46%
Other	3%
None of these	12%
DK	6%
	(1504)

¹ Percents add to more than 100% because of multiple responses.

Punishments

Capital Punishment

Roper: Opinions differ as to whether there should be a death penalty for certain very serious crimes, or whether there should not be a death penalty for any crime, no matter how serious it is, How do you feel--are you in favor of the death penalty for certain crimes, or opposed to the death penalty under any circumstances? If Favor: For which of these crimes, if any, would you favor the death penalty?

	1974	1976	1980
Kidnapping when the victim is killed	62%	57%	63%
Premeditated murder	60	59	67
A paid killing	58	56	64
Hijacking a plane that results in death	55	50	55
The killing of a policeman or prison guard	54	52	58
Assassinating a high public official	53	50	56
Blowing up a government building that results in death	53	49	56
Armed robbery that results in death	51	50	59
Arson that results in death	50	48	55
Treason, espionage	37	34	37
	(1984)	(2002)	(2002)

Gallup: Do you favor or oppose the death penalty for persons convicted of...

	1985			1988		
	Favor	Oppose	DK	Favor	Oppose	DK
Murder	75%	17	8	79%	16	5
Attempting to assassinate the President	57%	37	6	63%	33	4
Spying for a foreign nation during peacetime	48%	47	5	42%	50	8
Rape	45%	45	10	51%	42	7
Hijacking a plane	45%	48	10	49%	45	6
Drug dealers not convicted of murder	-	-	-	38%	55	7
	(1008)			(1001)		

Harris: As you know, the number of people caught spying in the U.S. has increased greatly over the past few years. As a way of trying to control the growth of spying in this country, would you favor or oppose...

	1986		
	Favor	Oppose	DK
Giving a mandatory death penalty to anyone caught selling or giving secrets to a foreign country	62%	36	2
	(1254)		

Pollard

CBS/NYT: Jonathan Pollard was convicted of spying for Israel. Do you feel angry, do you feel embarrassed, or do you feel sympathetic toward him? (IF MORE THAN ONE ANSWER, PROBE: What do you feel most strongly?)

	1987
Angry	48%
Embarrassed	12%
Sympathetic	7%
Other	7%
DK	27%
	(1045)

CBS/NYT: Jonathan Pollard was sentenced to life in prison for spying for Israel. Do you think that sentence was too harsh, too lenient, or was the sentence the right one?

	1987
Too harsh	16%
Too lenient	9%
Right one	57%
DK	17%
	(1045)

CBS/NYT: Which bothers you more--to learn that Israel spied against the United States, or to learn that once again Russia was caught spying against the United States?

1987

Israel	26%
Russia	46%
Both equal	15%
DK	13%
(1045)	

Differences in Attitudes by Age Groups^a

Disliking Russia (-4 and -5)

Age	Year			Change 90-73
	1974	1982	1990	
18-29	18.3%	41.1%	10.4%	-7.9
30-39	22.4	39.7	16.3	-6.1
40-49	30.5	46.4	16.0	-14.5
50-64	31.7	57.3	19.1	-12.6
65+	37.7	67.1	13.2	-24.5

Communism as a Form of Government (Worse Form)

	1973	1980	1990
18-29	29.8	50.4	43.1
30-39	46.0	49.0	57.8
40-49	43.6	59.4	43.7
50-64	51.9	65.8	56.1
65+	56.4	71.9	59.6

Defense Spending (Too Little Being Spent)

	1973	1982	1990	
18-29	8.5	51.0	10.1	+1.6
30-39	12.9	54.1	6.6	-6.3
40-49	12.3	60.3	16.7	+4.4
50-64	14.5	70.4	24.6	+10.1
65+	11.3	68.6	10.2	-1.1

^aFor details on question wording see the previous section.

Confidence in the Executive Branch of the Federal Government (Great Deal)

Age	Year			Change 90-73
	1973	1980	1990	
18-29	24.6	12.5	30.6	+6.0
30-39	29.9	9.1	20.2	-9.7
40-49	29.1	12.3	17.1	-12.0
50-64	31.4	12.4	24.8	-6.6
65+	38.5	17.1	29.0	-9.5

Confidence in the Military (Great Deal)

	1973	1980	1990	
18-29	24.6	26.6	39.8	+15.2
30-39	31.5	20.6	30.3	-1.2
40-49	32.1	29.1	26.6	-5.5
50-64	37.6	35.5	35.0	-2.6
65+	42.1	34.6	36.6	-5.5

Obey Law (Should)

	1985
18-29	35.0
30-39	34.5
40-49	35.1
50-64	53.6
65+	54.9

Privacy (Very Concerned)

	1982
18-29	51.7
30-39	46.9
40-49	49.4
50-64	49.2
65+	50.6

Wiretapping (Approve)

Age	Year		
	1974	1982	1990
18-29	14.7	13.9	25.8
30-39	18.4	16.3	23.6
40-49	18.8	21.5	15.9
50-64	20.4	18.8	22.4
65+	14.5	20.0	28.7

Tap Phone of Criminal (Allow)

	1985
18-29	39.1
30-39	38.5
40-49	47.6
50-64	55.0
65+	51.3

Tap Phone of Non-criminal (Allow)

	1985
18-29	17.9
30-39	18.7
40-49	23.5
50-64	28.1
65+	21.2

Papers Publishing Confidential Economic Plans (Allow)

	1985
18-29	65.5
30-39	64.5
40-49	64.6
50-64	54.4
65+	57.1

Capital Punishment for Spies in Peacetime (For)

	1985
18-29	40
30-49	42
50+	59

Capital Punishment for Murderers (For)

	1990
18-29	80.6
30-39	79.7
40-49	75.7
50-64	78.4
65+	82.2

References

- Anderson, David A., "Spying in Violation of Article 106, UCMJ: The Offense and the Constitutionality of Its Mandatory Death Penalty," *Military Law Review*, 127 (Winter, 1990), 1-61.
- Astin, Alexander W.; Korn, William S.; and Berz, Ellyne R., *The American Freshman: National Norms for Fall 1989*. Los Angeles: Higher Education Research Institute, 1989. [similar volumes for 1966-1988]
- Bachman, Jerald G.; Johnston, Llyod D.; and O'Malley, Patrick M., *Monitoring the Future: Questionnaire Responses from the Nation's High School Seniors*. Ann Arbor, MI: ISR, 1987. [similar volumes for 1975-1985]
- "Civil Liberties and National Security: A Delicate Balance," *Northwestern University Law Review*, 68 (Nov./Dec., 1973), 922-941.
- Davis, James A. and Smith, Tom W., *General Social Survey, 1972-1989: Cumulative Codebook*. Chicago: NORC, 1989.
- Dimensions of Privacy: A National Opinion Research Survey of Attitudes toward Privacy*. Stevens Point, WI: Sentry Insurance, 1979.
- The Equifax Report on Consumers in the Information Age*. Atlanta: Equifax, 1990.
- Fletcher, Joseph F., "Mass and Elite Attitudes About Wiretapping in Canada: Implications for Democratic Theory and Politics," *Public Opinion Quarterly*, 53 (Summer, 1989), 225-245.
- Katz, James E. and Tassone, Annette R., "Privacy and Information Technology," *Public Opinion Quarterly*, 54 (Spring, 1990), 125-143.
- Halperin, Morton H., "National Security and Civil Liberties," *Foreign Policy*, 21 (Winter, 1975-76), 125-160.
- Halperin, Morton H., "Secrecy and the Right to Know," *Law and Contemporary Problems*, 40 (Summer, 1976), 132-165.
- Shils, Edward A., *The Torment of Secrecy: The Background and Consequences of American Security Policies*. Glencoe, IL: The Free Press, 1956.
- Smith, Tom W., "American Attitudes Toward the Soviet Union and Communism," *Public Opinion Quarterly*, 47 (Summer, 1983), 277-292.
- Smith, Tom W., "National Service," *Public Opinion Quarterly*, 54 (Summer, 1990), 273-285.
- Smith, Tom W., "Red in the Morning: Recent Trends in American Attitudes Toward the Soviet Union and Communism," *The NORC Reporter*, 1 (Winter, 1987), 4-5.

Mr. Snider is general counsel for the U.S. Senate Select Committee on Intelligence where he serves as principal legal advisor to the committee, drafting legal opinions and providing legal advice to the chairman on a variety of issues.

Changes Shaping the Security Awareness Landscape

Comments Preceding the General Discussion

by L. Britt Snider

I was particularly intrigued with the title of Maynard Anderson's presentation, "Geopolitical Trends." When was the last time we had a security conference to talk about geopolitical trends? My guess is that it was probably before World War II because we basically have been relying on the same geopolitical factors for the last 40 years in terms of justifying our security policies. It's been the Soviets, and their Eastern European allies who have been our principle concern, and to a lesser extent, China. From time to time we have had assorted Third World protagonists, Libya, Cuba, Iran, and most recently Iraq, of course.

Now we read in the newspapers that the West is about to consider aid to the Soviet Union, in a sort of Berlin airlift in reverse. And the Poles are asking if they can buy the F16 fighters. You have the Czechs, Hungarians, and Russians, all clamoring for most favored nation status. Incidentally, the Chinese have had it since 1980, notwithstanding Tienamin Square and those developments. The world is dramatically changing and I think Maynard is correct in noting that this is far from bottoming out. No one really knows what is going to happen in the Soviet Union. Are they going to hold this union of socialist republics together? Are they going to have more conflict in the Soviet Union? Is Gorbachev going to be able to stay the course there? I think there's probably less concern about the East European countries in terms of changing their political course, but their economies are still basket cases for the most part. How much economic pressure does it take before revolutionary political changes take place in those countries? I don't think we can rule that out. And what about developments in the Soviet Union and their impact on Eastern Europe? There's a lot to come clear here, not to mention the Persian Gulf, the conflict we're going to see there. What is our role in the Persian Gulf going to be after all this is over—after Kuwait itself is resolved? Not to mention the threat from those who claim to be our friends. For example, what are the implications going to be of a united Germany, both in political terms and economic terms? What sort of threats do

we see from Japan in terms of economic competitiveness in pre-empting the influence of this country?

All these things are up in the air. I heard Admiral Bobby Inman speak the other night, and he said he had never known such an era of uncertainty in his lifetime. And I think that's precisely true. It's very difficult, I think, to make decisions in this environment, and I'm talking about not only the "big picture" decisions, but things like security policy and security awareness programs which are affected by this. You have both in Congress and the Executive branch a debate going on about what to do with defense resources. What do we do with intelligence programs that have been targeted basically at the Soviet Union and Eastern Europe for the last 40 years? Where should we be putting these resources? How far we can go in arms control and how much should we be willing to commit to? Foreign assistance? We can just go on and on in terms of problems in the national security area that are essentially waiting for some sort of certainty to develop.

Counterintelligence is another issue—close to home for this group. We had a bill which was introduced in the last session in Congress—we held hearings on it in our committee—to make a number of statutory changes to tighten up our security. I don't know whether you are aware of this project or not. We had a lot of letters from people saying why are you doing this now? What's your point here? We don't need to worry about espionage anymore, so why are you guys doing this? It's a situation that we have to deal with. It may be simply logical to tighten up wherever flaws that we may see in the statutory system. But, we need some political steam to make this whole process work. And yet, uncertainty seems to be taking the political steam out of the engine. I think that we're likely to live with this for quite some time. I think we would like to have a firmer, surer basis for making those kind of decisions, but I don't see it coming any time soon.

What are the consequences, then, for security awareness? Dr. Tom Smith told us that changing public perceptions are having an impact. The public does see espionage as less of a threat—they do see less justification for obtrusive security measures. He suggested that we start emphasizing reasons other than a threat, to justify why classified information needs to be protected. Maynard in essence said something similar. I don't know. Perhaps we can discuss this a bit more. In order to explain the threat, I think we need to describe or explain how it's changed, and concede all of our uncertainties. I still think we have an espionage threat that's real without doubt. Will these changes in public attitudes really translate into a greater incidence of espionage? I don't think we really know the answer to that.

Maynard suggested in his remarks that perhaps with more contact with our former enemies being permitted, with more communications between us, the operating environment has been loosened up considerably for them, or

will be in the future. So can we expect more espionage? I don't know, we may or may not.

I think, for example, that people who have clearances now and are considering espionage have to realize that they might be received far less warmly than they have been in the past by the Soviets, or by any other Eastern European government. They might not be paid so much for the risks that they're taking. I think these are hard factors that are going to enter into people's calculations. I'm not saying that there won't be espionage—there will always be espionage. I'm just wondering whether we can expect a climate that's more conducive or less conducive. I'm not sure. I'm not sure that the evidence is really in. As far as I know we don't have a case yet, a post-Cold War espionage case. I will be interested in the first one that comes along to see what the facts are, but right now we are operating just on what seems logical.

So what do we do with this situation in terms of improving our program? I think Steve's message to us was that we can certainly can do better than we have been doing. There is certainly a lot of room for improvement in the 90s. I think that he's exactly right. I think it's also going to be even more difficult, maybe twice as difficult as it's been in the past, largely because of the uncertainty. It's very difficult to make a very convincing case to people to take security seriously when there are so many unknowns, when there are so many variables in terms of our national security and the threat.

Certainly, I think you need to keep your message current; keep it objective. I think we have all sat in before on a number of security briefings where the briefer just loses the audience; his presentation is so rote and so out of date, so unrelated to reality, that he ends up alienating the people being briefed because they resent wasting their time on this sort of presentation. It would be interesting for me to know just how often security briefings are being updated—the FBI's DECA's briefing, the Army SAEDA briefing, or the briefing DIS gives contractors. They need to be continuously updated, reviewed and made more relevant, every single time that they're given to an audience. People ought to think about who they are talking to before giving a presentation. It seems to me that if you can't do it right, it's better not even trying, because I think it can end up being very a counter-productive exercise and lowering rather than raising the appreciation for security matters.

Also, we need to think more about who needs to be briefed. I'm not sure that, as things progress, it's going to remain necessary that we reach with these kinds of programs everyone who has a clearance. Particularly in the face of diminishing resources it seems to me that we're going to have to start prioritizing the people we need to reach with this kind of subject. It seems to me that as the military threat itself recedes, there's going to be less attention paid to people who have access to order-of-battle information, readiness, and

information about that sort of thing. And on the other hand, there will have to be more of a focus on people with access to high-tech weapon systems, where they are been developed, or produced, or deployed in the field. We need to reach the people that are in these programs. We need to reach people in special access programs.

I understand that Ev Gravelle was telling you earlier this morning that they have finally begun at DODSI a training program for SAPs. This is really a tremendous step forward in terms of bridging this gap between the compartmented and collateral security worlds. We have too long, it seems to me, been keeping the two separate. As a result we have been applying fewer resources to the protection of information that is probably the most sensitive, and more resources to that which is less sensitive. I'm glad to hear that Ev has got this training program going.

Discussion moderated by L. Britt Snider, General Counsel,
Senate Select Committee on Intelligence

We have selected the following transcribed excerpts from responses of the panelists in this section to questions from the floor.

Question: With the change in the status of the Warsaw Pact and the Soviet Union, what changes are we likely to see, and how soon, in the designated country list?

Mr. Anderson: It's being reviewed and probably the list's name will change.

Mr. Snider: This is true and I may add I hear from Justice and the FBI that they are looking at a slightly different concept, by which they can put some of their counter-intelligence resources against a problem without a country being specifically on a criteria country list. I think this is an excellent step forward, but as I said, this is still being reviewed at Justice.

Question: This is a question to Maynard Anderson about the idea of identifying information by value. Isn't that something which classifiers have been doing or are supposed to be doing?

Mr. Anderson: I think it's what they are supposed to have been doing, but classification has become a process that hasn't been very effective. If you went out and took a look at what is being classified in the Department of Defense, you would find a great many things are being classified that should not be protected. I maintain that potential damage is very difficult for an original classifier to determine, given the fact that we are in an era of quick and unforeseen change. I do believe that an original classifier can look at a piece of information and say "this is valuable to the project, the government, the economy, the military, or whatever else is in the national interest", and it is much easier for him or her to make the decision on the basis of value and cost than it is to say that this is going to, now and in perpetuity, cause serious damage to the United States. I think there is an element there of judgment or decision-making that doesn't exist under the arbitrary standard.

Mr. Garfinkel: The problem that I have with the value standard is that the value standard suggests that we need to quantify potential damage. With the current standard for classifying, the threshold for classifying is "reasonably could be expected to cause damage to the national security." The question that I ask is, "What does that mean quantitatively?" I think we would all agree that for the classifier, if he or she were able to say that the

chance of damage to the national security is greater than 50 percent, then the item should be classified. But what is the cut-off point if we are looking for a quantitative standard? If we say that 60 times out of 100 there won't be damage to national security but 40 times out of a hundred there will be damage, do I need to classify it? Well, I think most classifiers today are classifying information that more likely than not will not damage the national security, but that possibility still exists. So the problem I have with the value system is that I don't know where to draw the line quantitatively and I think "value" suggests that we must do that.

Mr. Snider: There is a widely held belief in Congress that too much is classified and improperly so and every time you raise some kind of proposal that would contribute to security in a positive way, there is a full chorus over here saying, "What about all of this stuff that shouldn't be classified in the first place?" This is a basic misperception on their part but, nevertheless, it's a real problem that we have to contend with.

Question: I heard a comment earlier having to do with what I conceive to be a need within the security arena for something that has a close resemblance to Total Quality Management in terms of focusing on requirements, looking at customer needs, and then measuring effectiveness.

Mr. Garfinkel: I think Total Quality Management is a restatement of somebody saying "Let's use some common sense." But common sense is something we often lose when someone comes up with highfalutin' theories about how something should be structured or organized. I think all of us this morning were trying to say a little bit about that. For example, as I said in my presentation, it was my common belief that security education would cure any problem in security awareness. But this may not always be true, so we have to use some common sense. Where is it that we have failed, or what is it we haven't tried?

Mr. Snider: But, Steve, you mentioned in your presentation that basically you have no way of measuring the impact of these programs other than by a few anecdotes. It seems to me that this is a key thing for this conference to focus on—how do you evaluate impact?

Mr. Anderson: Our measure of impact in the past has been the presence of deficiencies and espionage cases.

Mr. Garfinkel: Although it may not be an important indicator as espionage or unauthorized disclosures, when we look at the classified product of an agency and count up the number of discrepancies per classification action, we

get a pretty good means of judging one agency against another, and the differences we see among the agencies are absolutely phenomenal. We will go to some agencies and look at several hundred documents and will find two or three discrepancies and that will be routine for that agency. Our overall government figure, however, is almost one discrepancy per two documents or two classification actions. That means in some agencies for each document you will find three or four things wrong. You can determine by this measure, at least in our area of activity, where there is good security awareness.

Question: A question for Mr. Anderson: In light of recent developments in the world how can we now characterize the hostile intelligence threat with reference to security education and awareness for a cleared population which is inclined to believe that the threat is no longer there?

Mr. Anderson: During the last 40 years we have been talking about hostile intelligence threats. We've forgotten that the statute doesn't say "hostile," the statute says "foreign," and I think that the perception of a "hostile" threat will have to change. When you classify information in order to protect it, you don't protect it merely from a hostile threat, you protect it from anyone who is not supposed to have access to it. We forgot that, but if we remember it, I think we will end up with less classified material—because we will be making a serious determination in each case. But I think that public opinion is important. I think that public opinion is important for us to understand—not necessarily whether or not we should classify because the public says we should or shouldn't. But I think it is important in terms of security awareness since we have to understand how to deal with public perceptions.

Strategies for Improving Security Awareness

Marketing Techniques

Robert Bailey, Executive Vice-President, Director of Marketing Services,
BBDO

Training Approaches

Henry M. Halff, Chief Scientist, Halff Resources, Inc.

Program Evaluation

Robert O. Brinkerhoff, Department of Educational Leadership, Western
Michigan University

Discussion

Moderator Richard S. Elster, Dean of Instruction, Naval Postgraduate School

Dr. Bailey is executive vice president and director of marketing services at BBDO advertising agency in Chicago. He has been with BBDO for 17 years and is responsible for the agency's Marketing Research Department.

The Role Of Advertising in Promoting Security Awareness

by Robert Bailey

This session is devoted to strategic tools for improving security awareness. The strategic tool I want to talk about is advertising and its potential role in promoting security awareness. I want to begin by absolutely assuring you that my intent is not to promote my own advertising agency. There are other audiences with whom I try to do that. Instead, my intent, I hope, is more lofty. I want to show you that advertising can be an important strategic resource to help you improve security awareness.

My agenda is as follows. First, a brief introduction. Second, a discussion of public issue advertising and how it motivates people to change their behavior. Third, a look at how the U.S. Government currently uses advertising. Fourth, a look at how advertising can be used to promote security awareness. And finally, a short conclusion.

Introduction

The challenge, some say, is to increase security awareness. And that's important. But, rest assured, awareness isn't enough. You need to move beyond awareness to persuasion. I'm told the old approaches aren't working well enough. There are too many cases of espionage. No one wants another case such as that of John Walker. He sold defense secrets for 18 years without anyone becoming suspicious and reporting his activities to a security officer.

I want to suggest to you the odds that a suspicious activity will be reported can be substantially increased. The tool to increase these odds is advertising. Highly targeted advertising can be a powerful way to promote security awareness.

Public Issue Advertising

The kind of advertising you need is not product advertising. You need a type of non-product advertising that we call Public Issue Advertising. Therefore, I would like to discuss public issue advertising. The examples (shown

during the symposium) were provided by The Advertising Council. The Ad Council is a volunteer organization that was formed after the attack on Pearl Harbor. At that time the president called together the heads of top advertising agencies. He asked them to mount advertising campaigns to get the people on the home front behind the struggle on the battlefield.

The campaigns were so successful that after World War II the agencies decided to stay together and do public service advertising. The first campaign that was not war-related was Smokey Bear. Since Smokey Bear, our industry has learned a lot about public issue advertising. We've learned that it stimulates awareness, action, and change. We've learned that public issue advertising mobilizes people to deal with issues that impact society.

Public issue advertising has increased funding for African-American colleges. The advertising theme, "A Mind is a Terrible Thing to Waste," has helped more than double fundraising levels for the United Negro College Fund. As a consequence, there are over 48,000 Black students who, without these funds, could not have afforded to go to college.

Public issue advertising also helps recruit new teachers. Phone calls to the 800 number shown in the Ad Council's teacher recruitment commercials now total 20,000 per month. And over a third of those who call take further action toward becoming teachers.

Public issue advertising has also discouraged drinking and driving. Since the Ad Council's campaign started, the percentage of drivers who are intoxicated has decreased significantly. Most gratifying of all, the biggest decrease has been among teenagers who are the main target audience for the campaign.

Public issue advertising is proving effective in recruiting nurses. Since the Ad Council's campaign began, calls to the 800 number shown in the commercials are coming in at the rate of 8,000 per month. And, a soon-to-be-released study shows that attitudes about nursing as a career have improved. In fact, this campaign may have to be stopped for awhile because more students have become interested in nursing than the nursing schools can accommodate.

My message to you is straightforward. Public issue advertising is a catalyst for change. If advertising can get people to change their drinking habits, contribute their money, or even change their careers, then it can certainly motivate people to report suspicious activity regarding defense secrets.

Why is public issue advertising so successful? Let me assure you that it is not because we in advertising have some secret weapon. All we possess is our insights into what will motivate people and our ability to turn those in-

sights into creative advertising. [Examples of advertising created by the volunteer agencies participating in the Ad Council were shown to the audience.]

U.S. Government's Use Of Advertising

The Ad Council isn't the only group that produces good advertising. One of the major U.S. advertisers is the Federal government. Since the U.S. government would be the key force in deciding whether advertising is the right tool for promoting security awareness, it seems appropriate to examine how the government is already using advertising. The bottom line is that the U.S. government is currently one of America's largest advertisers.

In 1989 the U.S. government's advertising budget exceeded \$300 million. And that reflects more than a doubling of the amount the government spent a few years earlier. The U.S. government now invests more in advertising than does IBM, United Airlines, General Electric or Hallmark. Clearly, the government has become a big-time advertiser. Several U.S. government units have found they have a legitimate need for advertising. These units include the Post Office, the U.S. Mint, and the various branches of the Armed Forces. The Armed Forces' recruitment budget represents a major portion of government advertising. It is probably fair to say that this advertising has helped make the volunteer army possible.

My purpose in talking about the U.S. government as a major advertiser is to make the point that the government is experienced at managing advertising. The expertise needed to manage a security awareness advertising campaign already exists within the Defense Department. I think the most important demonstration of this expertise is in the quality of the advertising that has been created. [Examples of federally-funded advertising were shown to the audience.]

Advertising To Promote Security Awareness

Advertising can do more than help with military recruitment. It can also help promote security awareness. That's the heart of my talk. And that's what I would like to address now.

Developing advertising has become a highly complex process. It's probably become overly complicated. After all, advertising is hardly rocket science—a subject with which some of you are conversant. There are five simple steps to follow in getting good advertising. If you do a competent job at each step, the ultimate results are likely to be highly satisfactory. The steps are as follows:

- First, decide on the purpose of the advertising.

- Second, develop an advertising strategy.
- Third, create an advertising campaign.
- Fourth, run the campaign in appropriate media.
- Fifth, evaluate the campaign's effectiveness.

Now that you are familiar with the five steps, let's discuss each step with emphasis on its relevance to creating a security awareness campaign.

The first step is to ***decide on the purpose of the advertising***. This is the most fundamental decision an advertiser makes. And, the most common mistake is to either fail to define the purpose or to define the purpose too broadly. It is critical that you specify ***exactly*** what the advertising is supposed to do.

Let me illustrate this with an example from the Amtrak campaign for the New York to Washington route. The wrong way to define the purpose of the advertising is to say "Take Amtrak between New York and Washington." Why is this wrong? Because it does not specify who the enemy is. It doesn't say what mode of transportation Amtrak should replace.

The right way to specify the purpose is to say "Take Amtrak instead of a plane between New York and Washington." The right way of stating the purpose tells the advertising agency who they must sell against in order to get people to take the train. This important refinement to the purpose of the Amtrak advertising had a major and a constructive impact on the advertising which resulted.

If you are advertising security awareness, I think it would be a mistake to define the purpose of the advertising as being to "make people more security conscious." Such a statement is too vague. A better formulation would more precisely state the behavior we want to elicit from the prospect. One reasonable way to define the purpose of security awareness advertising would be to say it is "to persuade people to inform the appropriate security officer immediately if they see suspicious activity."

Step two in getting good advertising is to ***develop an advertising strategy***. An advertising strategy is a blueprint for the development of advertising. I cannot emphasize enough how important the strategy is. It is the final instructions you give the creative people who write your commercials. The creative people will later return to you with storyboards that translate your strategy into imaginative advertising. But no matter how superb the advertising they do is, it will probably ultimately fail if you have given your creative team a weak, unmotivating strategy.

Despite my rhetoric, you may be a doubter and say, "Why have a strategy?"

I believe the most eloquent answer to that question was provided by the late Bill Bernbach who was the creative great who did the original VW beetle advertising. In explaining the need for strategy, Bernbach said, "A great talent, sailing in the wrong direction will, like the lost pilot breaking the speed record, reach the wrong destination all the more quickly."

An advertising strategy statement is usually one page long. It's brief. In case you haven't noticed, a lot of other important documents are also only about a page long. For example, there are the 10 Commandments, the Bill of Rights, the Apostles' Creed, and the Gettysburg Address. Like them, your strategy should not be longer than a page. Otherwise, it will be longer than the advertisement or contain more words than the commercial.

The advertising industry follows a fairly standard format for strategy statements. There are usually five parts. First, the objective or purpose of the advertising is stated. Second, the strategy which is the key idea we want the prospect to understand is stated. Third, the strategic support points which are the reasons why the prospect can believe the strategy are listed. Fourth, the target audience is defined. And fifth, the emotional tonality desired in the advertising is specified.

Let me share an example of a strategy that was used several years ago by the Kemper Group. Kemper sells many kinds of insurance as well as financial products such as money market funds and mutual funds. Kemper wanted a corporate advertising campaign which would cover both insurance and financial products. The chairman at Kemper said the objective of the advertising should be to make more people aware of the Kemper name and logo. The strategy became to position Kemper as offering the consumer financial peace of mind. There were two support points. First, Kemper can give you financial peace of mind because it offers you both sound insurance products and solid investment products. Second, as a consequence of Kemper's expertise you can have protection for today through insurance and opportunity for tomorrow through investment products. The target audience was broad—consumers, prospects, producers, and brokers. It is fairly common in corporate advertising to have a broad target audience. The tone for the advertising was defined to be trustworthy and human. This tonality fits well with positioning Kemper as offering people financial peace of mind.

Now let's look at the commercial that was created based on this strategy statement. Please notice how the creative team worked to achieve the objective of name and logo awareness by keeping the logo on screen throughout the commercial. Also, notice how they sought to communicate the strategy

and the support points while maintaining the desired tonality. [Kemper commercial was shown.]

A strong strategy statement does several things. One of the most important is to define who the prime prospect is. This definition is contained in the target audience line. Another thing the strategy statement does is to identify the strongest motivator. This is contained in the strategy section. Both defining the prime prospect and identifying the strongest motivators are important to security awareness advertising. Therefore, let's discuss each of these a little more.

First, let's turn to defining the prime prospect. I think the prospect for security awareness advertising is fairly clear. It is anyone who has access to defense secrets. But, that's a class of people and doesn't really tell us very much about the flesh and blood human beings who make up the category.

We must get beyond categorization to understanding. Creating good advertising requires an empathy for the people you are trying to reach. As Phil Dusenberry, BBDO's creative director says, "The prime prospect is a person, not a statistic."

Therefore, we need to understand the prime prospect's relevant problems, aspirations, values and feelings. Only with this kind of understanding can we expect to persuade the prospect to take the action we hope he will decide to take.

Let me show you an example of creative work that I believe demonstrates an understanding of the prime prospect. The example comes from the Drug Free America campaign. The prime prospect is not a current or prospective drug user. Instead, the prospect is the parents of children ready to enter their teen years. The objective is to motivate parents to talk with their children about the dangers of drug abuse. I believe the creative team did an outstanding job of showing parents the possible ultimate consequences of not talking with their kids about drugs. [Drug Free America commercial was shown.]

Next, let's consider how we might go about identifying the strongest motivators for security awareness advertising.

We know a lot about why people give defense secrets away.

People give secrets away because of greed, debt repayment problems, revenge, drugs, ideology, sex, to protect relatives who are foreign nationals or for reasons of mental instability. And there are a few other reasons. We know quite a bit about why people give secrets away. But we don't know what would motivate people not to give away defense secrets. Fortunately,

the group who gives secrets away is tiny. ***Advertising is probably not a cost-effective way to reach the tiny "at risk" group. The bigger challenge is to get all people with security clearances to always report suspicious activity promptly.***

Advertising can help meet this challenge. The group of people with security clearances runs to several million. This is a big enough group to warrant a highly targeted advertising effort.

But doing effective security awareness advertising won't be easy. Some long-held attitudes will have to be overcome. For example, many people believe too much information is classified. It's not easy to get people to meet the objectives of security awareness programs if they believe you're engaged in classifying lots of trivial information. Also, there is a long-cherished American attitude that you mind your own business. This means that you don't turn your friend, neighbor, or colleague in to the government. The hurdles facing security awareness advertising are such that a routine approach which rehashes old facts probably won't work.

To be effective, security awareness advertising would need to appeal to both reason and emotion. Reason is needed because the prospects are intelligent and must be convinced that there is a rational basis for what we are asking them to do. The advertising will most certainly need to be ***emotionally*** motivating. After all, we are asking people to "tattle," and that's a difficult thing for most of us to do. Consequently, some pretty emotionally compelling advertising would be needed.

The prospect's net impression from security awareness advertising should be twofold. At the rational level, the prospect should say "***I understand it and what they want makes sense.***" At the emotional level the prospect should say "***I believe in what they believe in. I believe it's important. And, I believe in it so strongly that I'm going to take the action they request.***"

A key challenge for security awareness is that the issue is *old*. Americans with security clearances have lived with the issue through forty years of cold war. It's stale. And, it's probably greatly diminished in importance to people as the cold war has diminished.

An old issue about which there is little new to say can become an uninteresting issue. Not only is our issue old, it's less important. People aren't as likely to get excited about Saddam Hussein as they are about hostile Soviets who have nuclear warheads pointed at America's cities. The new threats are real. But they aren't of the same magnitude.

After 40 years of Cold War, what more is there for the prospect to know about security awareness? Ask yourself, why should the prospect voluntarily spend time and attention on communications about security awareness? Prospects only perceive what is interesting and relevant. Therefore, I believe security awareness advertising must move beyond reciting the same old facts to emphasizing new facts and emotion.

Advertising research can help identify how to motivate people to report suspicious activity. I could talk at length about how existing marketing research technology could help you identify the strongest appeals. But that's a different speech. Suffice to say that market researchers have a tool kit of proven techniques to help identify the strongest appeal.

In the absence of research, let me offer what may be a controversial hypothesis. I think the old motivational appeals may not be worn out. They may only need to be made contemporary in their means of expression. It is true, of course, that many American attitudes and values have changed. Old-time values regarding sexual habits, the role of women and relations between the races certainly seem to have changed. But, because some old-time values may have changed does not mean all old-time values have changed.

I think there may be compelling emotional motivators in the area of security awareness. They include patriotism, the preservation of freedom, the protection of Americans, and a fundamental sense of responsibility and duty toward our country.

While some of these motivators may have diminished during this Age of Me, nevertheless I hypothesize that these motivators are still strong enough to be the basis for security awareness advertising.

Perhaps the strongest motivator of all may be to get prospects to understand the ultimate consequences to others of not reporting suspicious activity. If you realize that other Americans may be killed because you were thoughtless about failing to report suspicious activity, it can make you think twice. Effective security awareness advertising will require that we sort through the possible emotional motivators to find the most compelling one. ***Then the advertising should point out to the prospect the emotional reward he will get for doing the right thing.***

Step three in getting good advertising is to ***create an advertising campaign***. It's where the magic happens. Some of you come from scientific backgrounds. And almost all of you come from analytical backgrounds. But those skills don't do much to help you create great advertising. It's art. Not science. It's imagination. Not analysis. There are no logical deductions. If anything, creativity is inductive. It's where showmanship and salesmanship go hand in glove. There are no rules. There is no manual. There are only

results. Creative ideas that change the way people think and act. Logic, analysis, and thinking don't change imagination. But ultimately imagination changes our ways of thinking. That is the power of advertising. To illustrate this, let me show you some recent creativity from BBDO. [BBDO examples were shown to audience.]

Step four is to ***run the campaign in appropriate media***. Security awareness advertising should obviously not be placed in broad-based consumer media. There would be too much waste and expense. You need to reach a highly targeted prospect group. Consequently, security awareness advertising should be in media such as armed forces TV, radio, newspapers. And employee newsletters and magazines published by defense contractors. Posters and handouts at work should be a major media vehicle.

Step five is to ***evaluate the advertising campaign***. This is important. Smart advertisers try to find out what the return on their investment is. There are probably two principal pre/post evaluative tools for security awareness advertising. The first tool is to conduct surveys of advertising awareness and communication. This tells you if the prime prospect got the message. The second tool is to look at the number of suspicious activities reported. This tells you if the advertising motivated people to act.

Conclusion

Over the past 45 minutes I've discussed how advertising might be used by those of you charged with selling security awareness. In 1939, President Roosevelt set the precedent for using advertising to promote security awareness. Here are a few of the posters from the famous "Loose Lips Sink Ships" campaign. [Slides of posters from "Lips" campaign were shown to audience.]

In the 1990s I believe advertising can again be a powerful tool to promote security awareness. Today your challenge is somewhat different. But advertising is continuing to be an appropriate tool. Therefore, I hope I've stimulated you to think about how advertising can help you meet the new security challenges we face.

You are an intelligent and an attentive audience. I wish you the best in your important mission. And I thank you.

Dr. Halff is a research psychologist with over 20 years of experience in learning, instruction, and instructional technology. His interest is in computer-based instruction and applied aspects of cognitive science. In 1984 he founded Halff Resources, an independent consulting firm offering services to the education and training community.

Approaches to Security Education

by Henry M. Halff

Like most of the papers that I write these days, this one is assigned. The assignment reads something like the following.

Discuss the opportunities for applying technology, including telecommunications, computers, cognitive science, and instructional technology to increase security awareness.

However, as with most of my papers, this one does not really address the assignment head-on. It does address technology, but only after a lengthy discussion of what Grau (1984) calls "security education," a term that covers any and all educational efforts to help personnel meet their security-related responsibilities.

My disinclination to deal directly with security awareness and technology stems from several aspects of my background.

First, as an instructional designer, I need to be convinced that security awareness is an important objective of security education. Hence, part of this paper will analyze, albeit superficially, the primary and prerequisite objectives of security education.

Second, as an experimental psychologist, I tend to shy away from rather nebulous terms such as "awareness" in favor of descriptions of what people actually do or fail to do. Hence, I will try mainly to discuss awareness in terms of its specific concomitants: knowledge, decisions, and actions.

Third, as a cognitive scientist, I tend to think of mentality in terms of knowledge structures that are enlisted to deal with each particular situation, be it classifying a document or responding to a sexual advance in a café in Karthoum. I want to go beyond awareness and ask what particular procedures govern behavior in security-relevant situations.

Finally, as a consultant, I am leery of committing myself to a technological fix before understanding exactly what is being fixed. Hence, although I

will discuss technology in this paper, it will be within the more global context of security education.

Training Objectives

This paper's focus is on the several million individuals with an obligation to prevent espionage. These include all personnel with security clearances and many other individuals employed in secure facilities.

The basic security-related responsibilities of these individuals are to

- not themselves engage in espionage,
- report breaches of security and significant security risks, and
- implement and conform to regulations that protect classified information.

These three requirements each present their own training problems. In this section we will review these requirements with a view to listing the major problems associated with each. Then, in the subsequent sections, I propose solutions, technological and non-technological, to the problems identified in this section.

Avoiding Espionage: The Collaboration Problem

There are data to indicate that many or most of the security problems of the past decade arose because personnel chose, on purpose, to collaborate with spies. It may be useful to view these decisions as did Benjamin Franklin. Franklin proposed that decisions should be made by weighing the advantages of one alternative against those of the other. Collaborators may not, as Franklin proposed, explicitly list these advantages, but they probably employ a mental listing that has the same effect. Table 1 shows how a potential collaborator might apply Franklin's method.

Table 1
Ben-Franklin Chart for Collaboration

Pro (reasons to collaborate)	Con (reasons to not collaborate)
For financial reward	To advance social or political causes
To satisfy a blackmail threat	To avoid prosecution
To enhance social status	To maintain personal integrity
To ensure personal or family security	To ensure personal or family security
For revenge	To avoid difficult tasks
To advance social or political causes	To avoid stigmatization
For sexual or romantic rewards	

The general considerations in Table 1 have differing applicability to each particular case. For example, sexual or romantic rewards constitute an advantage in only certain cases. Note that many, if not most, individuals will give some weight to one or more of the items on Pro side of the chart; the cases of concern here are those for which the Pro side outweighs the Con side. The task for security education is, therefore, to increase as much as possible the weight given to items in the Con column and to decrease, as much as possible, the weight given to items in the Pro column

Controlling Espionage: The Vigilance Problem

Every cleared individual has an obligation to report certain situations that might compromise security. These situations fall into two main classes, as shown in Table 2. The first, and less difficult, cases are actual breaches of security: a safe left unlocked, for example, or an employee actually caught in the act of espionage. A second, more troublesome class, called adverse information reporting, arises from the requirement to report cleared personnel who show signs of becoming security risks.

Table 2
Components of the Vigilance Problem

Task Components	Situations	
	Security Breach	Adverse Information
Decide to Conform		
Recognize Situations		
Report	Call or Visit to the Security Officer	

From an instructional point of view, these two cases have three components:

- deciding to conform to reporting requirements,
- recognizing situations that should be reported, and
- reporting these situations.

For most cleared personnel, the last objective (reporting) is, or should be, trivial since a visit or call to the appropriate security officer is all that is needed. However, the first and second components present serious challenges to security education.

Deciding to Conform: The Big Brother Problem

Obtaining commitment to a vigilance program can be difficult or impossible. Whether one is asked to report on specific breaches in security or on generally suspicious behavior, we, as Americans, have a deep-seated resistance to becoming agents of a police state or Big Brother. This resistance, however, is not the only factor underlying an employee's willingness to report security problems and risks. A Ben Franklin chart for this decision (Table 3) illuminates some of the other considerations that figure in this decision.

Table 3
Ben Franklin Chart for Deciding to Report Security Problems

Pro (reasons for reporting)	Con (reasons for not reporting)
For financial reward	To avoid stigmatization
To avoid prosecution	To avoid harming friends and colleagues
To maintain personal integrity	To maintain personal integrity
To advance social or political causes	To ensure personal or family security
To avoid difficult tasks	

As was the case with the parallel chart for collaboration (Table 1), not all of the considerations will play a role in all cases. The cases of concern are those where the Con side outweighs the Pro side. A major goal of security education is to minimize the likelihood of these cases by increasing the weight of the Pro considerations and decreasing that of the Con factors.

Recognizing Security Risks

As Table 2 indicates, a second critical component of a successful reporting program is employees' recognition of security breaches or adverse information. Two approaches can be used to ensure successful recognition of these situations.

- One approach calls on personnel to interpret security regulations and to devise, for themselves, methods for maintaining vigilance against security breaches and adverse information.
- The second approach calls for providing personnel, not with "raw" regulations, but rather with interpretations of those regulations in the form of procedures for recognizing when situations or circumstances warrant a report.

Thus, on the first approach, personnel would be told, for example, to report any instance in which classified information was lost or potentially compromised. On the second approach, personnel would be trained to inspect safes, glance at desktops, and take other similar actions to promote effective vigilance. The first approach has the advantage of requiring little front-end analysis and of equipping personnel to deal with unforeseen circumstances. The latter has the advantage of relieving personnel of the burden of interpreting regulations and designing effective vigilance procedures.

A combination of the two approaches is best, as long as this combination is designed to take advantage of the strengths of each. Designing procedures that make inspection of secure areas part of an employee's regular routine is probably the most effective way of ensuring that he reports any breakdowns in the protection of information in the area. On the other hand, enforcing a fixed procedure for seeking out adverse information would probably be the worst way of ensuring that such information is reported.

Implementing regulations: The regulation-procedure gap

Teaching personnel to recognize what should or should not be reported is one manifestation of the general problem of designing instruction to implement regulations. For the most part, the security of information in this country is protected through a complex set of regulations and instructions. These regulations sometimes call for particular procedures, but they often are phrased in terms of goals or conditions that must be met. Many accountability regulations, for example, call for maintenance of certain records without specifying who makes entries into these records, when these entries are made, or exactly where the records are located.

Explicit procedures for protecting classified equipment, if they exist at all, can be quite complex. The procedure for reproducing SECRET or CONFIDENTIAL documents, which is among the simplest for handling classified documents, contains 24 steps, 10 of which call for decisions.

In addition to the challenge of creating procedures for protecting information, the security education enterprise also has the problem of making these procedures accessible to employees. A regulation-procedure gap exists whenever a regulation imposes some standard on an enterprise and the procedures for meeting that standard are not specified or partially specified. Every such gap constitutes a problem for security education because it relies on individual employees to create the procedures needed for conformance to regulations. Employees will often be unable or unwilling to create appropriate procedures and, as the result, will fail to conform to regulations. A prime goal for the security education community is therefore the narrowing or elimination of regulation-procedure gaps.

To approach this problem, we need to ask first how procedures are to be defined and second, who, within the security-education system is responsible for defining procedures.

Representing Procedures

A first step in narrowing the regulation-procedure gap is an appropriate scheme for representing procedures. Many mechanisms have been invented for this purpose. More recent representation systems arising from cognitive-science research provide a powerful combination of precision and psychological validity. All of these representations represent procedures in terms of the following major components.

- *Steps.* A procedure is a sequence of discrete steps that, between choice points (described next), are executed in a specific order.
- *Choice Points.* Most procedures require decisions or choice points that direct the procedure to alternative subsequences of steps depending on the values of certain variables (described next).
- *Variables.* Most procedures call for the manipulation and use of values that will change from time to time. These values are described as variables to be manipulated by specific steps and interrogated at choice points.
- *Subprocedures.* Effective management of attention during procedure execution calls for the use of independent subprocedures to represent large chunks of a procedure.

One typical representation system is the GOMS model introduced by Card, Moran, and Newell (1983). Table 4 shows how the procedure might be represented in GOMS.

Table 4
Partial GOMS Representation of the Procedure for Reproducing
Confidential or Secret Documents

Method to accomplish goal of reproducing confidential or secret document

- Step 1. Accomplish goal of determining classification level of document.
- Step 2. Accomplish goal of determining whether reproduction is permitted.
- Step 3. Decide: If recall that reproduction not permitted
Then report goal accomplished.
- Step 4. Accomplish goal of preparing document for reproduction.
- Step 5. Accomplish goal of making copies.
- Step 6. Accomplish goal of cleaning up.

Method to accomplish goal of determining classification level of document

- Step 1. Decide: If document is marked "Confidential"
Then retain that document is Confidential.
- Step 2. Decide: If recall that document is Confidential
Then report goal accomplished.
- Step 3. Decide: If document is marked "Secret"
Then retain that document is secret
Else report goal accomplished.
- Step 4. Decide: if document is for internal purposes
Then retain that secret document is for internal purposes.
- Step 5. Decide: If document is marked "Do not reproduce"
Then retain that reproduction of secret document is prohibited.
- Step 6. Report goal accomplished.

Method to accomplish goal of determining whether reproduction is permitted.

- Step 1. Decide: If recall that reproduction of secret document is prohibited
Then go to 4.
- Step 2. Accomplish goal of determining whether reproduction is essential for authorized purpose.
- Step 3. Decide: If recall that reproduction is essential for authorized purpose
Then retain that reproduction is permitted
Else retain that reproduction is not permitted.
- Step 4. Report goal accomplished.
- Step 5. Accomplish goal of obtaining authorization from contracting officer.

Step 6. Decide: if authorization granted
Then retain that reproduction is permitted
Else retain that reproduction is not permitted.

Step 7. Report goal accomplished.

Method to accomplish goal of preparing document for reproduction

- Step 1. Accomplish goal of determining number of copies needed to meet operational requirements.
- Step 2. Accomplish goal of determining date or event when copies will have served their purpose(s).
- Step 3. Decide: If recall that document is secret and reproduction is for internal purposes
Then accomplish goal of marking and accounting.
- Step 4. Accomplish goal of obtaining FSO approval.

Method to accomplish goal of make copies

- Step 1. Accomplish goal of gaining access to designated equipment.
- Step 2. Accomplish goal of clearing area of other personnel.
- Step 3. Accomplish goal of copying documents.
- Step 4. Accomplish goal of making 3 blank copies.
- Step 5. Accomplish goal of removing material to control station.

Method to accomplish goal of cleaning up

- Step 1. Accomplish goal of checking copies for markings.
- Step 2. Decide: if recall that copies are missing markings
Then accomplish goal of marking copies.
- Step 3. Decide: if recall that document is Confidential
Then go to 6.
- Step 4. Decide: if recall that not entered into accountability record
Then accomplish goal of entering into accountability record.
- Step 5. Accomplish goal of updating copy count in records.
- Step 6. Accomplish goal of disposing of waste and blank copies.
- Step 7. Accomplish goal of storing copies.
- Step 8. Report goal accomplished.

GOMS represents procedures in terms of Goals, Operators, Methods, and Strategies. Table 4 illustrates only the first three components; goals and methods are explicit in the representation; operators are primitive actions such as Decide, Recall, and Accomplish goal. Note that the analysis in Table 4 presents only the first two levels of the procedure's goal hierarchy. Further

expansion of some of the subgoals, marking and accounting, for example, would require expansion prior to developing instruction in the procedure.

There are many benefits to representing procedures using a formalism such as GOMS. Such representations test the integrity of the procedures and provide indices of their psychological demands. They constitute powerful instructional tools in that they can be objectively analyzed and presented to students in a number of forms. They can serve as the basis of computer simulations of procedures and thereby enable the application of computers to procedure training. Much could be done to close the regulation-procedure gap with a program of procedure design and representation that would cover regulations governing the protection of classified material.

The Bureaucratic Hierarchy and Procedures

A program of security procedure design and representation must first address the issues of what procedures are needed and who formulates or promulgates those procedures. The resolution of these issues lies in the bureaucratic structure that controls security education. This structure has three main levels.

- All security regulations are promulgated by some central authority. In the case of defense contractors, this authority is Defense Industrial Security Manual (ISM). Security in military facilities is governed by each service.
- In each facility, an office or individual security officer is responsible for implementing centrally promulgated regulations in the facility- or site-specific context. For defense contractors, these site-specific implementations are defined in volumes called the Standard Practice Procedures (SPP).
- Each individual employee has responsibility for implementing the provisions of both centrally promulgated and facility-specific security practices. Many of the procedures used to implement these practices will vary from employee to employee. These employee-specific procedures are rarely documented.

In some organizations the bureaucracy may contain more levels. For example, large facilities may have a central security office with individual representatives in different facilities.

Of central importance for our purposes is the notion that procedures promulgated through the bureaucracy become increasingly specialized at lower levels. Hence,

- some procedures, such as those for recognizing (and marking) classified material are fully specified in the ISM.;
- others, such as accountability procedures, are only partially specified in the DISM, but are fully specified in the SPP;
- still others, such as procedures for storing classified documents, are only partially specified in the ISM, leaving many aspects to the individual handling the material.

This hierarchy of increasing specialization provides the opportunity to achieve certain economies in the development of security education. Two principles apply to this situation.

First, employees should be taught procedures that are only as general as those that they need to exercise on the job. Thus, for example, it is more appropriate to teach a clerk that classified documents are to be stored in a particular safe than to teach him that classified materials should be stored in a GSA-approved security cabinet, a Class-A vault, a Class-B vault, a strongroom, or a Class-C vault.

Second, procedures should be developed at the level in the bureaucratic hierarchy where they are fully specified. Thus, for example,

- procedures for recognizing classified documents can be developed by a central authority such as the DOD Security Institute (DODSI) or the Defense Personnel Security Research and Education Center (PER-SEREC);
- accountability procedures should be developed by security officers at each facility;
- all individuals in a facility should be responsible for determining exactly how the classified documents under their purview are to be stored.

Problem Solving

It is important to understand that many aspects of the regulation-procedure gap are inherently unclosable. That is, many regulations apply to situations so unique that no fixed procedure exists for ensuring conformance. For example, no fixed procedure exists for determining when an employee has the need to know a particular piece of information. Emerging technologies such as facsimile and computers pose security problems that have no fixed solution. No universal procedure is available for recognizing when a colleague's behavior constitutes adverse information.

Because no fixed procedures exist for dealing with these situations, employees must rely on problem-solving skills to formulate an appropriate procedure. The current view of these skills is that of a combination of general problem-solving techniques (*e.g.*, breaking the problem down into sub-problems), and domain-specific techniques. The latter depend on classifying the problem into one of a small number of types and then applying a solution appropriate to the type.

The extent to which domain-specific problem-solving skills exist for security-related problems is an interesting research question. Until this question is answered, the best prescription for analysis of the security-related problem-solving requirements is the collection of a large number of important problems along with their solutions.

Summary

Before turning to other aspects of the security education problem, let us review the problems posed by our brief look at instructional objectives.

We have pointed out that security education has three main objectives:

- to ensure that personnel do not themselves engage in espionage,
- to ensure that personnel report any breaches of security or adverse information that might compromise security, and
- to ensure that personnel implement or conform to regulations designed to protect classified information at their facility.

In examining these objectives, we came across several critical problems that must be solved for effective security education.

The *Collaboration Problem* arises when an employee sees a greater advantage in collaborating with a spy than in refusing to collaborate. Security education's contribution to its solution is to maximize in each employee's perception the advantages to be gained from not engaging in espionage and minimize the advantages of engaging in espionage.

The *Big Brother Problem* arises when an employee sees a greater advantage in not reporting security breaches and adverse information than in reporting these situations. Security education's contribution to its solution is to maximize each employee's perception of the advantages to be gained from reporting adverse information and breaches of security minimize his perception of the advantages of ignoring reporting requirements.

The *Regulation-Procedure Gap* refers to the lack of explicit procedures for implementing any regulations designed to safeguard material (including those for reporting). Security education can help to solve this problem in two ways: by promoting the design of, representation of, and instruction in procedures for implementing security regulations, and by developing the problem-solving skills needed to deal with situations where no fixed procedure exists.

Note that these problems fall into two classes. The Collaboration and Big Brother Problems are what most would call "motivational," although they have critical cognitive components. The Regulation-Procedure Gap is primarily a cognitive problem with critical organizational aspects. We will return to this breakdown in the section on Approaches to Training, but before we can discuss applicable instructional approaches, we need to understand some important aspects of the training context for security education.

The Training Context

Security education would be easy if there were no constraints on the resources available for development and delivery of training. Unfortunately, the constraints on security education are more than severe. In this brief section, we summarize some of the more important constraints.

Training Load

Security education's training load, in terms of numbers of students, is tremendous. All cleared personnel are briefed upon receiving their clearance. In addition, regulations call for regular (usually annual) updates and for briefings upon special occasions such as changes in the security status of a facility or individual. Although exact figures are not available to me at this time, it appears that the load, in terms of numbers of employees briefed per year is in the millions.

Note also that some of these employees are blue-collar workers who require access to classified equipment. Others are white-collar workers who require access to classified information in the form of paper or electronic documents.

Training Resources

Security education has little in the way of training resources. At the DOD level, instructors and instructional designers at DODSI number in the tens. These individuals are devoted to creating and delivering instruction to security officers, who, in turn, are responsible for training the millions of employees referred to above. Security officers, by my reckoning, number in

the 10,000s. Hence, each level of the bureaucratic hierarchy described above represents a 23 order-of-magnitude increase in the target population.

In addition to these human resources, it is worth considering the physical resources, and particularly the media, available for security education. A prime consideration in this regard is the almost complete absence of dedicated training facilities, equipment, and media. Apart from dedicated facilities at DODSI, security education must use facilities and equipment available for other purposes at each facility. Worth mentioning in this regard is the fact that personal computers are, or will soon be, available to every white-collar worker in secure facilities. These computers, which fortunately employ one of a few standard operating systems, have considerable potential as training devices for security education.

Certain materials—in print, videotape, film, and other non-interactive media—are available for use in security education. Interactive materials for security education are virtually non-existent. As the cost of producing interactive materials decreases and as the equipment for delivery of interactive materials becomes more common, interactive delivery will represent a prime opportunity for more effective security education.

Priority, Motivation, and Feedback

In addition to the large training load and limited resources, other features of the training context pose particular challenges to the security education enterprise.

For the vast majority of personnel, security concerns are a low priority. Many of them will only rarely come into contact with classified material, and, when they do, their concerns are more for its creation, manipulation, and use than for its protection. Thus, one cannot expect much from the average worker in the way of attention to security education or indeed to any other aspects of security.

A concomitant of the priority problem is a low level of motivation among employees. Even during the times that they are engaged in security-related tasks, their motivation to succeed in these tasks will be low. Security education must either find ways of raising motivation or of ensuring that security is protected even when motivation is low.

Part of the motivation problem is the lack of natural rewards. Security measures, by their nature, are successful only when nothing happens. Feedback on security-related tasks is almost always negative. Because rewards are far more effective training devices than punishments, security educators must find ways of introducing positive feedback into their efforts or ways of

living with the reduced training effectiveness provided by negative reinforcement.

Approaches to Training

Above we made the point that the problems facing security education were of two sorts. Motivational problems arise in connection with efforts to teach workers not to collaborate with spies and to induce workers to conform to security reporting requirements. Cognitive problems arise in connection with instruction on the procedures needed to implement security regulations. These two classes of problems require different solutions.

Building Commitment

Inducing people to not engage in espionage and to report any circumstances that might compromise security is primarily a task of building commitment to the protection of classified information. The mechanisms responsible for this commitment and for its erosion are shown in Tables 1 and 3. Some of the factors in these tables are unimportant, and some are not under control security education efforts. However, employees' perceptions of some of the more important factors can be informed by appropriate security education efforts, including the following methods.

Forcing the Choice

Many of the employees who decide to engage in espionage or to turn a blind eye to security problems no doubt make the decision under circumstances that are not conducive to a rational choice. One approach to security education is to force employees to "pre-decide" under conditions more amenable to informed decision making. Part of security education should permit employees, before a clearance is granted, to confront difficult (hypothetical) situations and to make the collaboration and reporting choices in a non-threatening, supportive environment. In this environment, they could make explicit the considerations driving the choice (namely those in Table 1 or Table 3), and trainers could provide whatever data are available (damage estimates, for example) to guide the choice.

Public Commitment

A powerful means of increasing the weight of conscience or personal integrity in decisions is the use of a public commitment to undertake or avoid certain courses of action. In contrast to the relatively private use of signatures on official documents, employees could be encouraged to publicly commit themselves, in the presence of colleagues, to support the security measures applicable to their situation.

Informed Consent

As Table 3 indicates, one of the major deterrents to reporting adverse information or breaches in security is the strong public resistance to Big-Brother tactics. This resistance might be significantly weakened if the individuals at risk from adverse information reports would publicly give their consent to the relevant reporting requirements.

To obtain this informed consent, security educators might first build the groundwork by building a case for the reporting requirements at hand. (Such a case could be built by reminding students of the necessity for security controls and of the desirability of relying on workers themselves to exercise these controls rather than bringing in an army of police and professional inspectors.) After building this case, employees could be encouraged to publicly consent to the level of collegial surveillance required of cleared individuals. In this way personnel responsible for reporting would have the assurance that adverse reports are not in principle objectionable to their colleagues.

Vicarious Rewards

Although positive incentives for protecting information are rare in the workplace, they can be freely administered in many training situations. Successful completion of training exercises and problems should always be accompanied by some form of reward. These rewards can be tangible—money and prizes, for example—or they can be intangible reminders of good performance.

The Initial Security Briefing

In summary, the best hope of building commitment to maintaining security is to begin, as early as possible, to build each employee's perception of a clearance as a choice in which he willingly incurs common obligations. Needed to support this approach are two fundamental changes in the design and conduct of Initial Security Briefings, those briefings given to all personnel when they first receive clearances.

First, these briefings should be given as early in the hiring or change-of-status process as possible, and preferably prior to the employee's decision to accept a new position. The briefing should be promulgated as an opportunity for the employees to learn about essential security aspects of the job and to decide for themselves whether or not these aspects are acceptable.

Second, the briefings should rely heavily on exercises that build commitment to maintaining security. These exercises should require active participation on the employee's part and should emphasize interpersonal interactions. One possible view of such a meeting has three phases.

- After a brief introduction, the instructor explains the importance of maintaining security, sketches the procedures used to protect classified information, and describes the rationale for these procedures.
- Employees form small groups that role-play some of the most troublesome situations for security decisions. Employees develop Ben Franklin charts for each situation. During a debrief these charts are presented to the larger class, and the instructor offers feedback and information as appropriate.
- To close the meeting, each employee makes a public promise to adhere to security regulation and expresses his willingness to remain under the informal surveillance of his colleagues. (Opportunities should also be provided for individual employees to opt out of the situation if they are uncomfortable with any of the security requirements of the job.)

This view of the Initial Security Briefing is somewhat different than that promulgated by, say, the DISM. Sacrificed, on this approach, are all of the details of the procedures needed to implement an effective information security program. Employees leave the briefing with a commitment to the main objectives of this program but without the knowledge and skills needed for its execution. Hence, in addition to the briefing described above, additional instruction on particular security procedures will be needed.

Building Procedural and Problem-Solving Skills

The techniques and technologies for teaching procedures are quite different than those proposed above for building commitment. Following on the points made above in the section on implementing regulations, employees need to master:

- explicit procedures that implement the regulations applicable to their responsibilities to protect classified material, and
- problem-solving skills used to deal with situations where no applicable procedure exists.

Procedure Training

The former case is more easily dealt with since a sizable literature exists on teaching and learning procedures. The literature can be summarized by the recommendation that procedure training be based largely on *guided practice*. The elements of a guided practice regime are exercises and examples presented according to a few simple rules. A minimal set of two rules proposed by VanLehn (1987) follows; other more elaborate guidelines have been proposed numerous psychologists and educators.

- Exercises and examples are presented in discrete blocks or lessons. Each lesson illustrates a particular choice point in the procedure.
- Exercises and examples should be presented in such a way that intermediate, conceptual steps and variables not normally evident in the problem are made explicit.

Consider, as an example, a curriculum for teaching the procedure shown in Table 4. Such a curriculum would attack each major step or subgoal in turn. Thus, the curriculum would begin by teaching how to distinguish between confidential and secret documents, and how to determine whether reproduction of secret documents requires authorization. Exercises would require students to indicate all intermediate steps such as deciding whether or not the document is to be reproduced for internal purposes. It would provide examples of authorized and unauthorized purposes for reproduction and would ask students to make a determination, in each case, of whether copying is permitted.

After exercises on determining whether reproduction is permitted, the curriculum would focus on document preparation and, in particular, provide a series of exercises on marking. The curriculum could then provide some practice in making copies and finish with lessons on cleanup and accountability.

Problem-Solving Training

Instruction in cases where set procedures do not apply cannot be approached by the structured, guided-practice methods sketched above. What can be provided are instruction in general problem-solving methods and a number of practice problems or examples along with solutions.

The teaching of general problem-solving skills has received considerable attention over the past 10 to 20 years, and a wide variety of instructional approaches are available. Most of them view the problem-solving process as a series of stages. The following is a typical breakdown of these stages.

- Define the problem. Develop a statement of the current situation and the goal.
- Characterize the problem. Determine the main differences between the current situation and the goal. Identify the means available to eliminate these differences.
- Reduce the problem to more easily solved subproblems, if possible.
- Develop candidate solutions.

- Evaluate the relative utilities of each solution and adopt one or more on the basis of this evaluation.
- Implement the chosen solution(s) and evaluate the result.
- Repeat the process until the problem is solved.

Isolated instructional programs on problem-solving methods like the one outlined above are rarely effective in helping employees deal with particular situations. They may, however, have some positive effect,

- *if* they are introduced in the context of job-relevant problems,
- *if* the results of each stage are made explicit, and
- *if* they are practiced with a variety of problems sufficient to illustrate their range of applicability.

Even without instruction in general problem-solving methods, exposure to a wide range of problems and solutions cannot help but improve problem-solving skills within the range of problems presented. Indeed, I believe that any time devoted to indoctrination in general problem-solving skills might be better spent in informal practice with real or simulated problems.

Fortunately, in the case of security education, problem-solving practice (and perhaps general problem-solving training as well) can be provided in a format that is both instructive and motivating. To be specific, the genre of games known as adventure or role-playing games could be used with only minor modifications in format.

Role-playing games, for the uninitiated, place players into fictional scenarios and allow them to move about in the scenario, examine aspects of their environment, and manipulate the environment in certain ways. In some implementations, these games are conducted under control of a human moderator. In other implementations, a computer is used to simulate the fictional environment.

A role-playing game that uses, as a scenario, some fictional cleared facility, furnished with classified documents and populated by spies and collaborators, is an ideal mechanism for exercising security problem-solving skills. Among its benefits are the following.

- Systematic coverage can be provided. The game can be designed to require successful exercise of all of a selected set of judgments and actions.

- Feedback can be immediate. Failure to conform to a regulation, for example, can be immediately and consistently followed by some adverse consequence or another.
- Feedback can be informative. The moderator or computer can cite the regulations and procedures that bear on both correct and incorrect moves in the game, as well as the rationale for those regulations and procedures.
- Positive feedback can be provided. The machine can congratulate students on correct moves and it can "engineer" happy endings for normally negative actions such as reporting of adverse information.
- Instructional support can be provided in context. Copies of regulations and written procedures can be made available for use in specific game situations. In human-moderated, and some computer-controlled games, a tutoring mechanism can provide hints concerning the relevant regulations or procedures.

Instructional Methods and Media

It should be obvious that the traditional briefing environment is far from appropriate for guided practice, for role-playing games, or even for instruction in general problem solving. Needed instead are

- actual or simulated materials for a wide variety of exercises,
- media that can exhibit the conceptual or mental aspects of each exercise, and
- control mechanisms that track student performance and provide appropriate feedback.

For some purposes, programmed learning materials using print media provide the above-listed elements. However, the medium of choice for interactive practice is a computer-based training. Computers offer certain instructional advantages, including ease of use and realistic simulations. They also offer advantages in development and delivery, topics covered in the next section.

Summary

This section focused on two overall classes of objectives for security education.

We first considered how to build employees' commitment to their security-related responsibilities. Proposed was a training program that encourages

workers to make the more difficult choices required by this commitment early in the hiring (or other change of status) process and to make public their commitment in a supportive environment.

We next considered how to provide the knowledge and skills that employees need to implement required security measures. Proposed were programs of guided practice in the use of established procedures, context-specific training in general problem-solving skills, and problem-solving practice provided via role-playing games. The interactive nature of these programs makes computers a promising medium for their delivery.

Based on these suggestions, every cleared employee (and selected non-cleared personnel) would be given as *initial training* (before hiring or a change in status)

- a security briefing designed to build commitment to the protection of classified information,
- a curriculum of self-paced interactive exercises covering the established procedures applicable to her situation, and
- a collection of role-playing games that exercise problem-solving skills, perhaps in conjunction with training in general problem-solving skills.

Recurring training might consist of modified versions of the elements listed above. To maintain commitment, each employee might be asked to serve as a "resource person" in an Initial Security Briefing, say, once every three years. Interactive refresher exercises and games could be made available once a year to maintain skill levels and introduce employees to new regulations and procedures.

Ignored thus far are the means for developing, delivering, and administering these proposed programs. In view of the limited resources available for these purposes, this discussion would not be complete without some attention to a broader view of the security education enterprise.

Developing and Delivering Security Education

The preceding section was concerned with the educational needs of the millions of individuals working with classified material. This section is primarily concerned with the 10,000s of security officers directly responsible for meeting those needs and the 10s of professionals at DODSI and perhaps other institutions that are responsible for supporting the security officers.

The numbers of individuals at each level of the security education bureaucracy, in addition to conveying the resource-limited nature of the security education enterprise, suggest an overall investment strategy.

- Heavy investments at the highest level of the hierarchy are entirely appropriate since the multiplying effect of these investments is in the 100,000s.
- Considerable investments in the training and equipping of security officers is also warranted since increases in their effectiveness is multiplied by two orders of magnitude.
- Significant investments in individual employees should be considered very carefully since, at this level, one unit of cost buys only a single unit of benefit.

This strategy and the constraints listed in the section on the training context suggest the following approach to providing an educational program like that described above.

Materials and Support

The approach described above requires that a security officer would be responsible for conducting the Initial Security Briefing, distributing self-study materials, and ensuring that the self-study courses are completed. To support this officer in these tasks, the following materials and training might be provided

- A course in the conduct of an Initial Security Briefing. This course would cover the interpersonal skills needed for the briefing, the goals of the briefing, and the conduct of the briefing.
- A computer-based kit for the creation of computer-based training materials. This kit would contain the following elements.
 - » A catalog of lessons addressing various procedures along with a computer-based decision aid for choosing lessons for individual employees.
 - » Fully operational lessons for universal, fixed procedures (*e.g.*, recognizing the classification level of a document or parts thereof),
 - » Lesson shells that could be configured by the security officer to match procedures at her facility. For example, a lesson on storage could be configured to include information on the locations of relevant storage containers at the particular facility.

- » A curriculum generator that would produce (on a floppy disk or file server) a computer program with a complete curriculum for a single employee. This curriculum would include lessons selected for the employee together with testing and certification procedures to ensure successful completion.

It is my strong recommendation that such a kit be made part of a larger computer-based facility that would address the broad range of the security officer's duties. Possible functions of this broader program might be the creation of the facility's SPP and other security-related instructions, databases for tracking security-related data, and electronic copies of important regulations and procedures.

- A library of computer-based role-playing games that would provide practice in problem-solving and the application pertinent procedures and regulations. A cross-index of these games to regulations, procedures, and instructional objectives would permit the security officer to select games appropriate for particular applications and individuals.
- A support and update service that would keep the security officer informed of changes in procedures, supply her with updated instructional materials, and provide assistance with particular problems that she might encounter in the course of her job.

The items proposed above are not completely consistent with the strategy of minimizing per-student training costs. In particular, the class size of Initial Security Briefings would need to be limited to approximately 16 students, and the briefing might run longer than those now given.

Some of the extra per-student expense, however, would be recovered by using computers as a medium for distribution and delivery of instructional material. Since this instruction would be self-paced, it would, of necessity, provide maximally efficient use of student time. In addition, savings would be realized in the costs of distributing instructional material. Worth noting in this regard is the presumption that any employee with access to classified information will also have access to a computer. Along with this presumption is the requirement that the computer-based training material provided to employees should run on all common hardware and operating-system suites.

Design and Development

The responsibilities for designing and developing the materials that make up the training program outlined here, and for training security officers in its delivery, fall to organizations such as DODSI and PERSEREC.

The major activities needed to provide support and materials are as follows.

Research and Analysis

The program outlined here requires more in the way of analysis than the simple collection and distribution of regulations and case descriptions. Some of the analytical and research requirements directly related to this program include

- analysis and specification of both general and facility-specific procedures in order to close the regulation-procedure gap as much as possible;
- collection and analysis of critical or difficult security problems for use in problem-solving and commitment building exercises;
- research on the overall effectiveness of existing and new security measures (including education); and
- determination of the scope of the training problem, including numbers and types of employees, numbers, qualifications, and commitments of security officers, and availability of training equipment and facilities.

Instructional Design and Development

Needed to support the program described above are four main instructional products.

An Initial Security Briefing package should be produced. Since no special facilities are needed, this package can consist of an instructor's guide, instructional materials such as overhead transparencies, and student materials.

A development kit for computer-based training must also be developed, either as a stand-alone program or part of a broader computer-based support kit for security officers. The development kit must contain not only the lessons to be provided to students, but also the facilities whereby the security officer can configure those lessons to meet the needs of his students.

Also required is training for security officers. This training would specifically cover the security officer's educational role, but it could be offered as part of training in other aspects of his job. For our purposes, it would teach security officers to conduct security briefings and to use the computer tools provided for the development of procedural training.

Finally, a library of role-playing games must be developed. The library can be as large as is needed to cover important issues and regulations in a variety of contexts. I am no expert on the development of these games, but I understand that there are several development options available. On the low end, subject matter experts could employ a commercially available adventure-game shell such as *World Builder* (Appleton, 1986) to create the games. At the other extreme, the DOD could engage the services of professional game developers, who would work in conjunction with subject-matter experts to create the materials.

Taken together, these materials call for a massive development effort. A reasonable cost for the security briefing package (2 hours of instruction) and two-day workshop for security officers is \$75,000. The development kit, which at this point would be very much an R&D effort, could easily cost \$500,000. The library of adventure games could, depending on the volume of material, cost \$175,000. The reader is warned that these costs estimates are very tentative; an order-of-magnitude error is not out of the question.

Training the Trainers

Mentioned above is the need for training of security officers. Along with this training are the facilities and personnel required for its implementation. An appropriate facility would house conventional small-group classrooms and breakout areas for training in security briefings. Also needed would be computer labs for training in the development and configuration of computer-based instruction. A single instructor could serve each class for, say, a day's workshop on delivery of the Initial Security Briefing and a second day's worth of computer-lab training. Administrative and technical personnel would be needed for scheduling, computer-lab maintenance, and other similar tasks.

This brief description can be used to make a rough estimate of resource needs for delivery of security-officer training. If two classes of 16 could share a classroom and computer lab for a two-day workshop, then four facilities would permit the training of some 15,000 security officers per year, if operated a full 240 days per year. Two instructors would be needed to staff each facility so that eight instructor years would be required together with the technical and administrative staff needed to support the effort.

It is also worth mentioning, in connection with security-officer training, that these individuals will need ongoing support. They will need to be kept abreast of changes in security-education practices and provided with updated materials. They will also need help when they encounter particular problems in either the classroom or in the use of computer-based training tools.

The materials and support suggested above are designed to minimize the instructional burden on the security officer, but they do place a heavy burden on central facilities for design and development of the materials and support. What justifies this enormous expense is that it ultimately provides security education to millions of people. The costs, although they cannot be reckoned here, are probably miniscule on a per-employee basis.

Summary and Conclusion

I began this paper with the assignment of discussing opportunities for technology to promote security awareness in workers at cleared facilities. What I have actually done is to address three questions that appear to me to be central to the concerns of security educators.

What are the main goals and issues facing security education?

Security education has the goals of promoting the avoidance of espionage, conformance to reporting requirements, and implementation of regulations governing the protection of classified information. Its major problems are those of nullifying the attractiveness of collaboration with spies, of overcoming strong resistance to security reporting requirements, and of endowing employees with the procedural and problem-solving skills needed to implement security regulations.

What contextual constraints limit or facilitate security education?

We considered three features of the training context. First, the training load is massive, numbering in the millions of students per year. Second, resources are limited since there are virtually no dedicated resources and since training is only a small part of most security officers' jobs. Third, motivation for security-related activities is low, partly because security is simply not a large concern for most employees and partly because there are few rewards for fulfilling security-related responsibilities.

What should security education provide in the way of training?

Training to build commitment to security-related responsibilities should encourage workers to make difficult choices early and in a supportive environment rather than in the "heat of battle." It should also encourage employees to make a public commitment both to conform to security regulations and to submit to whatever surveillance is required by those regulations. The ideal mechanism for implementing these training measures is the Initial Security Briefing.

Training in procedural and problem-solving skills should be built around exercises. In the case of procedure training, exercises can be presented using the techniques of guided practice. Problem-solving practice can be provided in the form of role-playing games and/or in conjunction with instruction in general problem-solving techniques. Computer-based training is the medium of choice for both procedural and problem-solving training.

What is required for development and delivery of the training proposed here?

Training should be delivered by security officers at each facility. These officers would provide each newly cleared employee with an initial security briefing designed to build commitment to security-related concerns. He would also configure and distribute a package of computer-based instructional lessons and games to provide training in security-related procedures and problem solving.

Materials and support for these security officers should be provided by a central organization such as DODSI. Needed in this regard would be materials for the Initial Security Briefing, a kit for development of computer-based training, training in both the initial security briefing and computer based training, and a support and update service.

Two general conclusions concerning technology and security awareness emerge from the answers to the questions addressed above.

First, there is a role for technology in security education, namely that of providing practice in security-related procedures and problem solving. The use of computers to deliver such practice has the potential for dramatically increasing its effectiveness and of decreasing its cost. Increases in effectiveness can be expected through individualization, active involvement of the learner, and increased motivation. Decreases in cost can be expected through the advantages of computer media for delivery and distribution.

Second, the major motivational problems that security education faces are not amenable to a technological solution. These problems, at their heart, concern relations among employees, and only by increasing the quality of communication and understanding among employees can security education have any effect in increasing workers commitment to effective security measures.

References

Appleton, W. C. (1986) *World Builder*TM. San Diego, CA: Silicon Beach Software.

Card, S., Moran, T., & Newell, A. (1983). *The psychology of human-computer interaction*. Hillsdale, NJ: Erlbaum.

Department of Defense Security Institute (1989). *Protecting SECRET and CONFIDENTIAL Documents* (Subcourse DS2104, Edition 9). Richmond, VA: Department of Defense Security Institute.

Grau, J. (1984). Security education: Something to think about. *Security Management*, 28 (10), 25-31.

VanLehn, K. (1987). Learning one subprocedure per lesson. *Artificial Intelligence Journal*, 32, 140.

Dr. Brinkerhoff is Professor of Educational Leadership, Human Resource Development Studies at Western Michigan University. He is the author of seven books on evaluation and training. Dr. Brinkerhoff has worked for a variety of clients in performance management and assessment, productivity analysis and measurement, project management and training design, delivery and evaluation.

Security Awareness Program Evaluation

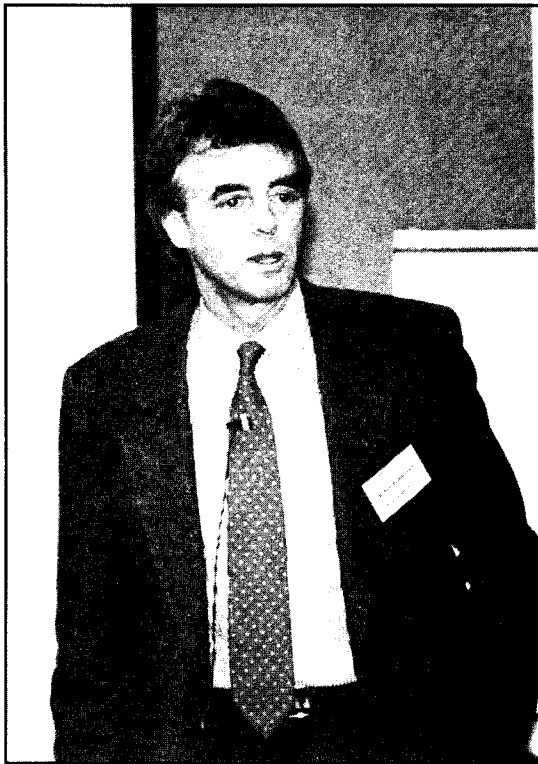
by Robert O. Brinkerhoff

The task I was challenged with was to apply my learning about evaluation of training programs in corporate (business) settings to security awareness. This I found intimidating for two reasons: One, the more I work on evaluation of training, the more questions I have versus answers. Secondly, what I know about security awareness is very limited, amounting mostly to what I can remember from 20 some years ago when I was a lieutenant in the U.S. Navy, in other words, not much. So, what I have done in this presentation is to tell you about the critical questions and issues that I think we face in any training endeavors, and leave you to transform these into "answers" in your area of security awareness.

It is very difficult, and often confusing, to think about how to evaluate training, because training itself is an elusive phenomenon about which I find considerable confusion. Some view "training" in a narrow sort of way to consist of tightly organized interventions (such as workshops and courses) intended to impact on specific job skills and behaviors. Others see training as including more broadly developed educational endeavors intended to provide more general results of increased capacities, or changes in attitudes. Others yet see training to include awareness and information transmission efforts (which might include advertising, such as we have just seen). Different attitudes, as well as concepts, about training abound. Some see training as an indispensable part of organizational effectiveness and competitive advantage; others contend that training is "fluff"—a sort of staff benefit that is, an expense out of which we should expect little return. If we are to evaluate training, we have to sort out these different attitudes and concepts, and be very clear about exactly what we mean by "training."

Before I move on to present a view of training that gets us over some of these definitional hurdles, I want to make it clear that, however we define training, it poses some inherent issues and problems for evaluation that have to be dealt with. First, training is always a marginal sort of intervention. Training can have some very clear and discrete, readily observed, immediate results in the form of learning, such as an increase in awareness, or an acquisition of a skill or concept. But, when transferred to the work place, these

learning results get quickly attenuated, altered, reshaped, even overwhelmed by the far stronger forces of policy, tradition, reward, incentive, habit, and so forth. Changing behavior is a complex issue, and learning (capacity) provides only a small piece of the larger performance puzzle. Training can work, but it can only work in concert and integration with other organizational interventions, such as supervision, coaching, rewards, and so forth.



Professor Robert Brinkerhoff

This fact of training life means that (a) it is very difficult to isolate pure "training" results, and (b) that it makes little sense to try to do so in the first place. Capacity to perform, in the form of knowledge, skill, awareness, and attitude, is an indispensable part of work performance. I don't need any evaluation to "prove" this fact. But it is also a fact that people perform in ways that are virtually independent of what they may know, or be able to do. I know, for example, that a poorly tuned car drives ineffectively and costs more to run than a well tuned car; I have no knowledge deficit here. I can even recite some of thermodynamic principles and factors that cause this poor performance. I am overly trained, in fact, but I persist in driving a van that barely starts, sputters, smokes, and guzzles gas. Why? Because it runs. For one thing, I'm short of time and energy for getting it fixed (which is a hassle), and I don't have

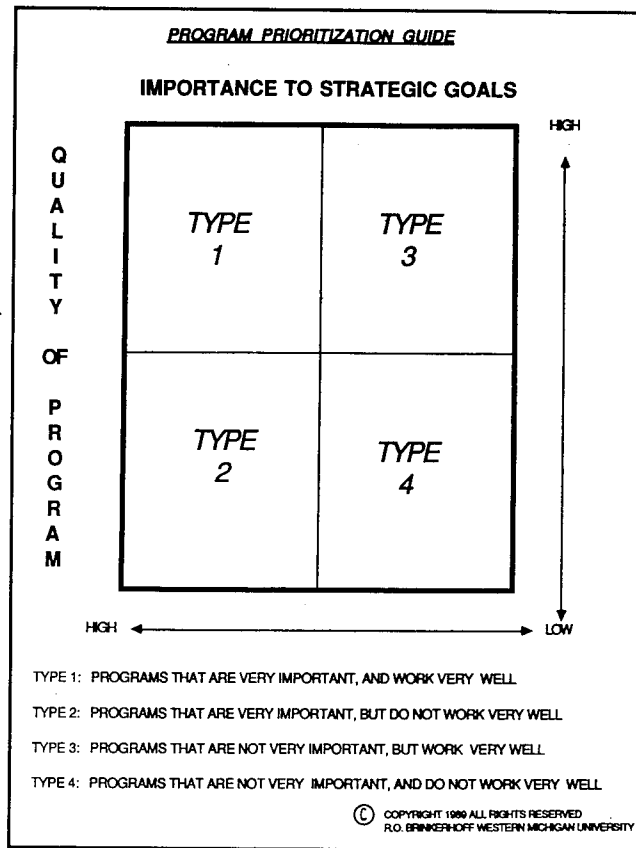
anyone (my wife drives another car) on my case to get it fixed up. I don't need any training, in short. But the fact remains that my knowledge is probably a precondition to action—necessary but nowhere near sufficient. If I were ignorant, getting me to act would be altogether impossible.

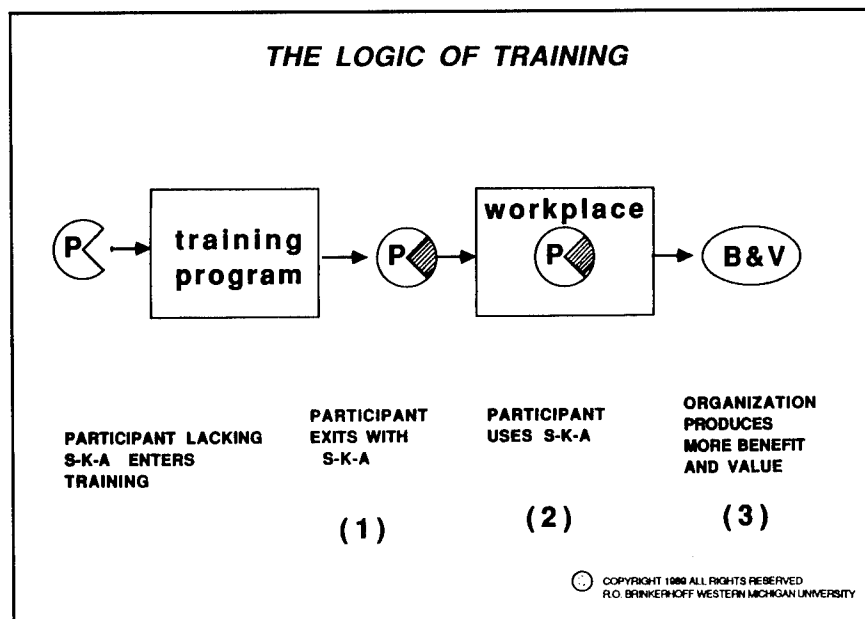
Training is always needed. The question is, what sort of training, how much, when, where, how frequently? These are good evaluation questions, and we can readily pursue them. In fact, they cannot be answered without evaluation. And any good training program has already answered these questions. Thus good training and good evaluation are integrally connected. You have to do evaluation to do good training. And, evaluation and training will have to look broadly at the context of training—the organization into which we want to inject training results—as well as, probably even more than, the training programs themselves.

The following 2x2 matrix shows two major dimensions of training: quality, and strategic value. All training varies along both these dimensions. Some training is far more important than other training, as this question is always relative to strategic goals of an organization. Clearly, for example, security awareness training (no matter how good) is of very little value where security is of little concern. On the other hand, where security lapses can quickly and critically damage strategic goals, the value is very high. Likewise, as we all know from painful experience, some training is "better" than other training. Some training is a joy, and runs smoothly, teaching well and thoroughly. Other training is misery, drags on interminably, and teaches little except a strong dislike for the perpetrators. I think that we can, and should, use systematic evaluation to assess both these critical dimensions, so that we can maintain high quality, badly needed training, improve badly needed training that doesn't work well, dispense with unimportant training regardless of how well it works, and stop improving training that isn't needed in the first place.

When it comes to defining training, I maintain that all training is alike in that it has virtually no intrinsic value. As the figure below shows, training value derives from whether training results endure, to be used and referred to in the work place. The logic of training insists that training be (a) clearly tied to important work place behavior that leads to important organizational results, and (b) that training provide learning results that clearly tie to the important work place behaviors. If we are to evaluate training value, then we can only do so by collecting information within and about the work place. Evaluating only the training event (the left-hand side of the figure) can only lead to more quality, but can address nothing of value. That is, we can improve learning effectiveness by evaluating the training event, but we can discern nary a clue as to whether the training has any value unless we venture into the right-hand side of the figure, the work place.

When training as a function can be crippled is when the administrative bureaucracy of training removes training decision makers from the arena of





training value. If trainers spend all their time and energy in training "centers," then the risk is great that they do well, or even increasingly better, what isn't worth doing in the first place.

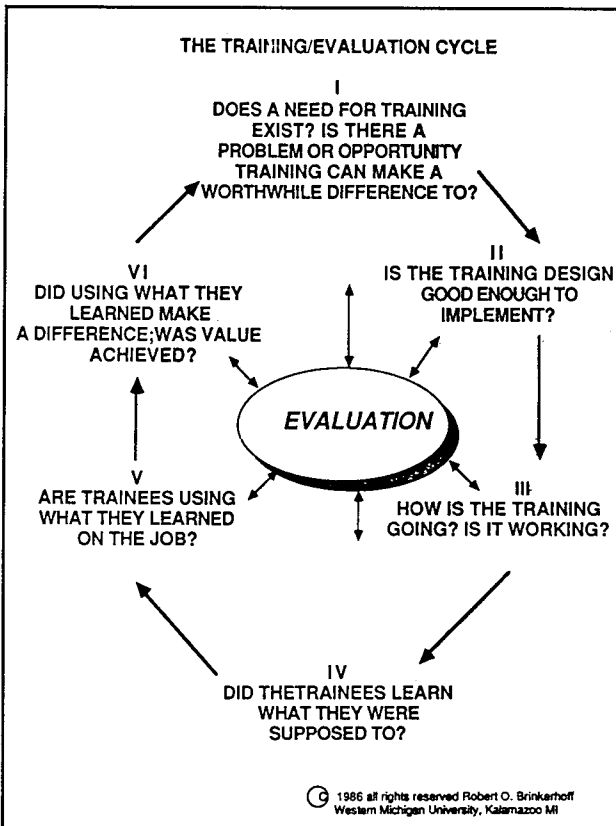
Evaluation is our bridge to the value arena; we need evaluation to keep in touch with needs, with usage,

and with workplace realities.

THE LOGIC OF TRAINING - AN EXAMPLE			
Who is to receive training?	What skills, knowledge, or attitudes will be changed as a result of training?	How will recipients use the new SKA--what on-the-job behaviors will change?	What social/organizational benefits will accrue?
CAFETERIA LINE SERVERS	* AWARENESS OF RESULTS OF CUSTOMER WAITING * KNOWLEDGE OF REPLENISHMENT GUIDELINES * SERVING SKILLS * K & S IN RESPONDING TO CUSTOMERS	* MORE PLEASANT AND ACCURATE RESPONSE TO CUSTOMER QUESTIONS * SPEEDIER REPLENISHMENT OF DISHES * ADHERE TO SERVING GUIDELINES	* DECREASED CUSTOMER WAITING * INCREASED CUSTOMER SATISFACTION * INCREASED CAFETERIA USAGE
SUPERVISORS	* AWARENESS OF LINE-SERVER SUPERVISION NEEDS * AWARENESS OF ACTUAL WORKING CONDITIONS * K & S IN SUPERVISION TECHNIQUES	* INCREASED SUPPORTIVENESS IN INTERACTIONS WITH LINE-SERVERS * INCREASE IN APPROPRIATE & TIMELY SUPERVISORY ACTIONS	

© copyright 1987 all rights reserved
Robert O. Brinkerhoff

I have designed and used frequently the 6-stage evaluation model (on pp. 103 and 112) that I, and others, have found useful in keeping training's eye on the strategic value ball. This 6-stage model ties training and evaluation together, and defines evaluation as the information gathering function that informs each of six critical training decisions. First, is there a need for train-

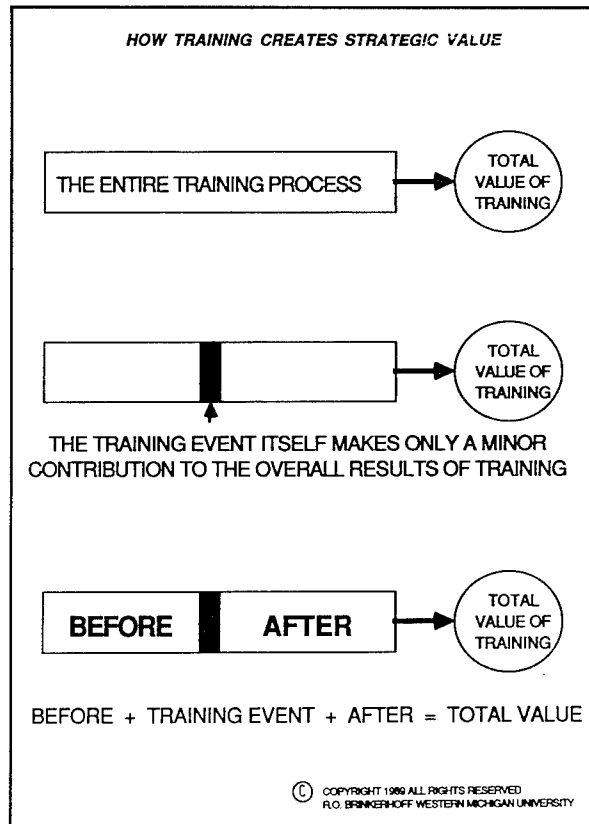


ing, or a problem or opportunity to which training can make a cost-effective contribution? These opportunities and problems need to be systematically evaluated to keep training goals aligned with important needs. Secondly, is the design chosen — or, which of the design alternative possible to choose — the best? Will it work to meet the goals? Thirdly, given that the goals are needed and that designs are valid, is it working? This third stage of evaluation is tantamount to control; it involves collecting operational data to be sure that training is moving as planned, and as needed, in right directions. The fourth through sixth stages examine results of training, at key levels of effect, from immediate learning results, through usage (or

retention, in the case of capacity training, such as giving persons the capability to perform when conditions warrant), to organizational impact. The table on page 112 lists the many evaluation techniques available for each of the stages. This, then, is the way that I see evaluation tying into training. And the six stage model shows the overall strategy of evaluation. The problem remains, of course, as to how evaluation should be characterized and pursued in security awareness programs. I want to turn now to some thoughts and issues that I think you may find useful in guiding your thinking.

One of the ideas that I think we need to look at and think about is: Where and how we do evaluation of training and even where and how we spend our time in training. In the top third of the following diagram, the rectangle represents the whole training process—that's everything you do in thinking about and doing training. And if the circle is the total value, that training returns to your organization, wherever you are. And notice that I have defined the result of training in that circle as *value*; not learning, not behavior, but *value*.

Then I want to ask the question—How much difference to the value of training does the training event itself make? And what I mean by the training event is the engagement of the learner with the learning materials or the instructor. So the training event is what happens if it is a workshop when people come in the door, until the time they leave. If it is a briefing, from the



time the briefing starts until the briefing is over. If it is computerized instruction, from the time they flip the computer on until they flip it off, that's the training event. And how much of the total value the training returns is accounted for by the training event? I tried to draw that to scale, except that if I drew it truly to scale I don't think you would be able to see it. My point is that the training event itself probably doesn't make a whole lot of difference.

How well you do the training doesn't make as much difference as how well you *plan* the training. You can do it well, but if it wasn't a good idea in the first place, it's not going to bring back any value. And if you don't support it afterwards or if you don't assure that *somebody* supports

it afterwards or if you don't assure that it fits with the support system that is in place in the organization—then it won't return any value. That is, *what you do before training and what you do after training is what makes training pay off*. Another way of saying that is by the time trainees arrive at a training session most of the value of that training was already fixed, and there isn't a whole lot (if it wasn't a good idea) that an instructor and materials are going to do to turn that around.

Now what we need to ask ourselves is: if we are going to evaluate training, where should we evaluate? I'm saying we can probably leave this, the training event, pretty much alone. What we should evaluate is how well we plan and design training and how well training is supported on the job. Evaluating the event itself isn't going to give you a lot of leverage; it is not going to pay off a lot for two good reasons. First, it doesn't really matter a whole lot and secondly, you already probably do it really well. Most training transactions themselves are pretty well designed and they're not bad.

Where we need to get better is the before and after zones. There are some other ideas that are compatible with this and have shaped my thinking considerably. I've listed three of them in the chart which follows. One is the notion that really transformed manufacturing and that is "just-in-time inventory," or in Europe, that would be called "zero stock saleship." It's what the automobile companies now use. Rather than putting their money into having a lot of parts in inventory, they plan production on a daily basis and

use up all the parts so at the end of the day, they have no inventory left. And that has given tremendous profitability and leverage to the production process. I think there are great implications for training in that as well.

Most training programs front load training. They give people all kinds of stuff way before they need it. We front load them with skills and knowledge way before they are going to need them. Let me give you an example from when I was in Officer Candidate School back in 1964 in Newport, Rhode Island, learning all about how to be an officer. I also got some security awareness training; we saw a movie about how sexy Russian women would try to get us to tell them secrets (secrets we didn't even know yet, by the way) by luring us into bars and trying to get us to tell them the secrets. And I still remember to this day my reaction to that. Afterward some friends and I went out on to the marching field to march off some demerits. We talked about it and wondered where those bars were where those ladies hung out. But when I *needed* the security training was when I got to the job where I was supposed to use it, and that's where I *didn't* get it. So giving training when the behavior that requires the skill and knowledge is needed, "just in time" training, that's something I think we could look at. And that involves our getting to know the training application arena pretty solidly.

A second notion that really drives the evaluation of training and can pay off a lot is quality assurance. Edwards W. Deming tried to tell American industry. The Japanese listened. He said if you want quality, shoot the inspector. You can't inspect quality into a product. You must engineer it in. If you want to do quality training, don't evaluate it after the fact, because if you wait to assess the quality of training until the training is all done, you can save yourself the effort—it probably doesn't have much. Build it in, up front.

SOME USEFUL PARADIGMS FOR TRAINING - NEW THOUGHTS FOR THE 90'S

1. "JIT" Inventory (a.k.a. "Zero Stocks")

Needs driven vs. Program driven training strategy

2. Quality Assurance (vs. evaluation)

Engineer quality into training

Quality assessment at each step in training design, delivery, follow-up

3. Customer Service

Who are training's "customers"?

What are customer expectations and needs?

Are they satisfied?

The quality assurance process requires that we "explode" the production process into its steps and parts and then assess quality at each step, "shutting down" the line if you get negative results at any point. That is, don't go further, unless all quality indicators are positive.

And the third, very powerful notion is that of *customer service*. Customer service has transformed a number of organizations. One thing that is so powerful about it is that it asks you a very important question— who is your customer? For whom are you providing this service of training? We need to know who our customers are. I think that one thing that has happened to us in the training profession is, we've increasingly come to see our customers as the trainees. And thus, we do everything we can to entertain them, to keep them happy, to make them like us. And they may not be our primary customers, and in many cases they are only one of several customers. We need to know who our customers are, what they expect, why they expect it, and why they need what we can give them.

Now I have put all those things together to create a paradigm for training (as opposed to an education model). I've laid it out in the following chart as it might look for the computer industry in which I've worked. IBM or another company goes into a large organization to sell them a computer system, the "install" which is the parallel of training. The install is a *minor* part of the work they do. What they do is a whole lot of work up front to get to know the customer, get to know the users, understand their characteristics and their business means. Then they design a system that will give them just what

Putting it all together: Training as Service/Product Marketing (vs. Education)

Our "product" = new skills & knowledge

The marketing & service process:

- * Determine business needs, opportunities, user characteristics
- * Match products to needs
- * Help clients prepare for transition
- * Do quality "installs"
- * Provide user service
 - follow up troubleshooting
 - assess success of usage
 - identify new needs as business changes
 - provide upgrades as needed
- * Assure quality throughout
- * Keep the customer happy!

©1990 R.O. Brinkerhoff
all rights reserved

they need. Then they spend a lot of time supporting that customer in use of the system. And the way I look at training is, training is equivalent to providing somebody with a new computer system, because if it were potent when you send that person back into the job place, they have a new awareness, they

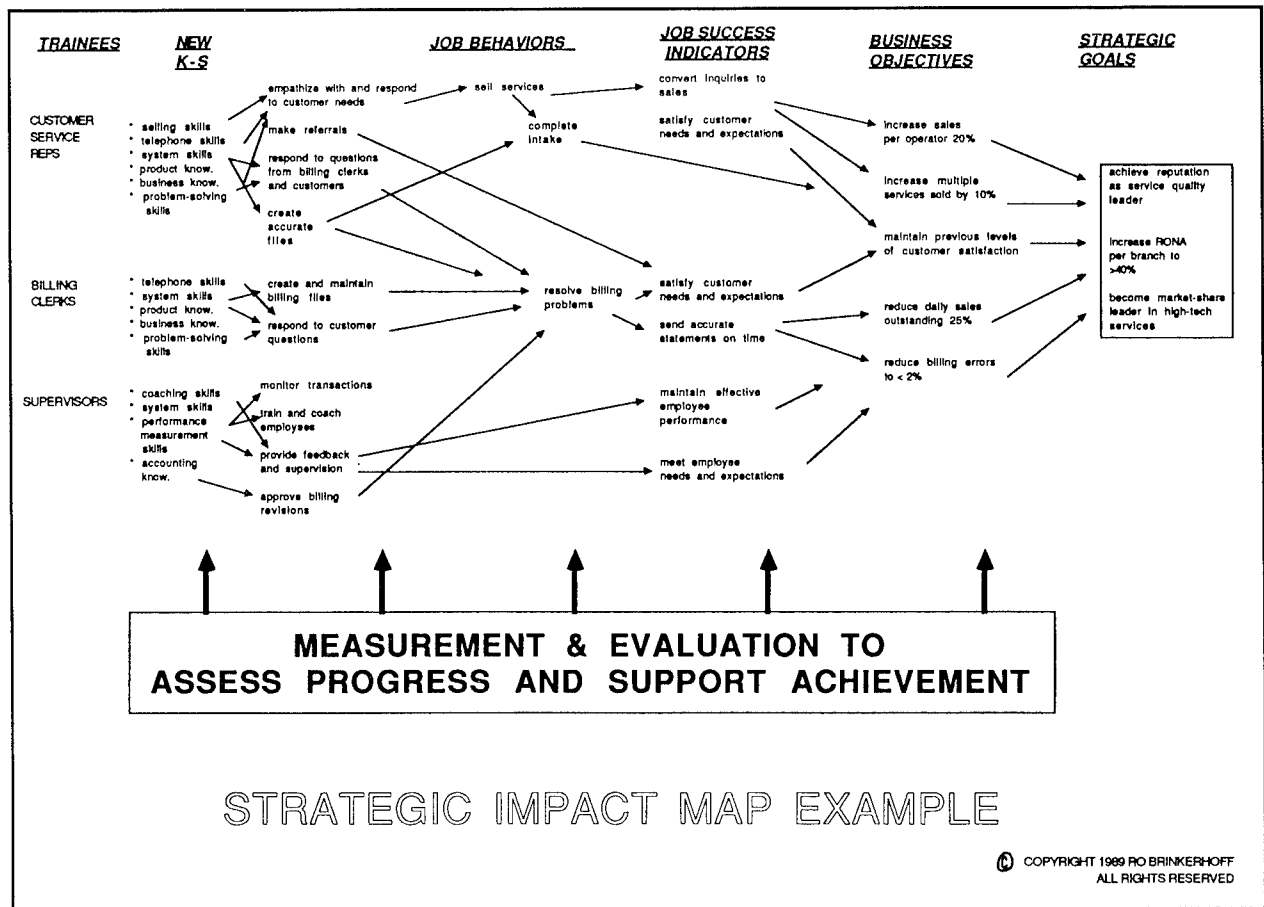
have new skill, and they have a new knowledge that they for sure won't use unless it's supportive. And they for sure won't use unless there is a real good need and that need has been made crystal clear to them at the beginning.

Now the next two diagrams are an example from working with a recent client who was a customer service provider where the training was supposed to train all the employees in how to follow new procedures for billing and accounting, and interacting with customers. And what I show you here is partitioned by before, during, and after. Some of the critical evaluation questions

we asked, and then on the right hand side, some of the methods we used to answer them.

EXAMPLE: CUSTOMER SERVICE SYSTEM TRAINING		
A MAJOR SERVICE PROVIDER RE-ORGANIZED THEIR OPERATION. THE "OLD" BUSINESS WAS LARGELY HAND-WORK AND PAPER DRIVEN, PROVIDING SERVICES VIA 300+ REGIONAL OFFICES. THE NEW BUSINESS EMPLOYS FAR FEWER PEOPLE IN ONLY 4 "SERVICE CENTERS", AND USES A NEW COMPUTERIZED TELEMARKETING SYSTEM TO SELL, COORDINATE, AND BILL FOR SERVICES.		
SOME EVALUATION QUESTIONS		METHODS
B E F O R E	* What are the strategic goals for the company?	- interview management
	* How will business success be measured?	- Observe job performers
	* What job results are most important for success?	- Analyze job descriptions
	* Who are job "customers" and what do they expect?	- analyze other industries
	* Which job performers are most successful now?	
	* What skills are most important for job success?	
	* What skills do supervisors need?	
	* How appropriate are current training materials?	
	* What skills can be best supported with job aids?	- Review division training materials
	* What is the least training we can do?	
D U R I N G	* How willing and able are supervisors to participate in training?	- Analyze job requirements
	* How "job-like" are the exercises we planned?	- Interview supervisors
	* Do our performance checklists accurately and adequately assess needed performance?	- Review draft materials with management
	* Are trainees keeping up the module completion pace?	- Observe training
	* Who is having trouble learning?	- Test performance
A F T E R	* Are supervisors adequately assessing learning?	- Interview trainees
	* What other skills and knowledge have to be included "on the spot" during training?	- Analyze performance scores
	* How well did trainees perform in the simulation?	
	* Do supervisors provide immediate and accurate feedback?	- Track complaints
	* What proportion of inquiries is converted to sales?	- Analyze performance data
	* What is the billing error rate?	- Interview supervisors
	* How accurate and timely are statements?	- Observe performance
	* What are customer opinions of service?	- Analyze telephone data
R	* What problems are coming up?	- Survey sample of customers
	* What is the call abandonment rate?	

The next diagram is based on an analysis we did at the training that represents the same thinking that I've used in looking at the logic of training. What I'm trying to do with this (what I call a map), is show how training relates to the strategic goal of the organization. In the analysis we did with this training, we started way on the left-hand side with who the trainees were, and the knowledge and skill that the training was to give them. And then what we worked through was how that would impact their job behavior, how if their job behavior were impacted, the indicators of success that we would see (measurable indicators), how those job success indicators transformed themselves into business objectives, and how the business objectives



impacted strategic goals. So when we were asked the question, how does this training *fit*, that was the answer. It fits this way, that's why you need this training. And what do I increasingly do with clients now in working with them to evaluate training? I draw maps like this, and sometimes it takes a lot of work to draw the maps, but it has always been worthwhile, because it's clarified to the critical customers, in particular to the people who are paying for the training: Why they need the training and how it fits. And to me one of the biggest issues in evaluating training and defending training is not saying that we do it well, but it's making the argument that it *fits*, we *need* it. And if you cut the training out, you jeopardize some of the critical goals of this organization. I tell them, "Let me show you how this training fits." And then we simply measure and evaluate along the way as we implement it to demonstrate that it does fit.

Let me just walk through some suggestions that I would have for you, if I were doing some evaluation of training:

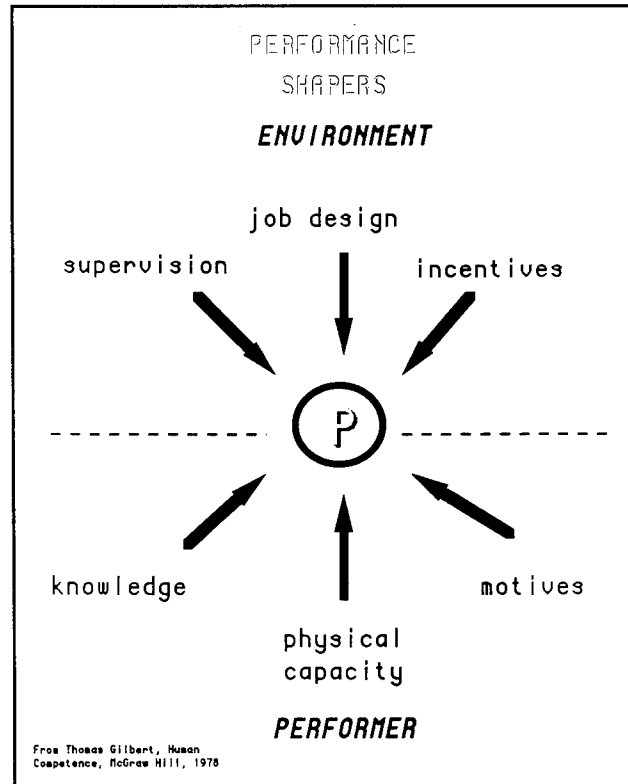
- The first recommendation is disaggregate the training. Be very specific about the training you want to evaluate. You cannot evaluate security awareness training in general. You must disaggregate into a specific training program and you can evaluate those. (I will conclude my presentation with a couple of suggestions for those whose concern

is *all* for security awareness training and how we might do some evaluation about that.)

- The second recommendation is work with customers to specify the logic of all the training that you do. Work with your customers and draw maps and complete those logic of training forms; be really clear about what are the objectives of training and how does it fit.
- The third recommendation is to embed evaluation. Look at evaluation like quality assurance. Embed evaluation into training. Begin doing evaluation when you begin to think about training and embed the evaluation into the training. Good training has invisible evaluation; it's built into the training. When I give people a test at the end of training, it's to let them know how well they're doing so they can modify their behavior to do better. It isn't to measure whether I did it or not; it's a part of the training process.
- Another recommendation is prioritize programs; use the four-cell matrix, the two dimensions of quality and strategic value of training programs and prioritize your training programs. Not all training has the same value, not all training has the same quality. Use evaluations to prioritize programs and you may reduce the amount of training that you do. And it's nice, by the way, when *we* reduce the training we do, rather than let *them* reduce the training we do.
- Another recommendation would be to evaluate alternative designs. Do stage-two evaluation. Think about those programs that really have too much stuff in them—are given too early to truly impact behavior—and think about the "just-in-time" inventory notions. Let's not front-load training so much, let's evaluate alternative designs. Jack Boucher who is director of training for IBM, in his book, *Educating America*, urges us to redesign training to make every 10 minutes count. Look at all the training you do, even in a five-week training program, and make every 10 minute segment count. And if it doesn't count, get it out—clip it. Another thing I would do when I was evaluating alternative training is I would be wary of "general training." General training which is meant to fit is just like suits that one size fits all. They usually don't fit anybody. Target training. Make training specific. Pick an organizational goal that needs to be met and target training on it in a specific place. Now, these next couple of recommendations could apply as well to the policy level.
- Use success cases and critical incidents. What do I mean by success cases? I referenced that method on the 6-stage model handout. If I have 100 people that go through training and I have the question, "Does this training do anybody any good? Does this training work?"

Does everybody use it? Does it stick?" I don't have to follow a whole lot of trainees up to find that out. What I do is I'll pick out the 3 or 4 people that clearly were successful in the training—and I know they were because I measured whether they had learned it or not, and they clearly love it and liked that training—and I know that too because I ask them that. And I'll pick a handful of those people—two or three people who really got out of the training what we wanted them to get out of it. And then I'll find out what they're doing with it.

They're like the pioneers; I will assure that if they're not using it *nobody* is. If it didn't stick with them, it didn't stick with anybody. That's what I mean by success cases. I can apply that to programs as well. And critical incidents studies as well; looking at—and I know that you produce these and do research on them—security violations. (I like to think as well that critical incidents could include situations where there might have been a security violation and there wasn't.) Then do some analysis of those from the perspective of what role *training* played in these violations. Did somebody not do what they were supposed to do because they didn't know it? What was the role of training? I would refer you to the last diagram, something called Performance Shapers. I've drawn this from the work of the behavioral psychologists who tell us what we already know and help us understand it—that training is only a bit player in the performance puzzle. The way people behave at work is influenced by a lot more than what training gives them, skill and knowledge. It's influenced by supervision, and job design, and incentives. So I would say that when we look at these critical incidents, let's look at what was the role of supervision, job design, and incentives as well; and as Henry Halff pointed out to us, we probably need to build far more incentives in, positive incentives.



- Do some evaluation that shows how much you spend on training. Now, a lot of times in training we want to keep that kind of quiet be-

cause it's a pretty big number. But what I would want to do is show it *relative* to, in this case, the cost of the whole security program. What does it cost to have the procedures? What does it cost to classify information? What does it cost to control information that is classified? What does it cost to supervise and implement? That's *massive* dollars and I'm betting that training and security awareness is only a tiny fraction of those. And I can show that the relative cost is very low and that's going to help me argue return on investment.

- And the eighth recommendation is: Tell the story. Evaluate some of this training. Don't wait to be asked if your training is paying off. Find some that *is* paying off, maybe get Bob Bailey to help you advertise it. But tell the story. Training works. And I don't expect you to take that on faith. Let me give you a story. A lot of trainers say, "Gee, nobody asked us for evaluation information." Well, I use the dope dealer approach; give free samples. It works!

THE 6-STAGE EVALUATION MODEL
"Evaluate Your Way to Worthwhile Training"

STAGE	SOME KEY QUESTIONS	SOME USEFUL METHODS
I. Goal setting: are training needs and opportunities worth pursuit?	- What's the problem or opportunity? - Is it worth fixing? - Who could be changed? - What kinds of learning and behavior changes are needed? - Would these changes happen? - If these changes happened, would the problem or opportunity be "fixed"?	surveys; performance audits; records analysis; "front-end analyses"; interviews; panel and group reviews; nominal group technique; research studies; brainstorming; site visits; case studies; expert opinions.
II. Design evaluation: is the design good enough to implement?	- What alternatives exist? - Which alternative is best? - How good is training plan "X"? - Is Design A better than Design B? - What revisions need to be made? - Is it likely to work? - Is the plan ready to implement?	literature reviews; trainee reviews; expert reviews; checklists; pilot tests; visits to other programs; experiments; research data; feasibility studies; comparative analyses.
III. Program implementation: is it working?	- Is it installed as per the design? - What is really happening? - Is it on schedule? - Is it on budget? - What problems are cropping up? - Are enabling (interim) objectives being achieved? - What, in fact, took place?	observations; checklists; logs and diaries; participant feedback; "happy sheets"; record reviews; participant observers; key informants; interviews; artifact and refuse analysis; "wear and tear" analysis; user records.
IV. Immediate outcomes; were skill, knowledge, attitude objectives achieved?	- Did they learn it? - How much did they learn? - Who learned it? - What did they learn? (unanticipated outcomes included) - How well was it learned?	knowledge and performance tests; attitude measures; pre- and post-testing; self reports; trainer reports; observation checklists; simulations; work-sample and product analyses; quizzes.
V. Usage and re- tention: are on- job usage and retention objec- tives achieved?	- Who is using it? - How well are they using it? - How is it being used? - What parts of it are being used? - What is not being used? - Who is not using it?	self, peer, and/or supervisor reports; records analyses; surveys; visits; observation; "success-case" studies; follow-up surveys; work-sample analyses; logs and diaries; performance appraisals
VI. Impact: did it make a worth- while difference?	- What difference did using it make? - Has the need been met or reduced? - What else has resulted? - How much difference did it make? - How much are differences valued or worth? - How do results compare to costs?	surveys; performance audits; records analysis; interviews; panel and group reviews; nominal group technique; profit-loss studies; productivity measures; cost/benefit analyses; corporate performance measures.

© 1986 all rights reserved Robert O. Brinkerhoff

Discussion moderated by Richard S. Elster, Dean of Instruction,
Naval Postgraduate School

We have selected the following transcribed excerpts from responses of the panelists in this section to questions from the floor.

Question: A question to Roger Denk: Has there ever been any consideration by PERSEREC or other elements of looking at the emotional impact of advertising aimed at security awareness?

Dr. Denk: I am not sure that advertising techniques have been employed in security awareness. I have been involved in the production of a video, as some of you may know—with the cooperation of the Hughes Corporation and the Federal Bureau of Investigation. This was an instructional video as opposed to advertisement. I think there's a vast difference. The video is about 30 minutes long—the average commercial is from 15 to 30 seconds—but yet the impact, it might be argued, is equal. At PERSEREC we have not focussed on that yet, but I would recommend to the group that this is something we should do.



Dick Elster, Bob Brinkerhoff, Bob Bailey and Henry Halff

Question: Was there ever an evaluation after World War II on how effective that program of "Loose lips sinks ships" was? Did it result in fewer ships sunk by U-boats or not so much information getting into the hands of the enemy?

Dr. Bailey: I have never been aware of any evaluation of that program. At that time in advertising it would have been really unusual to have had research to evaluate a program. In fact even today when you get into so many public-issue kinds of campaigns there is very little evaluation being done. The best evaluation work being done is in the big packaged goods corporations in the United States like General Mills and Pillsbury, and so on.

Dr. Elster: Could one structure an experiment to take a look at the effectiveness of personnel security awareness advertising?

Dr. Bailey: I believe you could do that. And one of the things we are often involved in is putting together experiments on a pre/post basis with test and control groups to look at the effectiveness of that kind of work.

Dr. Elster: I would like to ask the educators here before me, do you think that improved security awareness leads to improved security?

Dr. Brinkerhoff: I want to respond to that because, coming back to the question that was asked earlier about whether the poster actually saved a ship from being sunk—if I'm going to evaluate a training program or an ad campaign as well, the first thing I do is to show why it's very important why people have an attitude because an attitude is going to lead to predicted behavior. And a behavior that would have drastic consequences, like a ship being sunk. I don't need to go out and collect evidence or invest in a research study. I think it would be a waste of time in fact—to try to show that a poster saved a ship from being sunk or a training program saved us from a multi-million dollar security breach. What I would show first is that the training did fit, for example, that it was a good poster and that I hung it in the right place where the right people would see it. I would also find out whether anybody saw it or not. And at that point I would rest my case.

Question: A question for Dr. Brinkerhoff: What are some management strategies that we might adopt to deal with shrinking budgets with regard to security education?

Dr. Brinkerhoff: The first thing I would try to do is to preempt the cutters; I would do some cutting myself. What I would want to avoid is an across-the-board sort of training reduction because a lot of babies are going to

get thrown out with the bathwater. So I would try to do some prioritization, as I mentioned in one of my recommendations, and find out which of my training is most important and which of it seems to be working best. Then I darn sure would try to hang on to that training by preempting (the cutters) with some evaluation of my own. We are never faced with the question of should we evaluate training, or whether to evaluate training. Training is always evaluated. The question is who is going to do the evaluation and how well are they going to do it? I'm recommending us!

Question: A question for Dr. Bailey: I seem to recall that you indicated that you have a trade-secret technique for assessing your customer and his needs before you make your sales pitch or presentation. Can you give, without revealing what kind of methodology, some indication of your approach to us as a group and how you looked at us and what you thought our needs might be?

Dr. Bailey: I must confess that I only talked to Lynn Fischer and he gave me a short briefing about what your needs and interests might be. But I like the spirit of your question, particularly because I believe there is available to you in advertising research a whole set of technologies which are really in the public domains—they are not really trade secrets—that might be carried over into your area to help you define what to say to your trainees and how to best say it in order to motivate those people to increase the odds that they will exhibit the appropriate behavior in the security area.

Dr. Brinkerhoff: I wish to respond to that as well because I think that advertising and training need assessment which share many of those technologies. For example, the focus group. And it's no trade secret—just talk with people, just talk to your customers. They will tell you a lot.

Question: A question for Dr. Brinkerhoff: How can we reconcile the two issues of increasing centralization of training product development in the Department of Defense in the interest of efficiency and cost reduction and the need to develop training which is designed to meet very specific needs?

Dr. Brinkerhoff: I think that you are absolutely right that they are two issues that need to be reconciled. One of the problems we face in training, particularly in business and industry, is our own success. As training has become more integral and as more money is being spent on it, we have our name on the door. We have a Training Department, and what that centralization has given us is some benefits like better instructional design and better access to resources and higher quality programs with greater workmanship. But the downside is that we are removed from our customers

and we stumble over our bureaucratic selves in training and we don't understand the needs as well. So what I think we need to do—I'm not recommending that we decentralize training—we can try to decentralize our thinking by using more evaluation and more communications techniques to stay in touch with all of those various customers and clients we have. We can do evaluation, get feedback and I would say develop core training materials and techniques and also encourage their revision and customization on site. And yes, you do run a risk of their not being used well. But again, I think if the need has been identified well, and there is support for following it up, then if they're not used particularly well, you have at least done your part.

Dr. Halff: I think what has been said already needs to be said in a different way. The question that is posed is part of the larger question of training for the entire security community. I think it's a mistake to think that you are thinking only about how to design training. What you should be thinking about is how do I design a process for protecting information and in the course of designing that process, you will answer the question just asked. What are the responsibilities that come with the job of security officer? What are the responsibilities of cleared individuals? And at that point you will have an answer to that question about which of these are specialized, which of these are specific to particular facilities or jobs, and which can be promulgated more generally to avoid re-inventing the wheel. But you can't just think about designing training alone, think about designing a process or system for protecting information in this country.

Question: A question for Dr. Brinkerhoff. Many of our programs are based on minimum requirements or minimum standards for awareness programs in the community. Should something be done in the policy arena to evaluate policy and to deal with this spray-and-pray approach to security awareness?

Dr. Brinkerhoff: I certainly agree with you on that. I have worked in the nuclear regulatory arena where required training happens over and over again, and it's an opportunity for a lot of trainees to catch up on sleep. There is a problem. The fit between good training practice and policy is probably never going to be a good one because most of the people writing policy don't understand what training is. So I think what we will have to do is show them alternatives, show them the down side, and then give them something better to work with. And there certainly are better alternatives.

Dr. Elster: I would like to ask Henry Halff a question. In your talk you spoke of having an individual practice whether or not to collaborate in a safe environment? Could you elaborate?

Dr. Halff: Yes, when you are actually approached by a spy in a bar or where a spy happens to approach you, it's in a situation in which lots of things can happen to you that can degrade your ability to make an appropriate decision. What I would like to do is to say, all right, I am going to set up a situation in which you imagine yourself in a bar, do a role-play. You're approached and at particular times in this role-play you say, "Okay, stop the camera." What might cause you to go one way or the other way? Let's do a Ben Franklin chart for this decision. Let me as an instructor tell you what I know about what has happened in the past about these decisions and I want you to make the decision now, so that when you get into the dark bar, you won't have to worry, you will have made the decision, you will know what you are going to say.

Question: This is not so much a question as it is an observation based on the excellent discussion today. And it's thinking back to a comment that Maynard made earlier about those four words, "Ask what they think." Maybe one useful approach to analyzing our customer, that is the people we need to brief, is to cut them apart in terms of functions—the engineer, the administrator, the riveter, or whatever those groups are—and seek their input on what they think would be useful to motivate their kind of people on security awareness.

Dr. Denk: We are engaged in a major research project to do just that. PERSEREC has been out looking at security awareness in the DOD. We will report soon, by a technical report and briefings, about what has happened in that project. Tomorrow when Jim Riedel is speaking, and from others on that panel, you will hear some of the initial plots, not the results, of where we are now.

Mr. Anderson: May I respond to something I have just heard. On doing a Ben Franklin tree on a surreptitious approach in a bar. I think it's sort of dangerously misleading for one very fundamental reason. And that is, most of our spies in the past few years have been volunteers. That decision, whether to become an enemy agent or not, or to commit espionage, is done before any kind of contact with a foreign intelligence agent in most cases. So most espionage offenders in the United States have not been recruited in the James Bond scenario. They are recruited by an insidious, long-term, very slick advertising process, used very effectively by well-trained foreign agents.

Dr. Halff: That's a good point, and what you've just managed to reveal is my lack of knowledge about this whole business. But I think my general point still holds and the two principles are these: one is, get to them early—whenever they confront the decision. If you know when or how they

decide, all the better because then you can recreate the situation. And second, even if they have made the decision, maybe you want to bring them in and say, "Let's reconsider this." This is not anything new. We have studied this in the late 60s, there are a number of experiments on this, and I would be willing to bet that this would be an effective technique for security training.

Dr. Elster: Let me propose an extreme interpretation of what I heard from Bob Bailey today. We are going to have an organization where we all snitch on each other at the least opportunity. Is that what you envision?

Dr. Bailey: Actually, that's not what I envision, but what I do envision is that whatever advertising program you might consider putting together, you really need to define the purpose and objective of that program very tightly. I couldn't do that for you but I imagine it might be somewhere in that general domain.

Question: To Dr. Halff: With regard to your idea of forced-choice, are you using or basing your comments on Festinger's cognitive dissonance theory?

Dr. Halff: Take your pick. There are any number of them, and social psychologists are still arguing about exactly what theory can best account for these effects. But the effects are still there. Let me make a comment on the snitching-on-your-neighbor problem. I think—again, returning to the fact that you are designing a system for protecting information—it's possible to ask for too much security awareness. Remember, your clients or customers just want to protect the information. They really don't care how aware people are. If you are asking people to be so concerned with security that you are detracting from their other duties, then you are not meeting a client's needs.

Comment from the audience: I think that if you develop a security education awareness program effectively, you can't have too much. It becomes second nature to the point that the employees don't have to consciously think about certain things, they just do it properly. It just becomes a part of their being on and off duty.

Dr. Brinkerhoff: And that would take more than training. That would take some follow-up and feed-back to shape that behavior and make it stick.

Dr. Elster: I have a question for Dr. Brinkerhoff. As I heard you, I believe you said that training doesn't work unless it occurs in a context of other

interventions including incentives, job design, supervision—did I hear you correctly?

Dr. Brinkerhoff: Yes, I guess it's coming back to the notion that training has to fit. And the strongest training force in any organization is the organization itself, not the training. The organization can untrain people 10 times faster than you can train them. So you have to know the wind that you are training into, and you have to train a lot of different people. I not only want to train people to follow rules, I want to train their supervisors to measure whether they follow them or not, and reward them when they do. And I want to train their supervisors' bosses to make good rules, and I want to train their bosses to write policy that permits good rules to be written. So I have to know what the organization is in order to train in harmony with it and not against it. And we all know that the organization will untrain anybody quicker than you can train them and so you have to know what those forces are and then you can fight them.

Planning for the Future

Current Problems

James A. Riedel, Program Manager, PERSEREC

Deborah Russell Collins, Security Consultant, Collins Consulting Group

Ernest V. Haag, Western Regional Manager, HumRRO International, Inc.

Joseph A. Grau, Chief, Information Security Division, DODSI

Strategic Planning

William E. DeGenaro, Director of Business Research and Analysis,
3M Corporation

Discussion

Moderator R. Everett Gravelle, Director, DODSI

Dr. Riedel joined PERSEREC in July 1989. He has conducted and supervised personnel research for the Navy over the past 15 years. His research interests include organizational behavior, management, organizational design, and planned organizational change.

Contextual Factors that Influence Security Awareness

by James A. Riedel

Our panel this morning has the task of addressing the current state of security awareness. Our objectives are to identify problem areas, or impediments to security awareness, as well as to suggest some improvement strategies to remedy these problems. Some of the observations you will hear are based on current PERSEREC research activities, and others are based on personal experience. Our goal is to stimulate thinking about ways to foster security awareness.

Objectives of Panel

- Identify Problem Areas
- Suggest Improvement Strategies

Does anyone really care about improving security awareness? I think most of us do. Many of us are attending this symposium because we believe security awareness is important. Why is it important? I suspect that most of us believe, or at least hope, that people, when aware of their security responsibilities, will meet them. In a way this awareness is the cement that holds the security system together. No matter how many electronic devices and safes we employ to control behavior, we know that good security ultimately depends on individuals to do the right things.

Each of the panelists this morning will discuss problems and improvement strategies from a slightly different perspective. Ernie Haag will focus on the government, particularly the Department of Defense. DeeDee Collin's observations will reflect her experience in defense industry. Joe Grau's views will reflect his role as a security educator. I too have as an objective to identify problems and improvement strategies. But my focus will not be on the state of security awareness in the field. I will consider a more general problem, defining security awareness. I will address two questions: What is security awareness? How can we influence it?

These are not trivial questions. Our view of security awareness colors what we see as important to understanding it and improving it. You might say our view of security awareness gives us a set of lenses for deciding what is working well, what we see as wrong, and the improvement strategies we are willing to consider.

I believe that a commonly held, and perhaps predominant, view is that security education is the most important and primary determinant of security awareness. It is based on the assumption many of us make that if we properly train people, they will know what to do and then will do it. This view is over-simplified and narrow. This assumption itself is an impediment to improving security awareness.

How We View Security Awareness

"Properly Trained, People Will
Know What To Do,
And Then, Do It."

I would like to share with you a story to make the point. It was told to me by Steve Garfinkel. As some of you know, PERSEREC currently is conducting a baseline assessment of security awareness training and education (SATE) in the Department of Defense. In the early stages of the study, I had the opportunity to visit Steve and some of his staff at ISOO in Washington, DC. We talked about our research plans and security awareness. When our discussion turned to the subject of increasing security awareness, Steve related a story about an ISOO inspection of a small foreign affairs agency (not the State Department). In the course of this inspection ISOO inspectors observed, among other things, an unacceptable rate of security infractions and a poorly functioning security education program. ISOO recommended that the agency improve the security education program. In fact, after the inspection an ISOO liaison even provided the agency with advice and assistance in developing the new program.

In the course of a follow-up, a year after the new program was implemented, ISOO found that the agency now had an outstanding security education program. Things had really improved. The instructional materials were first rate and agency staff were actually getting the required training. The agency did exactly what had been recommended. There was only one problem. The agency was still plagued with an unacceptable high rate of infractions.

Steve and his staff were surprised. The security education program had no impact at all. It seemed reasonable to have expected that improved security education would have increased security awareness and, thus, had some impact in reducing the rate of infractions.

So what was going on? Clearly, a number of other potent influences were at work. If there is one thing that I've learned about understanding and changing behavior in organizations, it is the importance of context. Behavior does not take place in a vacuum. Applied psychological research has pointed to the importance of context in understanding and improving organizational behavior. Outstanding security professionals, as well, have recognized the importance of context. PERSEREC discovered this in a study of effective industrial security programs.

Context And Security Awareness Behavior

- Academic Research
- Beyond Compliance
- Improved SATE Requires More Than "Just A Better Briefing."

The findings of this study were reported in a PERSEREC publication, *Beyond Compliance*. A key finding of the study was that the quality of the instruction and instructional materials were only a small part in determining the effectiveness of security education and training programs. When asked, Facility Security Officers (FSOs) reported that contextual influences—both management and motivational—also were crucial to their success.

For example, effective FSOs conducted training needs assessments, carefully planned and timed the implementation of their programs, and made sure that they had sufficient resources to be successful. On the motivational side, the FSOs involved managers and employees, alike, in the overall security program and also considered consumer needs in developing the training content and media. These management and motivational practices were key to the success of the education and training efforts. Improved security awareness education and training required more than "just a better briefing."

So what do these stories tell us? I think they suggest that security awareness results from much more than education and training. Sure, education and training are very important, but we need to consider a number of contextual influences if we are serious about improving security awareness.

Therefore, I would like to begin the panel by offering a definition of security awareness and laying out a framework to bring into focus, more sharply, the range of contextual factors that influence awareness.

A Definition of Security Awareness

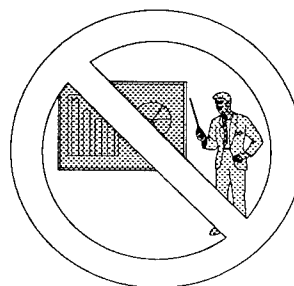
First, we need to decide what security awareness is and what it isn't. I would argue that security awareness is not security education and training. Nor is it

a program. Education and training are activities. Programs are activities. I believe we ought not view security awareness as an activity. We need to go further. We need to define security awareness as an *outcome* and clearly differentiate it from the activities or means for achieving it. If we fail to make this distinction, we risk confusing security awareness with the strategies for improving it.

My experience talking to security professionals in the field suggests some confusion on this matter. In the course of some interviews I conducted last year, I asked security professionals how they evaluate security awareness in their organization. Usually, the reply focused on the attendance figures for the required refresher briefings. These people, I believe, are confusing one avenue to security awareness (security education) with the desired outcome of effective security.

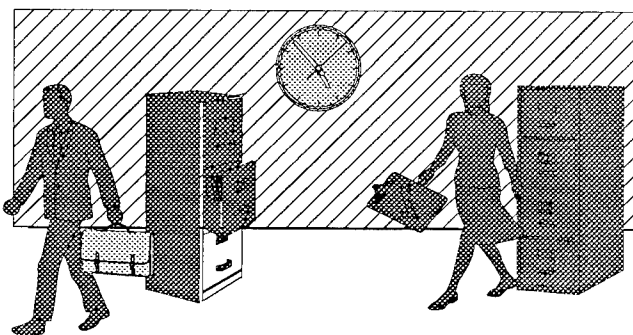
This confusion is understandable; oftentimes means are much easier to measure than outcomes. Take inspections as an example. Most security managers in government with whom I have talked tell me two things. First, very little security inspection time is given to security awareness. Second, the little time that is given to awareness is spent reviewing attendance records. Inspectors are more interested in determining if people are getting security briefings than evaluating whether the briefings have any positive impact. Clearly, it is easier to determine if people are attending required briefings than to assess the impact of the briefings on security performance.

Security Awareness Is Not Training and Education,



Nor Is It A Program.

Security Awareness -



Is It Intentions Or Behavior?

What then is security awareness? I think we should view it as an outcome, something to achieve. How about intentions? Does security awareness represent an individual's positive attitude, inclination or willingness to meet security responsibilities? Can positive attitudes can be viewed as an outcome?

I don't think so. People don't always do what they intend to do. If we define security awareness as intentions, we overlook an important fact. Security performance, or actual behavior, is volitional. People have a choice to perform well or not so well. And a number of factors other than intentions bear on that choice.

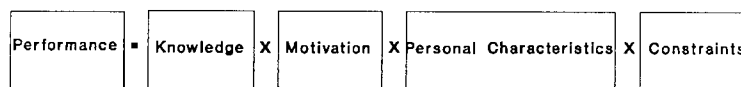
If we are really interested in the bottom line, we need to define security awareness in behavioral terms. That is, security awareness is all the individual behaviors required to maintain adequate security. Notice that my focus is on behavior as the outcome because ultimately we are interested in whether people perform their security responsibilities. All the favorable attitudes and intentions in the world do not necessarily translate into effective security performance.

The Antecedents of Security Awareness

For the moment if we accept a behavioral definition of security awareness, we need to think about how we might influence it. We need to identify the antecedents of security relevant behavior. Identifying the antecedents will suggest to us the types of strategies for influencing or improving performance.

The framework that I will present is an adaptation of a well-known model of work performance developed from applied psychological research. This model was chosen because security awareness activities have as their focus encouraging behavior relevant to maintaining adequate security. We could use other models, but I think that this one will suit our purposes.

General Model of Work Performance



The general model of work performance suggests that performance is the multiplicative result of four general factors or components: knowledge, motivation, personal characteristics, and constraints. I will first briefly describe the model's essential elements and then proceed to an adaptation pertinent to security-relevant behavior.

Knowledge includes the technical knowledge and background required to do a job, understanding job requirements, and knowledge of how to accomplish work efficiently in a specific work environment. Do people know what to do and how to do it?

Motivation has three components: direction, intensity, and persistence of effort. Motivation is viewed as a choice: the choice to perform, which reflects

direction; the choice of performance level, which reflects intensity; and the choice of duration of effort, which reflects persistence of effort.

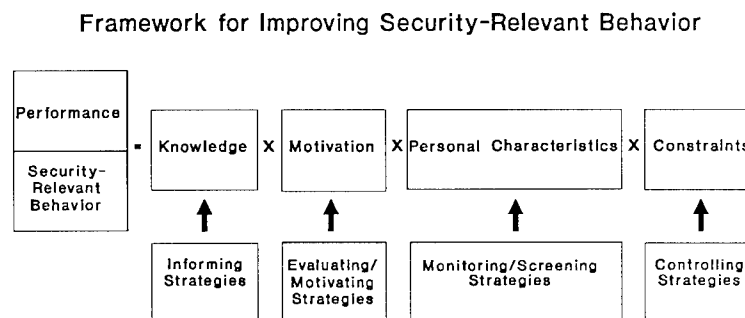
Personal characteristics include an individual's cognitive abilities, temperament (mode of emotional response), vocational interests, work and cultural values, and attitudes. Does an individual have the personal attributes required for successful performance?

Constraints are environmental influences upon performance. They are not necessarily negative. There are positive constraints too. For example, policy sets goals and prescribes appropriate performance. Situational constraints such as improper tools, equipment, and supplies may be obstacles to performance. The structure of an organization or work system design is a constraint that may facilitate or impede performance.

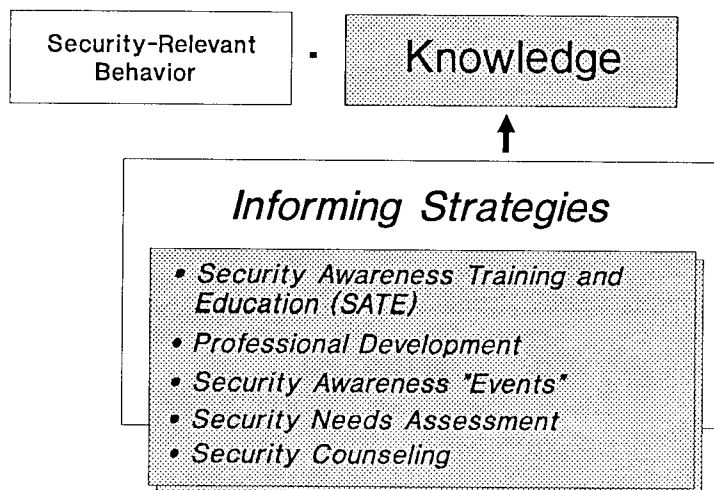
In addition to specifying the major influences on performance, this model emphasizes that performance is the multiplicative result of these four factors. This suggests that if any one of the four factors is deficient, overall performance will be poor. For example, even if people are highly capable of performing the job (have the required personal characteristics) and have the knowledge to perform the job, overall performance will be poor if they aren't motivated or if negative constraints to their performance are great.

A Framework for Improving Security-Relevant Behavior

Now I would like to adapt this general model for use as a framework for understanding and improving security performance. The focus of the framework is on general strategies for influencing security-relevant behavior. I am focusing on strategies for two reasons. First, we are not trying to predict individual behavior; rather we are trying to influence it or control it. Second, I think this focus will highlight the range of strategies available to us for improving security awareness.

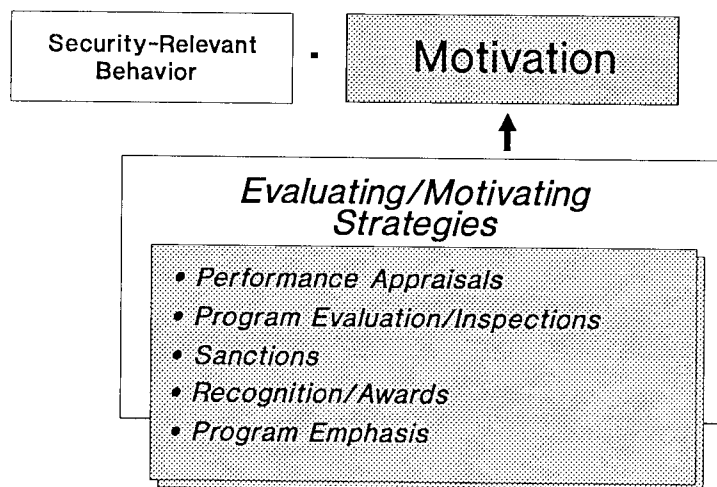


The framework suggests four types of strategies for influencing security-relevant behavior: informing, evaluating or motivating, monitoring and screening, and controlling. Knowledge is influenced through informing strategies—strategies for ensuring that cleared personnel understand their



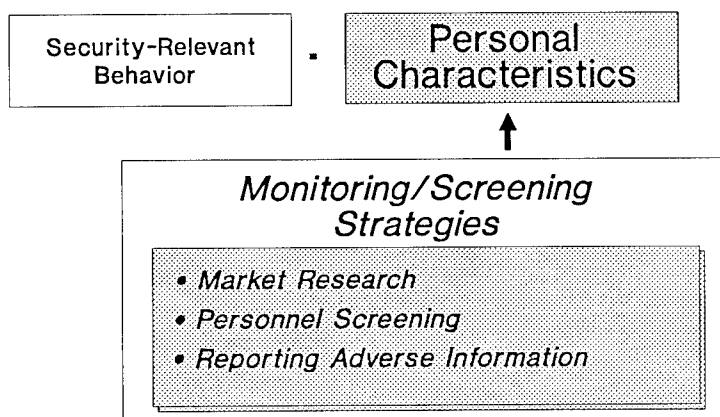
security-relevant job duties and their responsibilities to protect classified information. This is the most often used type of strategy. Typical informing strategies for imparting knowledge are SATE (indoctrination and refresher briefings), professional development (activities and training for security professionals), security awareness events (poster contests, special seminars, film festivals, guest speakers), security needs assessments (the formal process of identifying individual security knowledge requirements) and security counseling (one-on-one mentoring and informal assistance provided by security professionals).

Less frequently or effectively used than informing strategies are evaluating or motivating strategies—strategies designed to influence individual security behavior choices. Administrative approaches include mechanisms to ensure accountability, such as performance appraisals and program evaluation, inspection or accreditation programs. Performance management techniques include



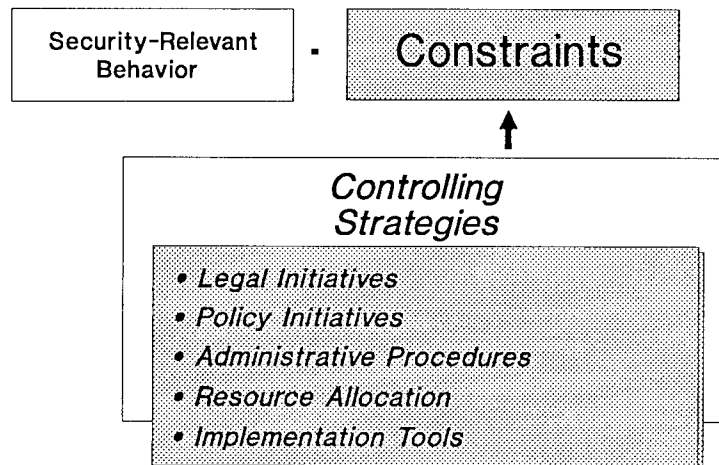
the use of sanctions and incentives, such as recognition and awards. A crucial motivating strategy is program emphasis—the priority given to security, specifically SATE, relative to other organizational objectives.

Personal characteristics are influenced or accounted for through monitoring and screening strategies designed to assess the beliefs, values, attitudes, interests, and other personal attributes of cleared personnel. Possible assessment methods and procedures include those used in the areas of market research, personnel screening, and reporting of adverse information. In the near term, we can do a better job of educating and influencing behavior if we know something about the beliefs, attitudes, and values of our target population. For the long term, prescreening of applicants and the continuing assessment of incumbents will, more directly, provide the organization with individuals whose personal characteristics are most consistent with the reliability and trustworthiness required for access to classified information.



Constraints are influenced by controlling strategies, strategies for influencing the context of security-relevant behavior. These strategies are intended to control behavior. They include legal initiatives (sanctions, privacy act limitations concerning what can be asked during prescreening, regulations governing the acquisition and use of credit information), policy initiatives (definitions of prescribed and proscribed behaviors), administrative procedures (content, amount, and frequency of training, access controls), resource allocations (budget for staff, equipment, and facilities) and implementation tools (aids to assist practitioners translate policy into practice).

As in the general model of work performance, this framework suggests that security-relevant behavior is the multiplicative result of the four factors: knowledge, motivation, personal characteristics, and constraints. In practice a great deal of attention has been given to influencing knowledge through informing strategies. The framework suggests a number of other improvement strategies available to us that have been under-utilized.



Current Issues Related to Key Strategies

Now let's turn to what is happening in the field. The panelists will address issues in the field related to some of the strategies I have highlighted in three of the four areas. Preliminary results of two PERSEREC research projects suggest that addressing weaknesses in these areas offers substantial opportunity for improving security awareness. By addressing only some of the strategies, however, we are not suggesting that others are not important.

Current Issues and Key Strategies

- Informing Strategies
SATE and Professional Development
- Evaluating/Motivating Strategies
Program Emphasis
Program Evaluation/Inspection
Performance Appraisals
- Controlling Strategies
Implementation Tools

In the informing area, panelists will talk about SATE and professional development. Here they will address the quality and availability of instructional media and materials for cleared personnel as well as the adequacy of developmental activities for security professionals.

In the evaluating/motivating area panelists will address program emphasis/program evaluation/inspection and performance appraisal. Program emphasis pertains to the degree of management emphasis reportedly given to security awareness compared to other organizational objectives. Program evaluation/inspection includes the adequacy of the mechanisms for assessing and evaluating performance at the organizational level. Performance appraisals may be useful in improving individual accountability for security performance.

In the controlling area panelists will consider implementation tools. Here the panelists will discuss the need to provide tools for security professionals that will enable them to translate SATE requirements into operational programs.

The panelists will also discuss problems in the field related to these strategies. I hope that the framework presented will be useful in showing how the improvement strategies proposed by the panelists relate to each other as well as meet the challenge of improving security awareness.



Howard Timm, Jim Riedel, Ernie Haag, and Gussie Scardina

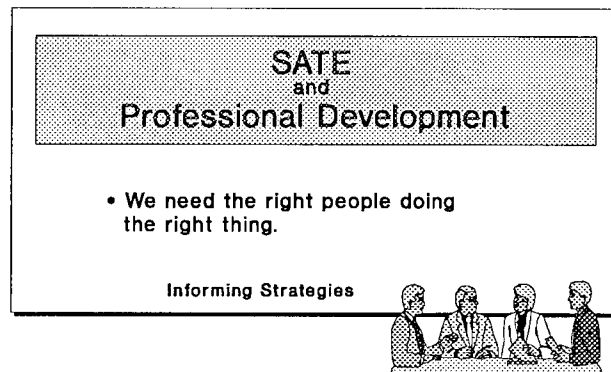
Ms. Collins is a past president of the National Classification Management Society (1990) and former manager for security administration and training for ESL, Inc. Ms. Collins is also the founder of Collins Consulting Group which emphasizes security management systems and security education programming. She is currently a consultant to HumRRO International Inc., concerning a major security education effectiveness study being done for PER-SEREC.

Security Awareness, Training and Education(SATE) From the Industry Perspective

by Deborah Russell Collins

SATE and Professional Development, an Industry Perspective

To put it in simplistic terms, we need the right people doing the right thing. In order to make a positive impact on the security-relevant behavior of our employees, as well as the overall mission performance of our organizations, we need the best people performing the job. In turn, these individuals require the tools, training and support systems to provide for a dynamic and motivating SATE program. I want to put my emphasis on getting the right people and what we need to do to get there. Ernie Haag has discussed the right things that should be done to deliver SATE in the organization.



Finding The Right People

Unfortunately, many individuals find they are given the job of security manager as a collateral, part-time duty and, worse yet, are not provided the tools to perform the job effectively. For average security professionals, specifically in the smaller organization, SATE is not the highest priority in their job. They put their time and energy on those things they perceive, or know from experience, to be the key areas that make the program survive and, hopefully, succeed. This situation has, in the opinion of many in both industry and government, been brought on by a lack of customer and internal organization emphasis placed on SATE. And for those who have done the job in a full-time capacity, SATE is not considered a career specialization. As a result, many of the most qualified people aspire to move on to greater things within the security career field. And who can blame them?

From personal experience in being given a position of being solely responsible for SATE in my organization, I heard time and time again that the only way I would find success in my security career was to move on to operational programs and security management. I did do that with time and found I was able to apply all of my SATE expertise and experience to the other positions. It made my career successful and allowed me the opportunity to increase the importance of SATE within my company.

Some of our best people do not even get the chance I did to deliver SATE as they aspire to make it to the top. SATE and the people who deliver it need to be acknowledged as critical to mission performance. You can call it, "putting our money where our mouth is" in that I have heard for several years how important security awareness is to the overall security mission. But in reality we do nothing to promote the profession. We have no uniform selection criteria for this discipline and it is by far one of the most demanding in terms of the job skills required.

Those of us who have been fortunate to achieve success in this area either brought the right skills in with us or struggled long and hard to acquire them. Unfortunately, we lose a lot in effective SATE efforts as a result. By way of an example, the closest thing I have seen to any uniform standards for SATE provided in the contractor community currently, specifically focusing on security briefings, has been the NSA briefers program. In order to indoctrinate personnel for NSA you must attend their briefers course and then receive NSA approval to serve as a briefer. While this does nothing to really guarantee a total quality effort, it does formalize the process and make the contractor keenly aware of the importance placed on the indoctrination briefing received by individuals cleared with NSA.

In turn, the company always ensures it has someone approved by NSA to do its briefings. By the formality of this "approved briefer" process, it cannot be just anyone in the security organization who performs this function. This is a critical and positive difference. And more recently, there is the phenomenon of the automated information system (AIS) security professional and the certification of members of this discipline by various government organizations that bring to light what should be done for the SATE security professional. This AIS certification process has done more in the past five years to legitimize the AIS profession than almost any other security career discipline. In both government and industry, we might take what we have seen relative to AIS as a career specialization and apply it to the area of SATE in our organizations.

The Right People Getting What They Need to Succeed

So we go forth and make the profession of SATE a legitimate and acknowledged discipline of authority, stature and respect. To do only that will do nothing to ensure SATE effectiveness in the big scheme of things. Right now

SATE
and
Professional Development

- Effective SATE programs are in the minority in our business.
- The people who need the help most don't seem to get it.
- More visible government support of SATE

- The DIS E & T Specialist should be reinstated and expanded.



Informing Strategies

there are several defense contractors, many represented here at this symposium, who have effective SATE programs run by the best SATE professionals in the business. But they are the minority in our business. The people who need the help most don't seem to get it—this means that we need to do more in our business of getting to those contractors that have the part-time FSO, the organizations that do not have the luxury to have a full-time

SATE professional on board, and more importantly providing for the improvement of the support systems in our business to help any one of us do a better job of delivering SATE.

To begin with, the Defense Investigative Service does not provide an adequate support system in the regions to train and monitor SATE efforts in industry. While serving as President of NCMS last year, I and the rest of my board of directors made a strong plea that the Education and Training Specialists (E&Ts) not be eliminated in the regional DIS offices. I understand dwindling resources are a concern for all of us and I understand the need to cut back, but to place the burden to support SATE efforts on the local DIS representative, already overloaded with a wide array of responsibilities, does nothing to communicate that SATE is of any importance in our business. We made the recommendation that the DIS E&T Specialist role should be expanded. If we want to acknowledge SATE is significant in how we effectively deliver security excellence, our companies need to see that our government counterparts place SATE at as high a level of visibility and attention in the organization as we should. Expanding the role of the DIS E&T Specialist should include some form of coordination and oversight in the certification idea proposed earlier in this discussion.

Secondly, with the growing acknowledgement of the need for us to work collectively on the activities that comprise SATE, and the Industry Security Awareness Councils (ISACs) we see emerging throughout the country, the E&T Specialist could take on the role of coordinating such a council in every region. It should not be mere chance that such an excellent networking vehicle appears in one region and not in another. An E&T

SATE
and
Professional Development

- SATE is not the highest priority on the job.
- SATE is not considered a career specialization.
- SATE and the people who deliver it are critical to mission performance.
- Uniform selection criteria and training.

- A certification program for SATE professionals.



Informing Strategies

Specialist, at the regional level, could lead this effort. In addition, this individual could provide regional training for the contractors in how to deliver SATE in conjunction with the ISAC.

Finally, when a contractor's security program is found, during an inspection, to be unsatisfactory in the area of SATE, this E&T Specialist should come to the facility to assist in developing a program that will work successfully. Why do we need a dedicated E&T Specialist at the regional level of DIS? For all the reasons alluded to in our discussion of demonstrating not only the importance of SATE but by, again, putting the right people in the job of supporting and monitoring SATE in the contractor arena. The same skills are needed of the E&T Specialist as would be a SATE professional within industry. We should

**SATE
and
Professional Development**

- FSO Training - too much too soon.
- DSI's Train the Trainers Program is a step in the right direction.

- We need more "how to" training.
- More individualized attention is needed for the part-time FSO.

Informing Strategies

put the best, brightest and most motivated DIS professionals into this job. Groomed by specialized SATE training provided through DODSI, they can and will do so much for the advancement of SATE in our business.

Another concern is that there has been an inadequate approach to current FSO training: the fire hose. And, unfortunately, many firms follow this same approach in deliver-

ing SATE to their own people. We tend to spend a lot of energy on telling people what is required but not how to effectively get it done. I commend DODSI for their Train the Trainers Program as it is a step in the right direction. We need more in the way of "how to" support systems to help people who deliver SATE to succeed. We need to ensure that the availability, timing and content of the support provided lends itself to helping people get beyond requirements, or learning how to survive, and does everything possible to ensure the right people are getting what they need to deliver a quality program. The ideal would be more individualized attention, particularly for smaller firms with the part-time FSO. Here, again, the E&T Specialist could be the essential support system we need to help the large majority of our contractors, the smaller firms, succeed.

Recommendation: To get the right people, allow for SATE career specialization. We need uniform requirements for whoever does the job, what is required of them, and possibly to include a formalized certification or training program for all deliverers of SATE in industry and government. We must provide those people what they need to succeed and this includes regional E&T Specialists who coordinate regional ISACs, regional SATE training, onsite support for contractors in need, and supervision of the aforementioned SATE certification process. They need more "how to" training. Get away from the fire hose

approach and look at training provided as early as possible to the new FSO, especially the part-timer.

Inspections and the Checklist Mentality: an Industry Perspective

We must increase inspection emphasis on SATE beyond asking whether a program simply exists. In the research I have done for PERSEREC the overwhelming comment from the industry SATE experts has been that the government inspection process does nothing to enhance efforts for SATE. The problem is twofold: For many years, the question was posed as "does a program exist," by asking if briefings were done and how many, where the security posters were

hung, and how many security violations the organization had. The inspector needed to be able to check off the list that security awareness was present in the organization. Ninety percent of the inspection process is spent on things we can count, with the remaining 10 percent on assessments like SATE and management security posture. The items that fall out in that 10 percent are the most critical to the success of the program, but we cannot get our arms around those areas as easily as we can the quantifiable measurements of a security program.

The view of SATE in industry and government will change if given higher regard in inspections. The analogy we can use is that when we were in school we studied what we had to in order to pass the test. We did not bone up on things we knew would not be covered in any depth. When SATE is not a major area of inspection, the contractors respond by putting their energies into those

areas that are covered in depth. If we acknowledge that security awareness permeates all aspects of a security program, that it is a much more important area of concern, then we will elevate it to the right level of emphasis. In the past two years we have seen inspections take on a new assessment as they relate to SATE in the industrial security arena. Unfortunately, it has become one of subjective assessment

Inspections

The Checklist Mentality

- "Does a program exist"
- The inspection process should enhance SATE.
 - SATE is difficult to measure.
 - Industry follows the government's lead.

- Place SATE higher in inspection emphasis.

Evaluating/Motivating Strategies

Inspections

We Need An Objective Approach

- Need standardized measurements developed jointly by government and industry.
- Inspectors must be specific in what needs attention, it's more than "do a better briefing."

Evaluating/Motivating Strategies

rather than any formalized assessment technique. We must come up with an objective process to assess the quality and effectiveness of SATE programs. We need to look for effectiveness indicators.

Standardized measurements should be the basis of such an assessment, developed jointly by government and industry. Why is this so harmful to the overall program? When an inexperienced inspector comes in, talks to a handful of cleared personnel, doesn't like what is said, and then debriefs company management by saying the "security education program needs to be improved," the response by company management is "do a better briefing." When specific issues and areas are not identified, through statistical sampling and standardized instruments, the response is non-specific. The result, in most cases, will be a program that gets a face lift but does nothing to improve the security-relevant behavior in the work place and that, in reality, is what we should be striving for in our inspection programs.

The efforts of the NISP to set forth a standard set of requirements of SATE within the industrial security program will help us focus our energies less on the activities that would be checked off the list and more on ensuring that effectiveness is achieved in our programs. Removing redundant briefings and requirements will empower security professionals to get out there and really see what is going on and allow us the flexibility to address our individual organizational needs that in turn will have a much greater impact on security-relevant behavior.

Recommendation: Move away from the checklist or subjective inspection approach. Government and industry jointly develop effectiveness indicators and standardized assessment instruments for inspections of SATE.

Performance Appraisal: An Industry Perspective

Put the Responsibility Where It Belongs

Organizations need to put responsibility for security performance on the individual—not the security organization. How often do we hear that "security is security's job". Because managers in industry are not exposed to the notion of security being an integral part of their business success, they fail to see how they, as well as their people, are responsible for their individual security performance. As a result,

Performance Appraisal

Put The Responsibility Where It Belongs

- "Security is security's job."

- SATE leads them to the water --- to drink is individual choice.
- Security performance - an individual responsibility

- We need to impose security performance review criteria with rewards/sanctions defined.

Evaluating/Motivating Strategies

unrealistic expectations can be placed on the security organization. An example I heard was when the expectation was levied on an organization to achieve zero security violations in the upcoming year. The security staff sat bewildered as to how they would be able to prevent their 1300 cleared employees from committing any security violations. An individual performance issue was being imposed on an organization that had some influence but could not guarantee that violations would not occur.

This also translates to a "do a better briefing" mentality when we see that security bears the burden for a lack of security knowledge by their employees. The fact may be that the individuals are indoctrinated, reindoctrinated, and "led to the water." If they drink, it's an individual choice; if they choose to support the security program, it's also an individual choice. SATE efforts can only do so much to motivate people to act on security. What we must do is provide for a management-supported system that backs up the message delivered in our SATE efforts. If we do not have a system by which consequences at the individual level for non-compliance with requirements are handled consistently within the organization, nothing done in the SATE program will impact behavior. If we see security as a vital part of our mission performance, we must have sanctions related to performance —our individual performance appraisal systems must make it an expectation that we are each responsible for security.

Recommendation: Strive for an individual security performance appraisal system by which there is a defined consequence relative to security performance.

Program Emphasis: An Industry Perspective

This symposium sets forth the premise that SATE is important in our business. We often say that, but we must move beyond lip service and demonstrate commitment to that end. Everything discussed up to now addresses SATE emphasis. Four recommendations were mentioned that, if implemented, clearly demonstrate that SATE is important to the organization and to the government customers. These concern career specialization, training and certification, E&T Specialists, and the support system to train and monitor SATE activities in the field.

We must place SATE higher in the pecking order in inspections and the performance appraisal systems that hold individuals accountable for their individual security performance. We must do what we advocate in our security programs to be seen as credible and professional. This principle can be applied, as well, when we discuss involving our management in the security program. There is a clear link between the organization mission and security. Managers need to be made aware of that link and then act upon it. Security-relevant behavior can be affected at both the individual and the organizational level. All

management training programs should contain some element that provides for security participation in our up-and-coming managers and leaders. Our managers should set the example for the work force. We need them to be as educated and supportive as possible in order to achieve security excellence.

In addition, government customers can do so much, through the contracting process, to make clear the linkage between business performance and security performance. A contract I supported early in my career stipulated that security was going to comprise five percent of the quarterly award fee. That one single acknowledgement, relative to profit for my company, gained me "a seat at the table" and a relationship that placed me as a peer with the other managers on the program. It was a refreshing experience. We should do more of that.

Most security professionals do all they can to insert themselves into the management process. It greatly helps their cause when the customer does that for you or helps make it happen.

Program Emphasis

Everything Discussed Up To Now Is Addressing SATE Emphasis

- Career specialization in SATE - training and certification
- E&T Specialists - the support system to train and monitor SATE activities in the field.
- Place SATE higher in the pecking order in inspections.
- Performance appraisal systems that hold individuals accountable for their security performance.

Evaluating/Motivating Strategies

Support Mechanisms Are Critical

At this symposium, we are meeting to discuss the challenge of security awareness in the coming decade. We must believe it is important if we are here. But how often have any of you experienced or heard from your peers that SATE is one of the first things to be cut in hard times like these? We say it is *critical*, but too often the perception is that it is fluff and is expendable. We must change that mind set. SATE must be institutionalized—just like the locks and alarms. We need to have people dedicated to a well defined program that receives the resources required to get the job done. It is not an expendable commodity.

Recommendations: In addition to the earlier recommendations, which are all aimed at improving SATE emphasis, we need security training for the non-security professional. Expose them, involve them, have them take on responsibility for the security performance on their programs. They set the example. Secondly, introduce security award

Program Emphasis

Support Mechanisms Are Critical

- It's the first thing cut in tough times.
- SATE must be a part of the culture -- it is not an expendable commodity.

Evaluating/Motivating Strategies

fees in government contracting. It brings security equal to many of the technical elements. To be elevated as such improves the standing of the security program in its credibility and visibility on any program. And lastly, get the support mechanisms in place to help the program succeed.

Bridging the Gap Between Objectives and Implementation: The SATE Desk Reference

SATE requirements in our business cover what has to be said. How to say it and say it effectively is the problem in SATE today. As stated earlier, a number of organizations have very effective programs. Unfortunately, practical guidance for the development and implementation of SATE programs has not been shared to the extent desirable. Of real concern, and we have highlighted it in our discussions this morning, are the smaller facilities in the industrial security community that make up the majority of the contractors in our business. They do not have the luxury of supporting SATE or full-time security on a full-time basis.

The SATE Desk Reference will be an attempt to fill that void. Like the other efforts you have heard about—the ISACs, the Train the Trainer programs, the efforts of organizations like NCMS to distribute materials—this tool will bring together what is working, who is doing it and how, and provide a centralized resource for the entire community. Based on interviews with SATE experts in the field, coordination through the professional organizations, and the results of a survey distributed to 200 facilities, we hope to pull together a reference that will benefit both industry and government.

The SATE Desk Reference

- There are organizations with effective programs - sharing is not the norm.
- The Desk Reference - an attempt to fill the void.

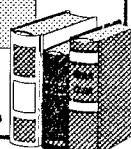
- deals with the delivery of SATE - beyond requirements

- a "how to" guide for FSOs

- focus on the needs of the small organization

- Through interviews and a survey, pull together what works!

Controlling Strategies



SATE Desk Reference Categories

• Getting the Word Out - Effective Communication Programs • Briefing Programs • Management Involvement • Employee Involvement	• Rewards and Recognition • Needs Assessment Strategy • External Support Mechanisms
--	---

Controlling Strategies

The Desk Reference, a "how to" guide for FSOs, will focus its discussion on the informing, motivating and managing strategies of SATE. Some of the categories will be: Getting the Word Out, Effective Communication Programs, Briefing Programs, Management Involvement, Employee Involvement, Rewards and Recognition, Needs Assessment Strategy, and External Support Mechanisms.

SATE Desk Reference Content

- examples of successful activities and events, along with suggested resource material
- suggestions for tailoring sample activities and events to meet varying organizational needs and conditions
- guidance for creating innovative new activities and events
- direction for implementing activities and events
- names of advisors to call upon for advice in developing or implementing specific activities or events
- names of organizations to call upon for SATE products and media

Controlling Strategies

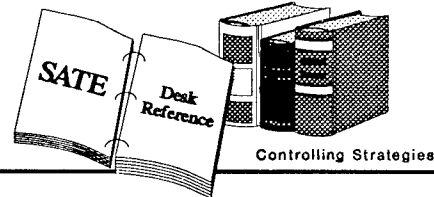
In each category the discussion will contain examples of successful activities and events, along with suggested resource materials; suggestions for tailoring sample activities and events to meet varying organizational needs and conditions; guidance for creating innovative new activities and events; direction for implementing activities and events, names of advisors to call upon for advice in developing or implementing specific

activities or events; and names of organizations to call upon for SATE products and media. The Desk Reference will be formatted in a way that will make it easy to read, organized around the SATE objectives, packaged in a loose-leaf binder (making sections of particular interest easy to find, use and update), and cross-indexed to link SATE objectives with specific activities, events and experts.

The feedback in our research in determining industry interest in this Desk Reference thus far leads us to believe there is a tremendous need for this type of tool. There are so many effective things happening in both government and industry. We need a centralized vehicle to showcase those accomplishments for the benefit of all who participate in the Defense Industrial Security Program and in other security arenas as well. This is really a project of pulling together what works and disseminating it in a way that will be useful to people in the field.

SATE Desk Reference Format

- easy to read, organized around the SATE objectives.
- packaged in a looseleaf binder - making sections of particular interest easy to find, use and update.
- cross indexed to link SATE objectives with specific activities, events and experts.



Controlling Strategies

SATE Desk Reference

- We need a centralized vehicle to showcase what works and how.
- We hope this will make that happen.

Controlling Strategies

Mr. Haag is a researcher and manager of western operations for Human Resources Research Organization International, Inc. His special interests are in personnel security issues, particularly in the area of security awareness, continuing assessment, and management systems.

Planning for the Future: Current Problems

by Ernest V. Haag

I hope that some of the things Jim has shared with you, along with what we all heard yesterday, have caused you to think about security awareness in slightly different ways. As Jim stated, our intent this morning is to examine security awareness through different lenses, to generate dialogue on what you, we and the other presenters see as issues for consideration, and to get the creative juices flowing for addressing the challenges of the '90s.

As some of you know, I see some familiar faces in the crowd. Dee Dee Collins and I, under PERSEREC sponsorship and Jim Riedel's management, have been conducting a project to define and assess the state of security awareness efforts in DOD, and to some extent to continue the work we started in "Beyond Compliance" in the contractor community. We have visited a goodly number of DOD organizations across the nation, conducted more than 60 interviews within DOD and a few in industry, and collected another 60-plus written surveys from security professionals and nonprofessionals in DOD, mainly from the operational unit level. We are also in the process of collecting survey data from about 200 FSOs in the civilian contractor community.

We do not have the data completely analyzed as yet, but since we have personally conducted all of the interviews, we do have some very tentative impressions, as well as some that are fairly solid. Dee Dee and I will share those with you as a means of eliciting your collective wisdom and thinking on the subject. We also hope that you will not confine those thoughts, or their sharing, to these few days of the symposium, but will keep up the dialogue in the days and months to come. We may be able to assist you in that as well.

We have organized our talks to address each of the three strategic areas Jim has outlined: SATE & professional development, within the framework of informing strategies; evaluation and motivation strategies; and tools for implementation which serve as controlling strategies, with some overlap into informing strategies. Although we will be taking different perspectives, DOD and industry, you will find that much of what we say and the recommendations that we make apply to both communities.

Security Awareness Training and Education (SATE) Delivery Issues

**Security Awareness Training
and
Education (SATE)**

- No DoD "System for delivery
- Train-the-Trainer Training deficient
- SATE materials dry and boring - not current

Informing Strategies



So what did we find? There is no DOD system for delivery of SATE. We need to look beyond what has been traditionally regarded as security awareness, education and training, and consider the context, the supporting infrastructure and the organizational determinants of success or failure. Security managers reported that they operate on their own, in most cases. And that support, where it does occur, most like-

ly addresses the "what" (the information) with little that relates to "how to."

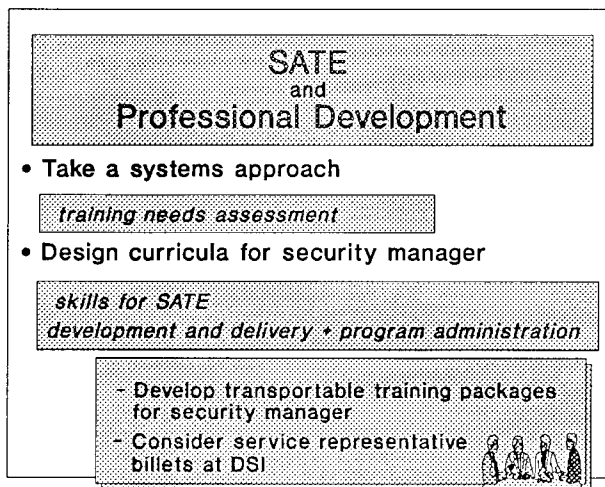
Few security managers ever receive train-the-trainer training, though security managers state that security education and increasing unit security awareness should be their most important objective. Training emphasis is largely on administrative duties. Some report having superficial presentation skills training as a part of their military professional development. Most indicated that such training usually occurs fairly early in their careers, with little opportunity to practice and reinforce or expand their skills. Most get no such training at all. The inevitable result is inconsistent quality, mostly standup reading of materials to the learner.

The news is by no means all bad. There are pockets of SATE excellence out there. Unfortunately, they are not being leveraged across DOD, or even within the services. We saw a few examples of individuals adapting new technology and learning theories to SATE, with apparent good success. There needs to be more.

Larry Stitt, from Fort Huachuca, is one of those examples who is with us this week, and there are others. I mention Larry specifically because he has offered to share his expertise and products for computer-based instruction with us. He will be available for a demonstration at the registration tables during breaks and by appointment.

Almost everywhere we went, SATE materials were reported to be generally dry and boring, out of date, and with little motivational content. "How many times, and how long, can we expect people to learn from the Walker tapes?" was a very common refrain. Unit security managers generally lack the time or skills to address this issue. And almost all expressed some frustration at their lack

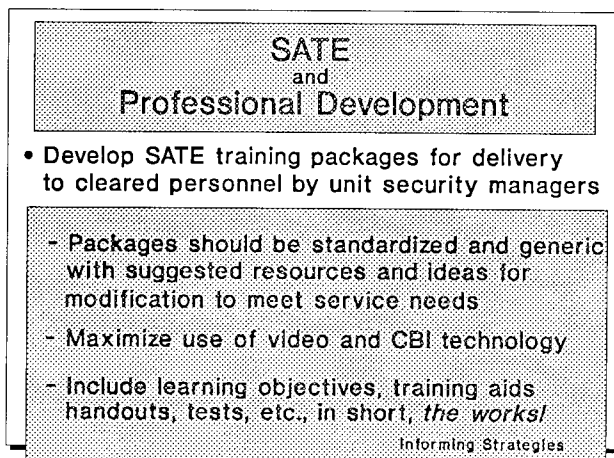
of knowledge about what works, what is available and how to get the most return from what they have.



All of this boils down to the fact that we need to have a strategy for SATE—a comprehensive consideration of the threat and our target population, our goals and objectives for SATE, the opportunities and methods for achieving them, and the resources required to do the job. We need to determine what really needs to be delivered to a diverse population, to what depth, and when and how often in both training and education for the security manager and for the cleared population. This will re-

quire some level of systematic needs assessment across DOD.

Based on that needs assessment, we can then design training curricula for the development of the skills required for SATE design/delivery by those responsible. The need seems to be for comprehensive training packages for security manager training, packages that can be customized to fit organizational needs without extensive design work. We found efforts to achieve this training going on in many places, nearly all of them without knowledge of the experiences of others. This is an area where more systematic sharing of ideas and solutions can offer real dividends. There is widespread support for DODSI "core" training for the security manager, but a strong expression of need for something more specific to service applications than is now the case. Several of those interviewed recommended service representative faculty billets at DODSI to allow for better coordination and to provide a service "tint" to the appropriate curricula.



Following the logic above, similar training packages for SATE delivery by security managers to the cleared population are high on the priority list of those interviewed. Some of the desired features for these transportable packages are:

- standardized to the max extent possible, and generic
- recommended areas to be customized, with suggested resources and modification ideas
- maximum use of video and computer-based instruction (CBI) technology
- learning objectives, training aids, handouts, newsletter articles, pre/post tests, etc.

**SATE
and
Professional Development**

- Establish a simple and responsive distribution system for SATE information to meet both planned and emergent needs
- Introduce a means of facilitating professional networking

- Exchange ideas, information on media products CBT initiatives, training techniques that work
- Reduce unnecessary duplication of effort across DoD
- Leverage the "pockets" of excellence and innovation

Informing Strategies

Once you have the delivery products to fit the needs, you have to get them to the user in a timely and efficient manner. Almost everyone expressed a great deal of frustration at existing service procurement procedures as not being very responsive. They also wished that they had a better idea as to what products are available for SATE. In my travels during the project I often found myself serving as a broker, passing along ideas I had seen at other commands, media I had collected, and

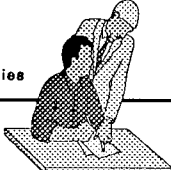
needs I had noticed. As one security manager commented as I departed, "This has been the best assist visit I can remember." There is a need there, and generally speaking we haven't done an adequate job of meeting it. As I indicated before, there are pockets of excellence out there doing exceptional support work. We simply need to spread the wealth of their experience and expertise more broadly across DOD.

Spreading the wealth can be accomplished in a number of ways that enhance professional networking opportunities. I will address one in particular later in the presentation. But regardless of the method, there are certain outcomes one might strive for. Among them are:

- facilitated exchange of a wide range of information
- reduction of unnecessary duplication of effort
- finding and maximizing the impact of those pockets of excellence
- providing support for and raising the standards for SATE

Program Emphasis Means:

- Committed and involved leadership
- Effective Program Evaluation/Inspections
- Effective Support Mechanisms



Evaluating/Motivating Strategies

Taking a more macro view of program emphasis, where DOD programs are concerned, leads me to many of the same conclusions reached by Dee Dee Collins.

One of the most effective strategies for motivation is certainly implied in the points she has made as a result of having been a committed and involved leader. Much has been accomplished by following a strong leader, and the

security "battle" cannot be won without the leadership factor.

The second area of program emphasis I will discuss repeats the next theme, program evaluation and inspections. And the third facet of program emphasis that I will touch upon adds to the discussion of support mechanisms for SATE.

In the organizations we visited, the role of the leader in supporting and emphasizing security objectives was always made evident by the interviewee. If the leader was, in fact, highly committed and involved, we didn't have to wait long for that point to be made. Security managers viewed that as a significant strength and the interviewee was eager to tell us about the impact of the leader's policies and activities. There was also obvious pride in being involved in a task for which there was so much top-level support. That pride was reflected in the enthusiasm of the security managers and the amount of initiative and creativity they seemed to exercise in their job.

**Committed
and
Involved Leadership**

- Visible and substantial involvement - more than verbal
- Security a central concern of leadership in all "Pipeline" training
- Bottom-line: Establishing/supporting link between individual and organizational security performance and mission achievement

Evaluating/Motivating Strategies

Central to the discussions of leader impact on security programs in general and SATE in particular was the importance placed on the visibility of the leader. In most of the interviews we asked the question, "How would you characterize the support of top leadership in your SATE efforts?" Most of the initial responses were positive in tone. The real payoff came with follow-up questions asking for examples of specific behaviors to illustrate leader support. When there was true commitment, they talked about visibility factors, active participation in SATE activities, and personal support and encouragement for SATE initiatives.

Unfortunately, more often than not, the responses were less enthusiastic, with few specific citations of active leader involvement. The bottom line was that the impact of leadership within an organization is always substantial, regardless of the area of its attention. As one security manager said, "Security needs to be ratcheted up a notch or two by the "heavies", and not just when something goes wrong."

Part of this problem is, of course, the immense level of demand for the attention of the commander and others in the chain of command. Mission always comes first, as it should, and that is what most of the training and experience of the commander involves. Security receives little attention in the "pipeline" training given service leaders at any level. There is a place for security in such training, a place for not only revisiting security requirements, but also for considering the leader's role in meeting the requirements and ensuring that security issues are fully integrated into command thinking.

All of this leads to what I think is at the core of the commander's (and his/her subordinate leaders') responsibilities—creating an organizational culture that firmly establishes that security is a critical element for achieving the operational mission, and that individual and organization security performance are the essential measures of success. We don't do as good a job at that as we might.

I will also very briefly touch upon an area that Dee Dee spoke of, some things that we in DOD might consider in assessing our security performance.

There were many instances when we were told that inspections of security programs were both infrequent and ineffective. The most frequent comment concerned the major emphasis on inspecting for numbers (of participants, of training sessions, etc.) while paying little or no attention to quality factors. Several security managers indicated that they really liked to be inspected, because that was the only time their area of responsibility could get command attention. As one expressed it, "What you get is what you inspect." Surprisingly, many also indicated that command security assist visits (rather than inspections) were nice, but that it was easier for the command to ignore or place less priority on assist visit recommendations. The more capable security managers seemed inclined to favor routine security performance inspection as a part of all organization-wide inspections, not just when things had gone wrong somewhere in the system.

Effective Program Evaluation and Inspections

- Routine review of security performance in all inspections
- Performance criteria and indicators of awareness
- Knowledgeable and experienced inspectors
- Systematic sanctions and rewards

Evaluating/Motivating Strategies

Now, having routine security inspections and having effective inspections may not mean the same thing. There do need to be criteria for effective security performance, both general and mission-specific. Almost all security managers agreed that they needed some way to assess the security awareness and performance of their organizations on a continuing basis.

They also agreed that current inspection methods leave something to be desired. A typical comment was that "the inspector came, asked his yes/no questions, looked at a few documents and publications and in 15 minutes told me I had an excellent program." "Pencil whipping" to respond to a check list was reported to be easy, especially when many inspectors were much less experienced than those being inspected.

The final point I will make about evaluating and motivating strategies is that the system as it exists in most service organizations places almost exclusive reliance on negative sanctions for enforcement of security performance. There were isolated examples of using positive reinforcement for motivating security

Effective Support Mechanisms
• Systematic recognition of security performance • Security training and performance factors for promotion and periodic performance review • Systematic means for C3 (communications, collaboration, coordination) • Training support • DoD integration of support is key
Evaluating/Motivating Strategies

performance. All, however, pointed at security personnel and their administrative duties, rather than actual security performance by cleared personnel. There are also some isolated initiatives under way within the services for recognizing organization-level security performance, but nothing systematic or widespread. For most security managers queried, the idea of systematic positive reinforcement of exemplary security performance

was not something that had ever occurred to them. Significantly, all agreed that it was probably a good idea, and that, with command support, it could be done.

Effective support mechanisms can encompass a number of potentially successful strategies. The comments I made previously about systematic recognition of security performance apply here also whether we are talking about exemplary individual actions noted in the workplace, or organizational efforts discovered during the inspection process. What you get is also what you reinforce.

One telling commentary from a security manager was his amazement that attendance at first aid, CPR and swimming training was a requirement for promotion recommendation, while he had real trouble getting people to attend security training sessions. Perhaps there is a need to consider giving security performance and training some of that same type of emphasis and priority.

One area of support for which there was unanimous agreement was a need for a way to enhance communications, collaboration and coordination across the entire security community. One thing that all security managers recognize is that there are large numbers of security managers solving the same problems, grappling with the same issues and sharing the same frustrations associated with inadequate resources, whether it concern SATE or general security functions. There are, again, isolated and fragmented efforts to address this need, but nothing that offers widespread benefit. I will say more about this area in the following segment.

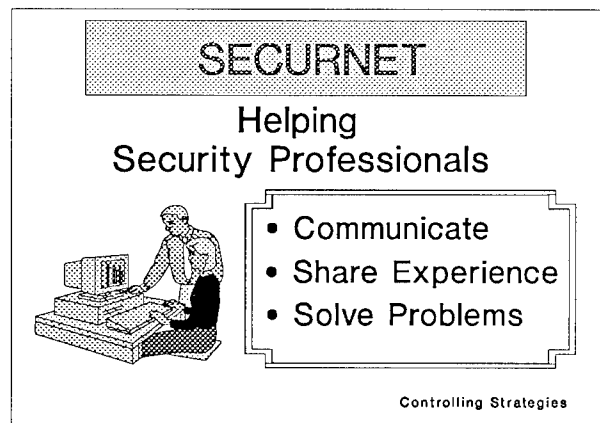
Another area needing enhancement is that of professional training. I have already addressed this to some extent, but it deserves revisiting here. There is ample evidence in our data which indicates a general deficiency of training in the security community. I will take this opportunity to say that the quality of DODSI training is generally held to be very high by those who have had the luxury of experiencing it. However, the issues of course and quota availability, cost and the timely relevance of professional training are real and need to be addressed.

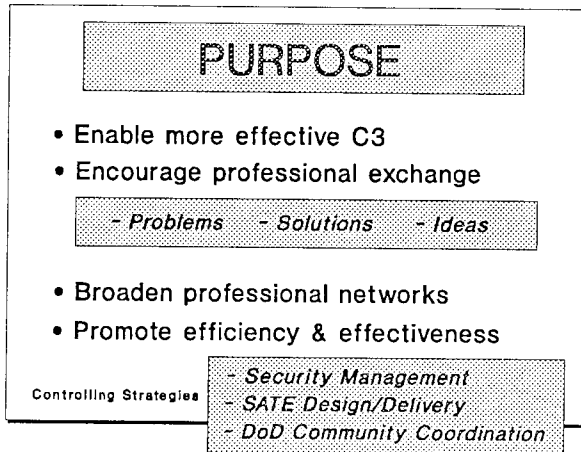
Media support and a more effective distribution system have also been previously identified as areas for improvement. In sum, the system for training and education support needs more attention.

Regardless of the type of support mechanism being considered, it seems to me that the Department of Defense must play a key role in ensuring that the needs are identified, that priorities are addressed and that resources are allocated efficiently and effectively.

In the 1990s, with shrinking resources, we may not be able to afford total independence (isolation?). Better collaboration, coordination and communications may be the most effective path to both improved SATE efforts and individual and organization security performance.

Now, moving to the final segment of our presentation, we take a look at two "products" with potential for bridging both the efficiency and effectiveness gaps. These fall in the area of controlling strategies in Jim's model, a way of guiding and directing consistent efforts. Both might also be considered as informing strategies, since that is the bottom line as far as the security manager is concerned.





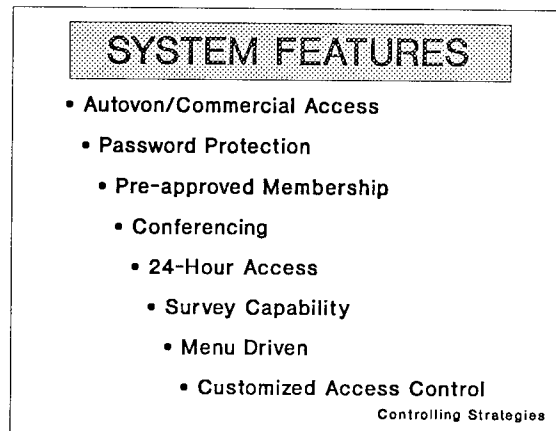
My offering involves what we have chosen to call SECURNET, an electronic, computer-based communications network that addresses several of the issues we have discussed.

I will be available after this presentation to demonstrate a prototype design for this system that will enable you to see how it works and what some of the potential might be. For now I will briefly

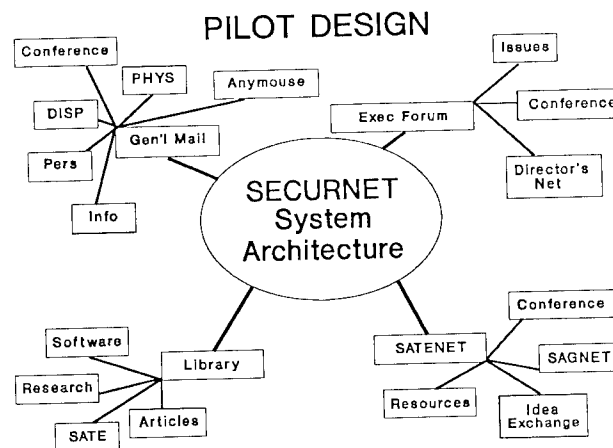
cover the purposes and the features of the system.

As you can see, we focus on meeting security community needs in our own SATE version of C3. Come to think of it, the more traditional definition of C3 might also be well served. We hope to support and encourage an effective exchange of ideas, as well as problems and solutions, with an emphasis on broadening the professional horizons of the security manager and staff. We think there are gains to be made in the three areas indicated: security management, SATE design and delivery, and in overall DOD security community coordination. The genesis of the concept was focused on SATE; the applicability seems potentially much broader.

System features will include those you see here.



At first the architecture might look something like this. The system is extremely flexible, and the final design will be one that is evolved during a pilot test, using input from security professionals from throughout DOD and the contractor community. As I said earlier, we have toyed with the idea for a few weeks and have a version operating for design test that I would also be happy to demonstrate on the computer at the registration desk.



Mr. Grau is Chief, Information Security Division, for the Security Management Department, DoD Security Institute. Prior to joining the Institute in 1983, he enjoyed a long career in security and law enforcement in various positions with the Army. Mr. Grau's writings on security subjects have appeared in many security and training publications.

Planning for the Future

by Joseph A. Grau

Jim Riedel asked me to try to concentrate on the question of what we are doing and should do to prepare people to deal with the sort of issues he, Dee-Dee and Ernie have been discussing. That's fine with me, because that's pretty much what I've been doing for the past 10 years or so.

Before I do that, though, let me lay out one of my biases on the table. You're going to notice that I'm not going to be talking about "security awareness." I apologize for that, but I'd ask you to be patient with an old dog who finds it tough to learn new tricks, particularly when the new tricks aren't any better than his old ones. When I talk about the things we've been considering this week, I use the term "security education." It's the term I've been using all my professional life; it's the term used by the majority of my colleagues in the business, and it's the term used in the Executive Order which establishes the Information Security Program. It's not really all that good a term, but for my money, it's a cut above "security awareness." "Security awareness" seems to imply that what all this is about is making people *aware* of problems, situations, ideas, and requirements. While that's undoubtedly necessary, simply making someone aware of something doesn't mean they'll do anything in response to the awareness. To me, we're looking at a much broader spectrum of activity—instilling awareness, enabling, motivating, and promoting understanding.

Now, what difference does it make what we call this stuff as long as we do it well? To me, this problem of terminology *does* make a difference. The language we use shapes not only other people's perceptions of our thoughts and intentions, it also subtly influences our own thinking on the subject. And I believe that the fact that some of us say "security education" and others say "security awareness"—while neither term is really a fitting description of what we're talking about—underscores the crying need for us to do what Jim suggested just a short while ago. Before we plod on doing things to make security education better, we must decide what it ought to be doing in the first place. We need to put some real attention and effort into defining the nature of the effort; we need to develop some reasonable, workable, and meaningful goals, and we need to "scope" the issue so that we can properly es-

establish policy, communicate requirements, oversee compliance, and enhance attainment of the objectives.

Now, I'm not saying that I agree entirely with the analysis Jim presented a while ago. In fact, he and I have some disagreements about a couple of his ideas. But that's fine. What's extremely important about his presentation is what it challenges us to do and that it gives us some solid groundwork for achieving. Put bluntly, it challenges us to stop and figure out just what we're talking about. And that's *long* overdue.

When I teach the security education block in our Information Security Management Course, I usually start out by asking how many people in the class feel that their organizations have truly effective, high-quality security education programs. Of the 45 to 50 people in the classroom, the average number of hands raised is four or five. I find it very difficult to believe that all those folks who see their security education programs as lacking in quality are wrong. I think we need to listen hard to those people telling us that their security education programs are *not*—to paraphrase a well-known recruiting slogan—all that they could be. I think we need to listen especially hard to them because many of them are the folks who are *responsible* for security education in their organizations. They're not criticizing someone else—which is easy. They're criticizing themselves—which isn't so easy, and deserves our careful attention.

What's the matter? What's missing? What's defective? Where's the flaw? Well, let me tell you about my friend Otto and the towel rack.

Otto retired a few months ago. After a few weeks of suffering Otto's gripes and grumbles about not having anything to do, his wife decided he needed a hobby. She figured woodworking would keep him occupied. So she went out and bought him a stack of wood. Nice wood. Good raw materials for woodworking. But Otto never really could figure out what to do with it. So it sat there. "A towel rack! Make a towel rack!" his wife finally said. "I've always wanted a nice towel rack." So Otto went out to try to make a towel rack. He examined the wood from one angle and then another, and ended up dumping it back on the pile. How can you make a towel rack without tools? Fair enough... Otto needs tools. So his wife—who saw his woodworking as the only possible hope for her sanity—went out and bought him a lathe and a jigsaw and a whole carton of assorted hand tools. And Otto set to work. He came up with some very interestingly-shaped pieces of wood, none of which had much to do with any potential towel rack. Otto needed instructions. So, driven by desperation, Otto's wife headed for the neighborhood bookstore, and came home with a gorgeous volume with detailed advice on the techniques of woodworking and beautiful, color photos of fine examples of quality wood-craftsmanship. Otto pored over the book, headed for the garage, and produced a set of truly excellent pieces of wood, roughly shaped like parts of a

towel-rack, with perfectly beveled edges, satin-smooth surfaces, and corners cut to perfect angles. And his wife is still without a towel rack.

Ladies and gentlemen, I'd suggest that this little story is a pretty fair allegory for where we are and have been in security education. Like Otto's wife, we've put in place a lot of the necessary precursors to our towel rack—quality security education. But we still don't have a towel rack.

Back in the olden days (before about 1980), the assumption was that given knowledge of a subject, people could teach it. Subject-matter knowledge—raw material—was the key, it seemed. We taught security folks how to do security things, and assumed they could and would then pass them along. We ended up with a pile of wood. The wood was very useful in terms of overall program quality, but *not* in terms of security education. Then we decided, about 1980, that people needed to be *motivated* to do security education, so we placed *emphasis* on it. And a lot of conscientious, well-meaning folks went out and worked hard and substantially increased the organizational resources being devoted to security education—and ended up simply rearranging the woodpile.

Then we decided people should be given tools. And we were right about that. We started churning out videotapes and handbooks and visual aids and posters and all sorts of wonderful tools. And folks went out and used them. They had little idea *how* to use them, so they ended up producing a lot of really strange-looking pieces of wood, and not much else. Then we got smarter. People needed to be taught how to use the tools. We started publishing how-to material, and the Institute began its Security Briefer's Course and Train-the-Trainers Course. Excellent efforts, that help people produce higher-quality pieces for their security education towel racks. But something is still missing.

What's missing, I think, is the ability for the people who are charged with realizing security education programs in our activities to *design* and *develop* programs which will fulfill appropriate and meaningful goals in the real world of their organizational environments. Many of them have the subject-matter knowledge that's our essential raw material, are motivated to put real effort into the program, can ferret out good tools to use, and can use the individual tools effectively. But they are at a loss as to how to go about determining what pieces are needed, how those pieces should fit together, how they should be shaped so they join properly, and what the final product should look like. We have security education programs which consist of people doing sometimes excellent things, but doing them far too often in an uncoordinated and thus less than optimally effective way. We have security education programs with ill-defined goals, that do not suit the organizational realities of their particular environments and target populations, and that

fail, not because of lack of craftsmanship on the cabinetmaker's part, but because no one prepares a guiding design.

So what do we do about this? First, I think, we need to do what Jim urged us to do—come to grips with the basic issues of what security education is and what it should provide us. It's essential to have a clear and realistic picture of what needs to be done before we can start enabling people to do it. We also need to find ways to articulate the goals and objectives we define, so that those trying to achieve them can work with a clear understanding of the results that are expected of them.

Second, we need to keep on doing the good things we've been doing. Perhaps, as we put those things into the context of a well-defined, goal-oriented security education program, we can do them better. We need to help our security folks acquire and maintain the subject-matter knowledge that's necessary. We need to positively motivate them to put forth effort—their best effort—to attain the program's goals. We need to help them obtain the tools that can make their efforts easier and more productive. And we need to help them better use those tools, through efforts such as the Security Briefer's Course, publishing "hints, tips, and how-to's," etc.

Then comes the step beyond. We must work to enable the security professionals and non-professionals who are out there trying to get the job done to take the tools, raw materials, techniques, and skills they've accumulated and use them in a rational, planned, effective and coordinated way to make our security education goals realities in the specific context of their specific organizations.

Notice, please, that I didn't say we should "teach" them to do it. Nor did I say "motivate," "educate," "help," or "require" them to do it. I said we need to *enable* them to realize our goals in their work settings. That means we must provide an environment in which it *can* be done, create a climate of expectations in which it *must* be done, help them develop the ability to do it *well*, and promote their confidence that they can do it. Let's talk about some specifics. Let me give you some ideas which I think represent the sort of things we could and should be doing to make all this happen.

(1) We need to *require* quality in security education, and make people accountable for providing it. This is extremely important in a time of constrained resources—like *now*. We have to start realizing that the people who are trying to do security education in the field are in continual competition for constrained resources. They need ammunition to use in obtaining those resources. If management is allowed to see quality in security education as something that's optional, nice-to-have, or "suggested," they'll put their money on the "essentials," and our security people are going to end up holding an empty bag. I heard of a comment by a rather senior security professional a few weeks ago that it's time to stop pretending people should be

doing more with less and start realizing that people are going to be doing less with less. I think he's 100% right, and that this means that less has to be *better*.

(2) We must realize that a narrow view of how security education "happens" is dangerous. People are learning all the time, whether we want them to or not. They're forming perceptions, developing understandings (accurate or otherwise), forming attitudes, and gaining knowledge (correct or not). They learn every time they have any interaction with our security programs. The inspector who concentrates on administrative nit-picking teaches them that security is just another administrative hassle. The security specialist who brushes off their question with a growled "because it's in the regulation" teaches them that their part in the security program isn't important enough to deserve respectful attention. And the security regulation that could only be interpreted by a Ph.D. in applied linguistics who also happens to have a doctorate in law teaches them that security is something so complex and difficult that it had *better* be someone else's job. As we attempt to enable our security folks to achieve our goals, we need to help them understand (and keep in mind ourselves) that there are important security education implications in every facet of the implementation and operation of our security programs.

(3) We must reach out beyond the narrow confines of the traditional bounds of our concerns and draw upon the resources of other disciplines and types of activities. And then we need to make what we find available to the people who are doing the job—whether we find techniques, ideas, models, approaches—whatever. When I saw the program for this conference, my reaction was: "Alright! Now we're getting smart!" We've heard Henry Halff giving us the benefit of an educational technologist's view of our problems, Professor Brinkerhoff helping us see things from an educational leadership point-of-view, and Mr. Bailey giving us a marketer's insight into what this is all about. And in a little while, we'll hear about strategic planning from Bill DeGenero. This is pretty heretical, having all these "outsiders" in here telling us about our business. But they're not telling us about *our* business; they're telling us about *their* businesses and showing us what we might find useful from their professional disciplines. If we're going to do less with less and make it count, we have to look beyond our narrow horizons and beg, borrow, steal, plagiarize and purloin every idea, approach, and technique we can find to help us do things more effectively.

Let me give you just one example. There's a particular item in the performance technology bag of tricks that acts as a substitute for training people—not an add-on or an enhancement—an actual *substitute*. It's particularly good to use under the following conditions: the task is complex or difficult, the task is sometimes performed infrequently, the method of doing it is likely to change, training time and money are limited, and the consequences of

error can be serious. Does this sound like a perfect description of some of the things we need people to do in our security program? It does to me. This is a description of something called a job aid. There's a whole technology associated with figuring out when job aiding should and shouldn't be used, designing them, putting them together, and getting them into use. In a three-day workshop, you can learn enough to do a pretty good job of job-aiding; in one day, I could get you started off using them and give you enough help that you could learn the rest by yourself as you went along. In a recent class of 29 students in our Information Security Management Course, I asked how many people could tell me what a job aid is. Not a single hand went up.

When we find ideas, approaches, and techniques that could pay off in security education, then we have some figuring out to do. In what situations or at what organizational levels can they be used effectively, who needs to be taking advantage of them, where and in what situations are these people, what sort of stability do we have in those positions, and what is necessary to implant the approach or technique? These questions will determine the means we use—ranging from teaching-by-example, through disseminating an article or handbook, to including it in courses of instruction or setting up workshops or seminars—to infuse the approach or technique into the security education toolkit. Then we can properly hold people responsible for effective selection and use of the tools available.

(4) The last item on my short laundry list is that we must make sharing ideas and material a recognized requirement in security education. Notice, please, that I didn't say a "good idea" or a "recommended approach"—I said "requirement." Now, I don't mean "requirement" in the sense of something that gets put into a regulation. I mean "requirement" in the sense of something that's expected as a core element in how we do business. If we're going to do better with less, reinvention of the wheel and duplication of effort must become things of the past. *Smart* security people have been taking good advantage of sharing opportunities for years, and have done terrific work in the past few years of expanding those opportunities. What we have to do now is *systematize* being smart.

Let me give you a couple of horrible examples of what makes me see a need for some real effort in this area—all taken from my experience in our classes:

An installation security manager who tells me his organization could really benefit from our Information Security Orientation course—and is totally unaware of the fact we gave the course two months before at an installation right across town from his.

A military officer who tells me she really could use some good, current information about the nature of espionage, and has never seen a copy of the *Security Awareness Bulletin*.

How this could and should be done is a matter I'll leave to your judgment. There have been some excellent initiatives with regard to sharing of materials lately—most notably the security education consortia that have been springing up across the country. These initiatives deserve support, and, beyond that, we need to install cooperative efforts as the general practice in security education in both government and industry. This should include not simply the sharing or cooperative production of materials, but also the sharing of ideas, skills, and approaches. We can't *afford* not to.

It's always nice to have a bottom line—and always a relief for people when I finally get to it. So here it is.... In order for the professional and non-professional security personnel working in our security programs to develop and implement security education programs which will provide optimum payoff in this era of doing less with less, we are going to have to—

- Develop and promulgate *policy* which establishes demanding yet realistic goals for the program in terms of the effects we want it to have in support of our security efforts.
- Translate this policy into *requirements* that hold organizations and individuals clearly responsible for not only doing the job, but for the quality of what is done.
- *Enable* security staffs to develop, plan and implement effective security education efforts by fostering organizational environments that will support these efforts and by helping them obtain the understanding, skills, abilities, and confidence to do the job effectively.
- Provide *support* to these people as they work—with materials and tools when appropriate, with advice and assistance when needed, and with an awareness of the part each of us plays in promoting or inhibiting the continual self-education of everyone in our organizations as they encounter our security rules, policies, procedures, and techniques.
- Demand and promote the continual *transfusion* of ideas, information, approaches, techniques, and materials across organizational borders.
- *Oversee* efforts in this field with a continual focus on the requirement for quality, sending a clear signal that anything less than quality won't fill the bill.

PRESTO? Well, maybe it's not magical—but I think these steps will take us well down the road to enabling our security personnel to work the magic of making security education realize its potential.

In 1986, after 20 years of experience in the 3M Company, Mr. DeGenaro was appointed to head a newly-created department of Innovation Resources to foster innovation among 3M's more than 80,000 employees. He recently completed a one-year appointment as Director of Strategic Countermeasures Planning for the Office of the Secretary of Defense, introducing strategic planning concepts and methodologies to defense counterintelligence and security. Mr. DeGenaro is noted for developing successful motivational techniques in the management of human resources for large, complex systems.

Strategic Planning

by William E. DeGenaro

There are as many strategic planning approaches as there are consultants and academics in the business. The approach that you use is probably not any near as important as the quality of thinking that goes into it. I'll share with you the outline of a process that 3M uses, which is a logical flow of thinking beginning with an all important vision followed by a business definition which is intended to define the boundaries of the activities in which you engage... leading to the next step of identifying key success factors. Key success factors must make the difference between winning and losing regardless of who is playing the game. This is one of the most critical steps in the process. Experts suggest that if you have more than three or four steps, you haven't thought deeply enough about your activity. Here are three possibilities. Each key success factor generates a set of current issues, which will define the stage between your current capability and the quality level required to meet the needs of the stated key success factors. Finally, critical issues should generate a series of programs which are the action stage of the planning process. Since vision is the beginning of it all, let's spend some time discussing this most important stage.

Often a strategic plan is revisited or new plan required when an organization is faced with a substantial change in its environment. Noel Tichy, one of the country's leading organization experts, says this about the beginning and most important step of the process:

Perhaps the most essential component of a transformation is a vision of the future desired state. Transformations require a dream and require the organization to aspire to be something. Yet some way of assessing the current reality is also required in order to determine whether the vision fits with reality.

We have discussed the diagnostic portion of the transformation process as a linear process, but in reality it is a less ordered exploration. It is a period when hypotheses are generated and tested out with some data. Nevertheless, we argue that the basis for future action depends on this process of diagnosis. It's here that the capacity for planful opportunism is created. It readies the organization for its own renewal.

While vision is a clear statement about the future, Tichy emphasizes the importance of coming to grips with current reality. Peter M. Senge, in the most recent MIT Sloan School of Management *Journal*, discusses the principal of creative tension which develops from vision:

Leadership in a learning organization starts with the principle of creative tension. Creative tension comes from seeing clearly where we want to be, our 'vision', and telling the truth about where we are, our 'current reality'. The gap between the two generates a natural tension.

Creative tension can be resolved in two basic ways: by raising current reality toward the vision, or by lowering the vision toward current reality. Individuals, groups, and organizations who learn how to work with creative tension learn how to use the energy it generates to move reality more reliably toward their visions.

A common characteristic of great leadership is vision. Senge also states:

Without vision there is no creative tension. Creative tension cannot be generated from current reality alone. All the analysis in the world will never generate a vision. Many who are otherwise qualified to lead fail to do so because they try to substitute analysis for vision. They believe that, if only people understood current reality, they would surely feel the motivation to change. They are then disappointed to discover that people 'resist' the personal and organizational changes that must be made to alter reality. What they never grasp is that the natural energy for changing reality comes from holding a picture of what might be that is more important to people than what is.

But creative tension cannot be generated from vision alone; it demands an accurate picture of current reality as well. Vision without an understanding of current reality will more likely foster cynicism than creativity. The principle of creative tension teaches that an accurate picture of current reality is just as important as a compelling picture of a desired future.

While Tichy and Senge stress the need for superior analysis in order to get a handle on the present, Tichy argues that:

The transformational leader's task is to align the organization with its external environment. To do this, the organization's systems must be adjusted to enable the organization to deal effectively with changing issues. The challenge for these leaders is to recognize that the drama is best represented as a dynamic jigsaw puzzle with pieces that need to be fitted together. The fit is never perfect and constant adjustments must be made. The extent of these adjustments depends on the relative stability of economic, political, and cultural factors in the organization's environment.

How might we begin thinking about a vision for security organizations? Charles Sumner, who has written extensively on strategic behavior in business and government, suggests that *utility should be the ultimate goal* for strategy. That all too much has been made of the profit motive, which is difficult or impossible for staff organizations or public sector entities to identify with; therefore, *utility*, he suggests, would appear to be a much more appropriate end game cutting across all institutions. Utility is judged by those we serve...customers or clients. It's the value our customers place on our output. Here is a quick summary of the process framework. The leaders in quality, *e.g.*, the Malcom Baldrige award winners, argue that we must understand latent customer requirements which go well beyond current needs.

In preparing for these comments, I contacted 3M's security organization to get a sense of how a staff security group, focused on total quality, looks at their business. They have a substantial commitment to their customers. A key element in all good quality perspectives is to recognize that everyone has a customer or a client.

Sumner states:

Economists have long held that all human beings seek physical products or invisible services that have an attribute called utility. Utility, in the last analysis, is the want-gratifying power of some good or service. At the same time, cognitive psychologists have pointed to the fact that material objects and services are instrumental to more basic needs. The hungry person finds utility in food. Food is an instrument for the satisfaction of a basic need: nourishment. The human being needing protection from raw nature finds utility in a house. The house is instrumental for the satisfaction of basic needs: shelter and warmth. The person who needs friendship and love finds that there is utility in a telephone call. Such a service is instrumental to a basic social need. A person who needs security finds utility in the operation of a police patrol. Such a service is in-

strumental to basic safety needs. This same utility is found in an insurance policy (instrumental to family security), a mortgage loan from a bank (instrumental to security of shelter), a day-care service for children (security for protection of loved ones), or a sanitation/garbage service (the maintenance of physical health).

In this sense, the primary and ultimate goal of all productive organizations, whether the Chase Manhattan Bank, the City of Detroit Sanitation Department, the Family and Child Service Association of Los Angeles (a Community Chest affiliate), the General Motors Corporation, or the police department in Atlanta, is the production of utility by means of a product or service to a certain constituency. The same might be said for the police department in Buenos Aires, the Commissariat of Agricultural Equipment in Moscow, or the Matsushita Electric Company in Tokyo.

Traditional economies have also regarded utility as the ultimate goal in the free paradigm. Utility and marginal utility are the starting points, the ultimate value goals, of all theories following this paradigm. Unfortunately, today leading basic textbooks on economics state bluntly that the purpose of business organizations is to make a profit, whereas the purpose of government organizations is to render a service.

Sumner's position is that all organizations are subject to the demand for utility. Over the long strategic life cycle, no organization can survive without supplying utility to customers and clients. If the organization fails to achieve this goal, resource suppliers from the outside will eventually cut off the support so necessary to survival.

Based on these inputs, we may have the beginning of a useful concept or at least a strawman vision for counterintelligence and security organizations. One that emphasizes utility or value which is primarily determined by those that we serve; customers or clients. In keeping with this attempt to relate security issues to a business strategy format, I interviewed, in addition to our own 3M security department, several companies which are in the business of marketing security products or services including the major casualty firms, alarm services, and a fire extinguisher smoke detector company.

You might be interested in just a few highlights from each of these interviews as I think you will find their issues, problems, and opportunities might not be as different from your circumstances as you may think. In all cases they agreed that security was, while important to everyone, one of the last things that people want to think about. In other words, it is not their primary mission. The awareness of the threat was sufficient in all cases as

was the focus on anticipating new threats. Perhaps the most significant common mindset is that new threats and vulnerabilities present new opportunity in the form of new products or services, and obviously the prospective customer remains their primary reason for being as utility is defined by the customers.

I would like to move on from the subject of vision based on utility and customers to current reality in order to create some necessary tension. Based on some work I did as Director of Innovation Resources at 3M and my government experience, I have become very aware of some key vulnerabilities, and more recently new threats. But first the threat.

New threats to our national security and corporate security are coming from many quarters in the form of economic espionage. Since returning to 3M from government, I have become even more aware of the growing threat of foreign competition ably supported by their national security organizations.

There are times when I feel that we have pitted a group of naive business amateurs against pros, and the outcome is predictable. Cases continue to pop up in the news—the latest being the announcement of Daewoo's latest listening post establishment just up the road at San Jose with a staff of 15 "scouts."

My own company has come under intelligence attacks far more aggressive than we have ever faced in the past. We have initiated a counterintelligence/info sec course and are working hard on raising the awareness to this increasingly serious threat.

Enough of the threat side—let me raise our most significant emerging vulnerability. How vulnerable are we? We know that disenchanted employees increase our vulnerability to all kinds of deviant behavior. Those who track work force attitudes suggest that there are negative trends developing rapidly. *Design News* reports:

KEMPEI TAI
THE JAPANESE SECRET SERVICE THEN AND NOW

"...INDUSTRIAL ESPIONAGE ACHIEVED A NEW PINNACLE OF RESPECTABILITY IN JAPAN WITH THE OPENING OF THE INSTITUTE FOR INDUSTRIAL PROTECTION, A SCHOOL AVOWEDLY ESTABLISHED TO TRAIN SPIES AND COUNTER-SPIES FOR JAPANESE CORPORATIONS."

"...THIS KIND OF INTELLIGENCE WORK IS REGARDED AS PATRIOTIC AND JUST AS VITAL AS MILITARY INTELLIGENCE GLEANED IN TIME OF WAR."

RICHARD DEACON

In recent times, the American work force has been decentralized, restructured, and downsized. Employee loyalty is declining because of a lack of confidence in organization stability. For management

this fact of corporate life has become distressing because employee loyalty and dedication creates and sustains a sense of drive and commitment that is vital to a successful organization. In a survey conducted by *Design News*, more than 40 percent of the respondents said they were dissatisfied with their jobs. Nearly 77 percent indicated they may voluntarily change employers within the next two years. One reason for the quest for change is higher earnings. The most important question seems to be whether management can improve this declining level of employee loyalty, or is it an inevitable product of today's business environment and our culture? (*Design News*, September 19, 1988)

According to an earlier *Forbes* article:

Right now Americans are working as hard as any people in the world. Whatever weaknesses our society suffers from, shiftlessness is not prominent among them. Two interrelated forces are transforming the worker's relationship to his employer: a revision in the way corporate assets are valued (both by owners and employees) and a decrease in the length of the typical product cycle. (*Forbes*, July 13, 1987)

The Human Resource Institute (HRI) in a 1990 study stated:

Trying to measure the motivating power of money is especially difficult in the U.S. where we are steeped in the Protestant work ethic. This ethic prescribes a commitment to the intrinsic value of hard work. Work has become the primary means by which we define ourselves as human beings.

For example, at social gatherings, as soon as we have the name straight, the next question is, "What do you do?" Not only does work form a major chunk of our personal identity, it is also a primary source of our sense of self-worth. With such a powerful work ethic, or 'worth ethic', it is difficult to weight the strength of money as a motivator. In spite of the ambiguous nature of monetary rewards, Americans generally rank money as the single most important factor in their job.

And the problem of money is also touched on in *Business and Society Review*:

Perhaps the main reason why we seem to be even more interested in money, especially within the last 15 years, is due to the fact that during this time, the standard of living for over 60 percent of Americans has stayed the same (the median family income has

remained virtually the same in constant dollars since 1973). Americans are concerned that they are working harder than ever, but they aren't being compensated for it. Thus, money is of particular and increasing concern for whether we have enough and what it will buy. (*Business and Society Review*, Summer 1988.)

The overall attitude being reflected in the recent *Fortune* survey:

A survey of over 5,000 executives and managers of ten Fortune 100 multinational corporations found that the importance of money has increased over the last 15 years.

The results echoed significant differences found in previous studies (according to race, religion, and social class), representing beliefs held by a particular socioeconomic profile comprised of white, upper-middle-class managers and professionals. However, it is evident that the increasing value we place on money has transcended socioeconomic boundaries. Our industrial society has become a nation of consumers, and money has become the basis for status. Ninety-five percent of the respondents either agree or strongly agree that, in industrial societies, people seem to define their importance and success by what they own. Education, which was previously intrinsically valued, has become a means to making money. Aesthetically valuable artwork has turned into 'investments,' homes are now 'assets,' and friends are 'contacts.'

B & E Review ran an article stating:

According to labor experts, Stephen Fuller and Irving Bluestone, 'Today's workers have an increased sense of entitlement, disregard for authority, and low esteem for our institutions... (they) place less emphasis on material achievement and more on personal fulfillment.' Similarly, management professor Michael Maccoby has concluded that a 'self-development ethic' is emerging among Americans. 'Such individuals are primarily concerned with personal growth and enjoyment of life at both work and leisure.' (*B & E Review*, April-June 1987).

Industry Week suggests that supervisors' attitudes about themselves are not shared by their employees:

Supervisors feel confident that they are a very trusted group. But when employees are asked, researchers find that that feeling may be more wishful thinking than reality. That's one of the conclusions gleaned from *Industry Week's* (August 1, 1988) survey asking readers, "What do you think about trust?"

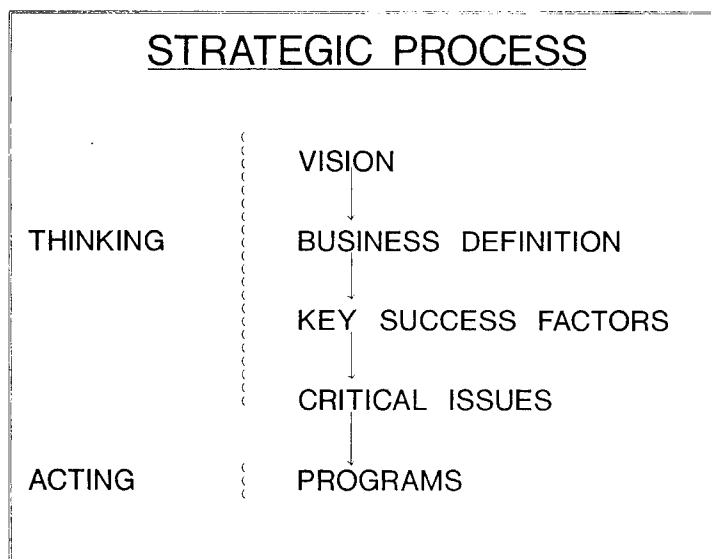
	Almost Always	Sometimes	Occasionally	Rarely
I trust what management tells me	27.4%	42.0%	20.7%	9.9%
I trust my peers	28.8	55.0	12.1	4.0
My subordinates trust me	51.8	41.1	4.6	1.1

Overall the greatest effect on morale may be in the middle management group according to HRI:

Morale and productivity of middle managers is in jeopardy as companies continue to downsize. A Hay Group report, covering 952 companies, shows that 37 percent reduced their work forces over a recent 12-month period. Another 26 percent offered inducements to older workers to retire early, and 22 percent announced hiring freezes. Whereas in 1977-78 nearly 70 percent of middle managers believed they had the opportunity to advance in their field.

In summary, let's revisit the main points of our strategic outline. The critical beginning point is establishing a vision, which I'm suggesting should be based on some notion of utility.

Defining the activity helps determine the utility and additionally establishes the boundaries in which we intend to perform. And finally here are some possible key success factors. The new threats are based on an insatiable requirement for information made necessary by global competition. This means more takers. The change in work force values and ethics may equate to more givers—all this in the context of less interest in the nation.



An environmental scanning consultant friend told me recently of input his firm gave to Pepsi a couple of years ago. "Get off the patriotic theme." Some

U.S. corporations behave as if they have become anational in sharp contrast to our foreign competitors.

In summary

- Good strategy requires a vision—the product of leadership and a learning organization
- Vision must be based on a form of utility as judged by customers.
- The necessary creative tension develops from the gap between the vision and current reality.
- Reality includes new economic threats and work force vulnerabilities.

SECURITY BUSINESS PLANNING

- CLEAR VISION/BUSINESS DEFINITION
- FOCUSED ON CUSTOMER REQUIREMENTS
- EMERGING THREATS REPRESENT OPPORTUNITIES
- TARGET MARKET AWARENESS ESSENTIAL
- RELATE BENEFITS TO CUSTOMERS' MISSION

Discussion moderated by R. Everett Gravelle, Director of the
Department of Defense Security Institute

We have selected the following transcribed excerpts from responses of the panelists in this section to questions from the floor.

Mr. Anderson: I would like to know about the element on which Joe Grau disagrees with Jim Riedel.

Mr. Grau: There's one basic difference I have with Jim and it has to do with scoping the effort. My concern is that Jim defines the outputs of security awareness as behaviors. When I look at the performance technology model, I see security awareness as properly attacking only two-thirds of what the performance technologists tell us are the influences on behavior. What we have traditionally looked at as security education attacks skill/knowledge deficiencies and motivation/incentive/attitudinal deficiencies. But then we have the environment. Jim identified the problem when he said we must look at it in the context of the constraints of the organizational environment. My problem with defining the outcomes of security education as behaviors is that this makes security education responsible for all of the environmental elements that form behaviors as well as what I think we can rationally expect. He's right that we, as a whole, have to be concerned about producing behaviors. But I think we need to put some reasonable bounds on what we are going to call *security awareness* or *security education* and limit the responsibility of the program to the outcomes that it can properly be expected to influence. The environment is something that is affected by the management of the security program as a whole, and the behaviors that Jim identifies are the kinds of things that the security program management as a whole have as the outcomes of their efforts. I'm not sure that it's going to be effective for us to include all of that in our concept of security education. I suggest we look at security education as producing conditions and attitudes, skills and abilities that promote those behaviors.

Mr. Anderson: But if you take some organizational training concepts, you can effectively say that training is only good until the training is over.

Mr. Grau: Then, sir, I would question why we ever called it good in the first place. I'm just concerned that specifying the behavior as the output may hold us responsible for a bigger bite that we should be taking. My indicator of success is the presence of the skills, attitudes, and motivation that promote the behavior.

Ms. Collins: I think right now we hold people responsible for behavior and that's what happens in our inspections. When we get inspected and people come in and they interview people and ask about security practices, it's the behavior question, that's what they are looking at, and in turn the security organization is held responsible. And so what I think some people are suggesting is, "How do we respond to that in a way that makes a difference?" Accountability—and if you've picked a theme from me about putting it where it belongs, it's because, from my own personal circumstance, and my peers in industry, we have each been individually burned enough times being held accountable for the masses that work in our organizations. Finally about three years ago I said, "I'm mad as hell and I'm not going to take this any more." I fought with a vengeance and got the president of our company to agree that we are going to do a formal appraisal system that has security included. And it's still taking time to get that implemented throughout the organization, but I've got his commitment that that needs to happen.

I think it's got to be a matter of individual accountability. I understand what you are saying is true, that education and training can only do so much and that training ends when you leave the room. You have got to have management systems in place that make that training worth anything out in the workplace. My frustration always was that I was out giving out the good news and they went back to the workplace and the manager said, "Don't worry about what security says, just get the job done." Why the hell did I give a briefing, why give indoctrinations, reindoctrinations, if out in the workplace the program managers, the technical element don't even endorse what we are doing? Inspections need to look at performance appraisal lists, too.

Question: I would address this to Jim Riedel or any panelist who would like to comment: You have all used the terms *training* and *education*. Could you give me an example of curriculum content that would illustrate what you mean by training and also would illustrate what you mean by education?

Dr. Riedel: I view education—activities that are directed toward preparing security professionals—as being of a broader scope. Training consists of more specific activities directed toward the cleared population for informing them of more specific security responsibilities and duties.

Mr. Grau: I have a somewhat different perspective: If I can specify exact procedures to be used, then I train people to perform those procedures; if I am in a situation where I cannot specify the exact procedures, then I need to educate people in principles that they can use to design or invent their own procedures to apply in that situation. The difference is in my ability to

specify the exact procedures or steps to be taken in a particular task. When I can do that, I either train or use a training substitute like job-aiding. When I cannot, I educate people to do something that makes sense to accomplish the objectives of the program.

Mr. Gravelle: Let me summarize in a few words: When you know what you want someone to do, you train them; when you don't, you educate them. That's from psychologist B. F. Skinner.

Meeting the Challenge

Government View

Brig. Gen. Frank K. Martin, Air Force Office of Security Police

Rusty Capps, National Coordinator, Development of Espionage and Counterintelligence Awareness Briefing

Willis J. Reilly, Deputy Director of Security, CIA

Industry View

Jed Selter, Senior Manager, Security and Fire Protection, The Boeing Company

Lawrence J. Howe, Vice-President, Corporate Security, Science Applications International Corporation

Catherine A. Dyl, Corporate Security Manager, Bolt Beranek and Newman

General Martin is the Air Force commander of the Office of Security Police at Kirtland Air Force Base, N.M., and the assistant inspector general for security, Office of the Secretary of the Air Force, Washington, D.C. He develops and manages Air Force security, law enforcement and information security programs, as well as programs for firearms training. In addition he provides leadership for more than 50,000 security police and 1,400 combat arms training specialists deployed throughout the world.

The Air Force Perspective

by Brigadier General Frank K. Martin

My compliments to PERSEREC and those folks that are putting on this superb conference. I would hope that in the few minutes that are allocated to me I can provoke you a little bit because that is precisely what I would like to do. I'm going to tell you a little bit about the Air Force and I'll start by talking about the security police where there are 36,000 folks on active duty. Most of them are first termers, that means they are between 18 and 22 years old. About 42 percent of the force is that age. They work in law enforcement and security and, yes, they do work in information security too—but only about 900 of those, and we will talk about them in a few minutes.

We have something else that we require of them, and I think that every military organization requires it. We require each of them to be a soldier. A soldier in the broadest sense, a warrior is what we would like them to be, require them to be able to defend bases and defend things. Not only things that appear in computers or that appear as classified material, but to defend aircraft. So we don't have narrow, confined functional lines that say, "This is your only job"—at least not in the security police world. Now we would like to think that in the Air Force we can get away from the slogans like "security is everybody's job." When a security guy talks like that, the rest of the Air Force looks at him and says you are just trying to get me to do your work, and perhaps there is some truth to that. We also hang on to this thing called "owner-user." It is not my responsibility as chief cop of the Air Force to take care of some little oxygen regeneration unit. Responsibility for that, of course, belongs to the authorized user. But cutesy phrases that we've developed over time—are, I believe, phrases that we need to get away from.

What are some of our folks doing today? Well it wouldn't take a whole lot to convince you, I don't believe, that what our folks are doing today is just like the rest of the United States military. They're over in Desert Shield as well as other places in the world. We train to do that sort of thing. And I think it is important for the military industrial complex to understand that we're doing it and we're doing it extraordinarily well. One thing that the United States military knows

how to do is mobilize. We know how to deploy, and you should be very proud of that, as I am.

Let me turn to the subject in hand: security awareness. We are talking about building security in from the outset. When you start something, when the germ of an idea comes out—and I watched the video out there a little while ago, and I thought it was just marvelous: When the statement of work, that we end up releasing to and working with industry on is written, that's where security needs to start. It needs to start as part of that contract. We develop the thing, it is nothing magical, it's called security systems engineering. Start factoring security in at the front end. That's very easy for the group of 160 or so seated here to agree with. But it is much more difficult to get the R&D world to agree with, to get the acquisition world to agree with it, and perhaps get some of your companies to agree with it. But it is our contention that will make the difference in the future as to where we go. With respect to security awareness, our goal is very simple, and I think most of you would sign on with the same kind of goal. If we would write it down, we would say, "to ensure that Air Force people understand their responsibility for protecting our nation's secrets and to motivate them to fulfill those responsibilities." My, that sounds great; that is easy to say; you can put that thing on that wall and you can get almost anybody to sign up to it.

Now how do you make it happen? That's what this whole week has been about. How do you make it happen? We need your help, and I think one of the most constructive things I've heard this morning was there is a lot of expertise in this building, in this room, and we are not sharing it. Perhaps we ought to be doing better. Security in our view doesn't start necessarily in the document stage, it doesn't start with the requirements (I'm a practitioner; I talk about bases, wings, and units). Security starts at the main gate. Whether or not that base looks good or looks secure may depend on who it is we have at the gate, or what the gate looks like. With all due deference to my colleagues from other services, as far as I'm concerned my goal is to make sure the Air Force doesn't get hit. And I hope the other services don't either, but if it comes down to one or the other, I hope we *look* and are more secure. Now some have said, "All that you are talking about is a kind of veneer of security." No, I am talking about perception, and I think that there is something in the perception of security that is important to pay attention to.

Our security education program then, if you would follow with me, starts at the main gate but it goes on. We try to avoid what was talked about this morning, the "too much too soon." Our security education process has three phases. We do believe that it is important to start when you bring the individual in—and it really doesn't matter whether they're going to be commissioned, part of the enlisted corps, or part of our civilian component. It's important to start talking about security—maybe that's the wrong word, perhaps it is more important to start talking about *responsibilities*—because that's what it's all

about. We teach them in basic military training how to march—we teach them discipline—all kinds of techniques are used—but there are some responsibilities that we need to lay in there. We'd like to think that we are doing it well, and we need to keep tinkering with that in my view. I can elaborate on that later.

We are not trying to teach the aircraft mechanic how to mark classified documents. We are trying to teach him how to use a classified tech order so he can fix the F16 so we can take off, because that's what his job is. We are trying to put that balance in there. So we start out with some initial training, and then we do some indoctrination training. I'm not sure that we do it well, badly, or even better than anybody else. But that training includes discussions of what it means to be on an air base and what security is about in your work center. It doesn't do a whole lot of good to take the F-16 mechanic and talk to him about security in the command post when the poor guy never knows where it is and is never going to see it at all. We need to talk to him or her in terms of the job they have to do within the Air Force and how it applies.

Local procedures: We can get hung up with local procedures if we are not careful. For those who have to handle classified materials, there's the time to start talking to them. We've got to be very careful that we don't create that environment that I think some of you have cautioned us against, of loading them up at basic military training only to have them arrive at their first base, and be told by their supervisor, "Forget what you learned there—this is how we do it here." Some of you have gone out and listened and talked to some folks, and I suspect that you have heard that damning comment on our whole program.

So we do basic training as an initial phase; we do indoctrination training when the individual gets to the base; and then we get to this thing called recurring training. You can talk a lot of training and you begin to wonder, "Maybe we harp too much on that." Are we training what we want the people to do, or are they interpreting the training for themselves? And that takes us to recurring training.

Recurring training can be done very quickly—we can do a great job and you've heard about it. We can give you this document to read and initial here, and when the next year comes around, initial again—we may even change the date of the document, then we sit back very smugly and say, "They're trained." But we happen to think in the Air Force that the program of Training-the-Trainer makes sense. We wish we could do more of that. We have been doing it for sometime, and we are going to continue to do that. But the trainer has to be trained in those areas that apply to the agency or work center that he represents. Annual plans, annual training plans can reduce that read-and-initial kind of mind set that we find ourselves getting into. I think another significant aspect of the United States Air Force education program is guidance, or you can call it policy, you can call it regs, you can call it pamphlets—but that's what we put out. Our information security staff is keyed to doing that. The

guidance needs to go to commanders, commanders who have the responsibility. Responsibility does not sit with the chief cop of the Air Force sitting at Kirtland Air Force Base. The responsibility sits with those wing, base, squadron, and flight commanders around the United States Air Force. We have to drive that message to them. We have to drive it home, and I would argue that it should be an essential element in the basic kind of training that we are doing, that's where it needs to be built up. But in general, we need to reach those folks who are responsible, and know their mission better than anybody else.

Trying to use technology to get away from doing things by the numbers to make things work a little faster: I'm quite taken by the comment that was made: "Maybe we ought to make an adventure out of this." Maybe we ought to put some of those computers to work and then go one step further. Let that count as training, and if we don't do that we are making a big mistake. Sometimes I wonder if those of us who are in leadership positions are willing to accept that risk; that is, let it count for training.

Our *Continuing Evaluation of Personnel* video is just another example. Our key is not to get folks to rat or snitch on somebody else. We tried to couch that whole production in terms of how you get help for people—people who might need help, rather than saying, "I want you to look at him and make sure that he does not have too much money or little money or something else that's a little squirrely about the individual." I don't know how well that is going to work. It's out; it out in the Air Force, and available in other agencies.

We're doing a video which is entitled *An Introduction of the Duties and Responsibilities of A Security Manager*. Remember what a security manager is; that's not a full-time job, and that might be true with some FSOs also, but in the Air Force many security managers especially those that are not in the security discipline—but they represent their work centers—are doing this as an additional duty. Those of you who have been in the military know how much attention additional duties get. We go back to Train-the-Trainer. We attempted to deal with this problem a little bit in the '80s, but we are not going to be able to do it in the '90s, and that is to get rid of security managers; "we'll do the whole thing ourselves," and put a professional in, or a number of professionals to cover the whole wing. We would still like to do that—but I don't think we are going to do it. I don't think we are going to be able to afford it. It seems to me that our goal does not need to be hung up by "administrivia," but determined by knowledge of what damage will be done to national security by whom, and in what way, and whether we can predict that and can identify it before the damage is irrevocable. That's the challenge for us; that's the challenge that I think faces us as we go into the 1990s. It takes people to make any program work and ours is no different. I think we have a great group of professionals.

Each year we send 300 information security professionals to DODSI for their training. Others take correspondence courses. I talked to you about the

Train-the-Trainer course working hand in hand with DODSI, and bringing that on line. Standardized lesson plans—the thing that we call educational subject block indexes: The term is terribly important; ESBI is what we use, but it is a computer-driven, computer-based menu of what it takes to understand and apply security regulations, whether they are security regulations in the information industrial or personnel security, or whether it is nuclear or non-nuclear security, the physical side of the house. It makes sense to us; we think it works out well. We continue to do that. It costs to do that, but it's worth the time and effort.

We have 900 people in the United States Air Force, out of that 36,000 that I told you, spending time in information security. Some of them have other missions and some of them do not. How do we get the word out to them? Quarterly security publications; recurring publications; publications which work well today, and will continue to work as long as we can get the funding for them. That is something we have to fight for, and it is one of the challenges of the '90s. Restrained budgets are going to make it more and more difficult.

We do one other thing: we take those 900 folks, and when they finish our training we give them a special experience identifier. Calling it by that term is not terribly important. The important message is to remember that now we have a tag on them. We know that they have been trained in the security discipline, we know that they have been trained as Information Security Specialists, and as we move them throughout the Air Force we can identify them. And smart squadron commanders will look though those special experience identifiers, rather than re-plow the old ground and start from the bottom every time there is a turnover of people. That makes sense. We also have coded every one of our positions in the Air Force, based on the requirement of that position. Not the individual, but based on the requirement of that position for access to classified material. Thus, we can cut down the number of people required, and we only have the level of access necessary for the job and the incumbent filling the job at that time.

There is another program that we have going that I think is a real success story. I've talked a lot about the folks having to go to Desert Shield, but there is another component of the Air Force, the civilian component that makes a big difference. We have men and women that are in the Air Force intern program; these are folks who are college graduates just starting out, working with the government, and we run them through a three-year intern program. They are top-notch recruits and, so far, we have used them throughout the DOD. Maynard Anderson has had a couple assigned to his staff over a period of time; he might have one right now working with him. The training includes the courses at DODSI and apprenticeships at various bases. Also they attend officer courses like the Security Police Basic Course.

We sent an intern down there just recently. Mind you, this is a civilian who, when we mobilize, is not going to pick up a gun (but everyone is pulling more than their share of weight at those bases that now find themselves rather short of people, because of the deployment). This individual went down to the school, and he out-shot everybody else. The number one gun. And there were a lot of folks in uniform who were embarrassed over that. I'm tickled by it. I think it's great. I think it's going to create some competition that will make some sense. We believe that it's a success story. The intern program has served us well; we will do everything to continue that. In fact, we would like to expand it throughout other disciplines in the Air Force. Those 60 graduates are going to be the senior leaders on the civilian side of the house and security police in years to come. And that's exactly how we ought to grow our leaders. We ought not to try to bring people from the top and plug them in. We ought to be growing them from the bottom.

People from all disciplines, as I mentioned before, perform part-time security duties. Remember, again, it's part-time. It's a challenge—a challenge that we have to work with. The key, as it has been mentioned here today so many times, and yesterday, is leadership: How you instill in the senior leaders the requirements to ensure that security is met. And you don't do it through inspection in my view, particularly sole dependence on inspections. I think Dr. Brinkerhoff was right on when he said, "maybe we should shoot the inspectors"; and I am one. I wonder if we have the nerve to do that. I wonder if we have the nerve and capability to build a program of security excellence and quality *early* into the program, rather than at the out-end. I would argue that they can if we are willing to take a little bit of risk. A former Chief of Staff once said, "We got to have a few mavericks around." We shouldn't shoot them, we need to listen to their ideas. Maybe out of every 100 ideas, 98 would be no good, but two gems will be there. We need to create in this discipline some of those mavericks and listen to them, and when the 99th idea comes up, we will know it if they haven't killed the person during the first 98. We need to do that.

They're two great lies in the world that have to do with inspections, and most of you have heard them. That's when the inspection team comes to the base and says, "Hey, we're here to help you," and the wing commander says, "I'm glad to have you." They are both lying, because our *philosophy* has been wrong. Our sins have been compliance—have you crossed the *t*'s and dotted the *i*'s, rather than, as mentioned here, "Do you have a program that works?" We can be very smug, sit back and say, "Ain't been any spies in the last 24 hours that we know of, so it must be that we're doing good." I'm not talking about that type of naive way of looking at it. I'm suggesting that we have qualified individuals, we give them responsibility, we give them authority, we make them accountable, we look at things like total quality management, which was brought up here yesterday. Is there anything wrong with that? I would argue not. I would argue there's a lot of things right with that, and we have to be willing to take that risk.

We probably ought to break out of the old rut to use the term a previous speaker talked about.

But where else are we going in security awareness? The Air Force doesn't operate in a vacuum. I think it's been clear, from some of the comments that I've made, that we work closely with DODSI, PERSEREC, the other services, and the Security Awareness and Education Subcommittee. This committee puts out pamphlets and brochures, and we're going to use them. We don't have a great pride of authorship. It doesn't have to say Air Force on it to be effective. It doesn't have to have the names of other executive agencies to be effective. We ought to cross-flow those things, and we ought to be doing that with a great deal of rapidity, and maybe we ought to give an award to the people who cross-flow the most information. Communication with and among departments and industry is going to be necessary if we're going to succeed in the '90s with some of our responsibilities.

In our view, and as been mentioned before, one of the basic things that we need to understand and be able to articulate is the threat. And we need to look to the intelligence community for threat information. The worst thing in the world, in my opinion, is for a security professional to get up and say, "The threat according to Frank Martin is as follows." That is meaningless. But the threat according to an intelligence agency is what we need to gear ourselves around. It's very easy to be caught up in the peace euphoria and suggest that there no longer is a threat. It is very easy for all of us in here to agree that that's not true. What we need is for the intelligence agencies to stand as they're doing, and suggest that it not only is not true, but there may be other pervasive threats and greater threats than we have faced in the past. That's the only way we are going to be able to cope with things like shrinking budgets.

Earlier speakers have said you have to get in there and fight for what it is that you need. There are some people who have suggested that we ought to re-look the entire way we do security, and we are going to do that in the Air Force, and in fact we are in the process of doing that. Because I know that there are going to be fewer than 36,000 people when we get to the end-strength for FY91. That is at the end of next September. There are going to be fewer people. There are few dollars to go around. But the question is, "What do you stop doing?" And if you don't go through it programmatically you end up possibly stopping the wrong thing. It's very easy for me to sit here with a group whose focus is mainly in information security, and say, "I wouldn't cut one position." Well, if I go to a meeting next week and the focus is nuclear security, and say, "I wouldn't cut one position," do you see where I am going? The point is, is nothing going to be cut? No, there are things that are going to be cut. The worse thing we can do is adopt the attitude that all too frequently I believe we do: We will have to do more with less. That was a bankrupt statement 10 years ago; it's more bankrupt today. In my view, we have to do less with less. The real key is deciding what it is we are going to quit doing. Who else are we going to

get involved; and we've got to be careful how we get them involved. Security needs to be included. Security needs to be a basis. Security needs to be followed up as a responsibility, and I suggest that maybe there is an ad campaign that can be used publicly.

Maybe we need some imaginative types who can go out and put together this ad campaign. They don't need to be necessarily pros. We just need to get the message out. I think the work that PERSEREC has done in the pamphlet *Beyond Compliance* is a step in the right direction. I would encourage you to read it and pay attention to what it says. I noted that they quoted both Peterson and Waterman, *In Search of Excellence*. In all respect to them, I would change one of their terms MBWA, *management by wandering about*. I don't like the term *management*. I like the term *leadership*. Leadership by wandering about: I think that's important because we've got too many folks who are arm-chair leaders or arm-chair managers if you will. If you want to know what's happening in your organization, you've got to get down to the flight line, or the assembly line, or the data automation room—any of those places—and then be able to sit and listen. Does it make a difference? You bet it does.

How can we crack the security nut? Well, we can create a sense of pride, a sense of pride throughout the entire organization. You can create for everybody a stake in the outcome. They've got to understand that they have a stake. I will argue that it begins at basic military training. If I could, I'd start at the recruiting process. If I really could, I would start back in high school. And, as some folks have mentioned here, you have to reward success. I would also quickly add, "and penalize failure." And there are ways of doing that without denigrating individuals; you need measuring devices and, yes, you need some form of oversight. But adding more layers of inspection, in my view, does not solve the problem. And you have to train, and train, and train. We lose sight of that. Grab the good ideas and run with them. Set goals. I see nothing wrong with setting goals such as fewer security deviations this year than last year. And when you reach that goal, move the goal line out a little bit. Get rid of the variances, make that curve kind of tight. To do that, you may have to take some risk. And we may have to take some risk. I think the goals ought to be fluid.

As we reduce in size, we accept the challenge to use existing and emerging technologies as much as possible. We are going to continue to automate security awareness programs; the use of interacting video makes good sense to us and we are going to try to use that and are already using it to some degree. I mentioned before I like the idea of an ad campaign; I think it's useable. We are automating our security clearance office so that we can cut down the time between the decision that an individual needs a clearance and that whole process through DIS and the adjudication process. Far too much time is spent with things in the mail, asking questions and because you forgot to cross the *t*'s and dot the *i*'s. Let's get back to what the real issues are, because I think that they are far too important not to.

Security awareness in our view is paramount in protecting classified objects, and protecting technologies; but it's really paramount for the nation. It's paramount for the Air Force to maintain the readiness that it maintains today. It's going to be increasingly critical for the Air Force to maintain that type of readiness in the future. And I will leave you with some words that were never spoken but were intended to be spoken—by President Kennedy, in Dallas, many years ago. He penciled these words as a marginal note on a speech he was going to give, and he said, "Above all, words are not enough. The United States is a peaceful nation, and where our strength and determination are clear, our words need merely to convey conviction, not belligerence. If we are strong, our strength will speak for itself. If we are weak, words will be of no help." Thank you very much.

Mr. Capps is the national DECA (Development of Espionage and Counterintelligence Awareness) coordinator at FBI headquarters. He has been a Special Agent for 16 years working in a variety of assignments. Prior to joining the FBI, he served for eight years as a U.S. Army officer.

The FBI's DECA Program

by Freddie L. (Rusty) Capps

I would like to begin by talking about the name we have chosen for our espionage awareness program. We call it the "DECA program" because, as Roger pointed out, none of us has time in any speech to say "Development of Espionage and Foreign Counterintelligence Awareness program" more than once or twice during a speech. The DECA program actually began, for those of you that are not aware, about 18 years ago. It was started on the East Coast by a very well known counterintelligence agent, Herb Clough. Herb was assigned as Assistant and Special Agent in Charge of the New Haven Office. New Haven had no foreign diplomatic establishments and, therefore, didn't have much of a Foreign Counterintelligence (FCI) Program. He decided there must be a way to initiate counterintelligence investigations in a smaller office, and contacted several defense contractors to see if their employees were being approached by hostile intelligence services. As Maynard pointed out earlier, we no longer call them hostile intelligence services, but this is a history lesson, so we'll regress a bit.

In his conversation with contractors, Herb found they were being contacted by the Soviets and the Eastern Bloc services. Several excellent double-agent operations resulted from Herb's efforts. By 1977, the program was instituted throughout the Bureau and called DECA, "Developing Counterintelligence Awareness." Two years ago we inserted Espionage into the program's title. It then became and is today the Development of Espionage and Counterintelligence Awareness program.

Today we have FBI agents assigned as DECA coordinators in all 56 of our field offices. You've got to understand, however, resources drive our program as they drive all of yours, and in some cases the DECA coordinator in smaller offices does DECA only about 10 percent of the time. Our DECA coordinator in Puerto Rico has only three defense contractors to worry about, while Dave Granish, who is in the audience today (the newly appointed DECA coordinator from Los Angeles) has more than 1600 companies within his division. In any case, Herb's program has now expanded Bureau-wide and there are several aspects of it that I want to discuss with you today.

I am hopeful that during the question and answer session we can deal with some of the important awareness issues that are on your mind. Some of

you have been candid enough to share them with me already and, truly, I do appreciate it. We are interested in making this program as effective for you, our consumers, as we possibly can. Anyway, we will talk a bit about our enhancements to the DECA program; about some of the different briefing modules that are available to you from the DECA program and then, lastly, we'll discuss the National Security Threat List which Maynard Anderson mentioned earlier. This is the follow-on to our criteria country list. As this new approach is finalized, it will certainly have some bearing on the designated country list.

Enhancements of the DECA program

First of all, you are looking at the first enhancement to the DECA program. Appointing Rusty Capps the National DECA Coordinator (NDC) was the first step in the process.

A second enhancement came in July, 1990, the National DECA Advisory Committee. This group brings together DECA coordinators from around the United States, to assist and advise in policy matters, conferences, and training.

Standardization of DECA tools available to the field (slides, speeches, videos)

One of the first things that I did when I arrived in Washington was to send updated slides and speeches to our field offices. My goal was to standardize and to upgrade the DECA briefings that we provided. One criticism that I heard was that some DECA briefings were boring and lacked currency. Quite frankly, coordinators in small offices who only work 10 to 15 percent of their time on DECA don't have the time to create the new tools and materials that they need. As an aside, you should know that my staff is not massive; as a matter of fact, you are looking at the entire National DECA staff. And you can imagine, there is a limit to what one person can do. But I can also tell you that we recognize the benefits of this program, the power of this program, and the impact of this program on the changes that are occurring in the world today. And though currently small, I anticipate that the DECA element at our headquarters will grow over the next few months and years to satisfy the additional requirements that we're placing on it.

Another area of concern to me is monies allocated to DECA. I am told that we are going to get some money in 1991 and 1992 for DECA. In 1993, DECA will be a line item in the FBI budget. That's good news to a lot of field DECA coordinators who are tired of paying for coffee and doughnuts out of their own pockets.

Another enhancement in which some of you participated in Denver, May, 1990, was the two-day DECA symposium. It generated some favorable feedback and we plan more symposia in the future.

Joint agency awareness training

We've had some real success in our relationship, first in Los Angeles and then around the United States, with the Defense Investigative Service (DIS). We want to expand on that success. When I did my first DECA presentations four years ago in Los Angeles, I recognized quickly that I could only speak to part of the problem—the threat from foreign intelligence services. My audience, many of you, had other issues about which I had little knowledge. For instance, issues involving something called the "ism." I had no clue what an "ism" was, unless it was a reference to communism. Well, with help from my friends at DIS I found out what an "ism" was. Fortunately, I had the benefit of a talented and flexible DIS Regional Director of Industrial Security in Los Angeles, Greg Gwash. Greg agreed to join me on the speaking platform and we developed a very successful joint briefing program in Los Angeles. I think that kind of joint effort is crucial to meeting the new threat we face today. Greg and I continue to work to expand on our initial successes.

The ISAC concept

ISAC has already been mentioned here earlier by Dee Dee Collins. ISAC is a favorite vehicle of mine for a number of reasons, not the least of which is because it works. It joins together government and industry, to share information and materials, in a time when resources are diminishing. We are in the process of expanding the ISAC concept. It will take some time, but I look forward to its expansion because I think it is a way we can do a lot more with what we have available to us.

Videos

We have heard a lot of talk here about the use of educational videos. Videos, I think, are helpful in getting the message out when you can't be in as many places and talk to as many people as you'd like. One of the first things I recognized on taking over Los Angeles' DECA program was that there were 1600 companies and 250,000 plus employees out there that I had to reach. That's a large audience and there was only me to reach them. There was no way I was going to be able to touch as many people as I wanted to, and I began to look for ways to clone our DECA message.

Fortunately, we had some very wonderful support from the private sector. First, we worked with Hughes Aircraft Company on "Espionage 2000." The thing that I think is most significant about "Espionage 2000," beyond the fact that it is an excellent awareness video, is that it broke new ground in the

area of FBI-private sector cooperation. Later videos had less difficulty in gaining approval because of the efforts of all those who participated in the making of "Espionage 2000." The Northrop video, "Espionage Alert," was our second joint video. It has received outstanding reviews and both national and international recognition. Copies of both videos are available from local DECA coordinators, DIS, or DoDSI in Richmond.

There are others videos out there that I would recommend to you. DIA has an excellent tape on the Pollard case. It makes one of the most significant points in the awareness education business. It tells our employees that it is okay to come forward and talk about something they have seen that arouses their suspicions for a number of reasons. This is the first video I've seen that, in a very credible way, addresses this important issue.

Another video that's a very effective awareness tool is the Diane Sawyer interview of KGB Chairman Kryuchkov, on *Prime Time*. It makes several awareness points, but is particularly effective in addressing the continuation, at very high levels, of intelligence collection by the KGB in the United States—*glasnost* and *perestroika* notwithstanding. As a matter of fact, at one point Chairman Kryuchkov says in an answer to one of Diane's (I frankly find it absolutely inconceivable that any Soviet, let alone the Chairman of the KGB, would subject himself to an interrogation by an American reporter)



Rusty Capps, FBI National DECA Coordinator

questions about their attempts to assist Soviet businessmen, "Well, you know we're not very good businessmen, and we are going to help and not hinder our efforts in this area. I think I've told you too much." Well, from my point of view, he didn't tell us too much at all. This is a very powerful way to show your audiences one aspect of what we can expect from the KGB in the future.

As a subject for future videos, I think that the next plateau in espionage awareness education is to look at the impact of espionage on families and co-workers of those traitors who have committed espionage. These videos could focus on the devastation of their families after the cases become public knowledge. The video's message would focus on negative aspects of espionage as a potential deterrent.

There is an ongoing project sponsored by the U.S. intelligence community. It involves the interviewing of espionage subjects in prison. They are now working on a video which will address this issue using some of the information and expertise acquired during their research. We hope the videos that result from this project will give you some additional tools for future espionage awareness briefings.

The last DECA enhancement that I would like to discuss with you is a new program being piloted in our Los Angeles office with the help of one of ISAC's working committees. Called the "Vulnerable Travel Program (VTP)," it is going to be a training package that will be sent to FBI field agents and industrial security professionals. In general terms, this is how it will work: briefers will receive a video, slides, and a lesson plan. They will be taught to prioritize a company's most vulnerable travelers—those people who, because of their access or because of the number of trips (or both)—are the most vulnerable to foreign intelligence services. Once selected, the briefer will provide these travelers with expanded travel briefings. After the traveler returns, a debriefing will occur followed by recontacts as needed. The goal of the program is to focus our resources on the most vulnerable of our travelers, raise their awareness level, establish rapport with them, and then check to see if they have been targeted by foreign intelligence services.

Current DECA modules available

Our current DECA briefing subjects are:

1) The World Intelligence Threat

I am not going to give you a threat briefing today, but I would like to give you a sense of the type of materials that we're making available to our field coordinators. The following is a portion of a recent travel report on the Soviet Union, dated November, 1990. It will relate to you some of the conditions in the Soviet Union today. The author was sent to contact several Soviet scientists who had not replied to invitations to attend a conference in the United States. This is what he had to say: "I secured a car and a driver through a family friend. The driver was necessary because many of the street signs in Moscow had been stolen and many other street signs and boulevards are being changed back to their pre-Revolutionary names. The price was about \$70.00 plus two cartons of Marlboros, three sausages, some coffee, and cosmetics. I'm reminded by some World War II veterans that this is not too different from post-World War II Berlin. And Moscow does have the look of a city after a battle—rubble-strewn garbage, ditches, rusting burnt out automobile bodies, broken glass abound. I was there in April and I could see that the physical condition of the streets had worsened since then. I expected that more repair work would have been completed over the summer—I was wrong. I recognized some of the dirt piles. My driver took me to

various institutes where I assumed that people I was looking for might be found. Most of the people working behind the reception desk were not helpful. I was often told that the person I was looking for was on break or out of the building. My driver finally pointed out there was a severe cigarette shortage and being an American meant that I could spare a pack. Try it, he said. Just like in the movies, without breaking eye contact with the individual, I would place a package of Marlboros on his desk. Big smiles all around. Within six days, I found everyone I was looking for. I should point out that this was true everywhere except at the reception desk at the Congress of Peoples Deputies of the Soviet Republic. When I pulled out a pack and placed it on the desk I was scolded by the duty officer and told that it was not necessary to give the Russian people bribes. I apologized. He kept the package of cigarettes.

2) The Intelligence Threat from the Peoples Republic of China

3) Foreign Intelligence Service Recruitment of Americans.

I consider this to be the most significant subject that the FBI has to discuss with Americans.

4) The Counterintelligence Impact of *Glasnost*

5) Core Technology Transfer (In development)

6) Espionage Since Walker

7) Nuclear Proliferation (In development)

**8) The Counterintelligence Impact of International Treaties—
Eastern Europe**

Lastly, as I mentioned earlier, I would like to spend a little time discussing with you the National Security Threat List (NSTL). I will tell you first of all that it replaces what was an ideological, country-based threat list—the Criteria Country List. The NSTL will be a two-tiered system: the first tier is the strategic country threat list (similar to the Criteria Country List); the second tier will be composed of specific issue threats. Some of the proposed issues are: nuclear proliferation; the threat to core technologies; active measures; targeting of U.S. government officials, government policy or the U.S. intelligence community; undeclared intelligence presence; national defense information; proprietary information; and international terrorism.

Well, after having shared these things with you, I think I would just ask for your help in being as articulate and vocal as you can in expressing to us in the DECA business how we can continue to evolve and provide you with

what you need. I am hopeful that I will be able to address some issues that are important to you in the question and answer session. Thank you.

Willis J. Reilly is Deputy Director of Security at the Central Intelligence Agency, and at the time of this symposium, acting Director of Security. Previous assignments in Mr. Reilly's 35-year career included deputy director for personnel security and director of the security clearance program at the CIA.

Meeting the Challenge: The View From the CIA

by Willis J. Reilly

It is always nice to visit California so we may think about the area's subject of greatest interest—earthquakes. While some may laugh about this comment, I would remind you that the average Californian well understands that the further you are away from the last earthquake the closer you are to the next one. It strikes me that there is a relevance of the earthquake issue to the topic of our interest, security awareness, and we should all ask ourselves to examine how people and institutions have dealt with each.

Just last week the people of Missouri were filled with *angst* over the prospect that the New Madrid fault was going to break loose and wreak havoc with a major Richter scale rumble. Well, last week came and went, the press has left the area, residents who conveniently put themselves out of reach have begun to return home, and the media are now dealing with it by benign neglect.

Only 14 months ago Santa Cruz—just across Monterey Bay—was rocked with the quake that stopped the World Series in the San Francisco area. Work still goes on in the region to pick up the pieces and return to a full and firm footing but, by and large, the rest of America probably has reduced its interest in this major event to its impact on a series of nationally televised baseball games. At the time of the earthquake the opposing managers made statements to the effect that the devastation wrought gave a clear indication of the relative minor importance of the games they played in the name of sport. I suggest to you that America, after a little over one year, is returning the World Series to a lionized perspective that ignores the statements of Roger Craig and Tony LaRusso.

So, unfortunately, I think we can look at the history of security awareness—a series of peaks and valleys marked by revelation of a major espionage case or, in the case of 1985, a series of such horrors, followed by emphasis on awareness programs to focus the threat and then a gradual building to pooh-poohing it all. And I do not exempt my own agency from this problem.

In many ways, despite the fact that great harm to the national security was uncovered, the "Year of the Spy" was a bonanza to the security com-

munity generally and the security awareness specialists in particular. For once it was clear that, between the Walkers, Howard, Pollard, Scrannage, Pelton and Wu-Tai Chin, the entire national system was affected. We have to say this to make the point that it is not a series of parochial programs that get compromised when espionage happens. Jay Pollard did not deliver to his case officers only material belonging to the Navy; he provided the best information from any source and any agency that he could locate.

The resultant fallout from these disclosures brought a national clamor for reform, recovery and renewal of the country's effort to protect its secrets. Because of the very positive interest of the Congress, funds were made available to reinvigorate our security programs and these programs have been attacked by the entire community with great diligence and, I believe, professionalism. I consider the fact that so many cases surfaced almost simultaneously as a long-lasting fuel that could drive security programs for more years than just one little earthquake could have done.

Aiding us in this revitalized work had been the confirmation that traditional enemies—as well as allies—were lurking out there ready to jump on any opportunity to negate the United States' efforts to ensure its national security and maintain its leadership role in the world. But—poof—the old order of world polity is fast disappearing and, short of Operation Desert Shield, a confused American public was starting to ask for its "Peace Dividend" and questioning the need for its defense establishment and, in some quarters, even the continuing need for a Central Intelligence Agency.

This should only suggest to us all, whether in my agency or some other element, that time may be running out on us as security educators and awareness specialists and that the earthquake-syndrome may be setting in. Fortunately, as a community, for once we have organized around the problem and have developed a strong and coherent program over the past four years. Commencing with leadership from the Stilwell Commission and the Department of Defense Security Institute, this work is being expanded upon by security education staffs of many agencies and departments and most relevantly by the Security Awareness and Education Subcommittee of AG/SCM's Personnel Security Committee under the dynamic leadership of Ms. Peg Fiehtner. But, make no mistake about it, the crossroads to future meaningfulness of our awareness programs is fast approaching.

In the aftermath of 1985 CIA did considerable examination of its security programs. It aggressively attacked its institutional personnel security programs, upgraded and modernized its physical and technical security capabilities, and went out on the hustings to preach the gospel of security awareness.

In 1988 DCI Webster created the Counterintelligence Center to better identify and negate the threat from hostile services and, I am happy to say, that center has a burgeoning awareness activity that has already developed a highly effective overview course on counterintelligence which describes methods used by hostile intelligence services in targeting U.S. government employees. This course is now becoming mandatory for all employees. Also it has developed and presented specialty programs for both components of our agency and other departments and is working on the development of more for sharing with both government and industry.

The Office of Security conducts general orientation programs on security and the threat to new employees, and re-orientes on-board personnel to ensure that all employees understand both the rules and regulations of our organization and the fact that those regulations exist because they are tied to threats and vulnerabilities against the national security. We are also very active in presentations to components of the agency on topics of special interest and relevance to their own particular situations, be they in the collection, analytic or support business. We also have an outreach program to industry with special emphasis on the training of corporate and project security officers as well as the government's elite program for training and certifying information systems security officers in the computer security field.

Special emphasis is given in addressing management level courses on the precept that security is a line function and that we cannot be successful and secure as an agency unless management takes this responsibility seriously. It is clear that, if we wait until we re-vet personnel at a cyclical five-year interval, the Office of Security can only determine how much damage was done. This theme has been constantly restated with management and it has taken hold. Bearing in mind that almost all identified traitors we have uncovered have carried significant "personal baggage," our message has been that we want to identify *troubled personnel* before they become *persons in trouble*.

Identifying troubled personnel itself is not enough and, in fact, would leave managers leery about the prospect of "tattle-taling" on their personnel only to get them in trouble or fired. Not only is "tattle-taling" not the best American tradition but there is also a tradition that addresses a separation of business and personal problems and a tendency for managers to ignore an employee's personal problems if the work is getting done. We believe we have sold management on the nexus of this theme as a security issue. However, and more important, the Agency has developed a series of programs geared at therapy and rehabilitation to restore the troubled employee to a productive and stable status. This has tended to convince the managers that attending to the troubled employee properly becomes a win-win situation.

All awareness programs are doomed to failure unless they are based on real, relevant and focused security programs. If they are not, they sow the

seeds of their own destruction as they get hung out for ridicule due to a non-responsiveness to threat. While it would be foolhardy to say that our concerns over the East Bloc are fully a thing of the past, if we choose to parrot pious platitudes expressing Cold War thinking we will fail in our mission. The basic message and concern will remain, but clearly we must update and refine the settings and situations as they exist today and downstream.

We are somewhat pleased with the progress and results we have achieved at CIA over the past four years, the key to which has been management involvement. At the same time I would say I am envious of the Air Force's model program at Norton Air Force Base which seems to catch the fabric of a total involvement program more fully. In that program professional security personnel have enthusiastically and ably infected an entire facility into developing an attitude that security is everyone's job. It is such an easy philosophical concept but so difficult to implement since people, not philosophers, have to implement and manage it.

We are looking for better ways to use awareness as the vehicle to ensure that the national security is kept intact and even strengthened. For that reason I believe that the development of a positive continuing evaluation program is not only the need of our times but also our insurance against forgetting about earthquakes. The key difference is that, right now, we cannot prevent the physical earthquake, but an alert and understanding work force in the intelligence and security business can certainly go a long way toward ensuring that there are no earthquake-like jolts to the national security in the years ahead.

And it is we who must take the leadership role to bring this about. Based on the progress of the past few years I am encouraged that we can succeed.

Mr. Selter is a career security manager with The Boeing Company. He is currently responsible for Business Management, and Computing and Communications Security. Mr. Selter recently completed two terms as Chairman of the Aerospace Industries Association of America (AIA) Industrial Security Committee and has helped in the development of the National Industrial Security Program.

Security Awareness: The Challenge of the '90s

by Robert J. (Jed) Selter

Introduction

I would guess the primary reason that I have been asked to be on this panel is because of my involvement with the National Industrial Security Program. The NISP has focused as much on people as it has on security issues. It has been a methodology for coordination. It has been and will continue to be people-based. If you take a step back and look at it, the NISP has been a strategy to increase communication among people toward a common end—collective coordination for process improvement.

In looking at the future, I believe we must anticipate and respond to changes in a rapidly moving setting. Some of this change will be well thought out and purposefully orchestrated. Much of it, however, may be a surprise—uncontrolled by us. Regardless, we will need to be responsive. We will be expected to positively handle it as if we had anticipated it. Situations may or may not be what we expect or want. More importantly, they probably won't be as easily resolved as we would like. As we address this change, I believe the one key element we can count on is...ourselves...security professionals. "We" may well be one of the few dependable constants on which we can rely.

To most effectively operate on this changeable scene, it is imperative that we re-evaluate and re-calibrate our focus and expand how we visualize and approach our profession and each other.

To deal with the fluidity of today's world, we need to become increasingly "general business" oriented; conversant with economic, political and social issues—both domestically and internationally—which affect and drive business. We cannot afford to be perceived simply as "specialists," or be looked at as slow moving, static, inflexible or set in outmoded ways. While attention to detail is necessary and appropriate, if we allow ourselves to get mired in dotting the "i's" and crossing the "t's", we will be left in the dust by forward thinkers, and eventually be left out. Instead, we must be prepared to think and act as "futurists" and in doing so, become credibly recognized in our cor-

poration hierarchies as involved, front-end contributors to our companies' plans and strategies.

This will require our ability to analyze increasingly less traditional problems in a very fast-paced environment. Our reaction time will be critical. More and more, we will be required to develop increasingly innovative solutions for flexibility: not temporary "quick fixes," but logically and methodically arrived at, long-term solutions.

To do the above, we must sense the environment and be introspective about *how* we react to it. I believe this involves several considerations: Our own *mental set toward change*, how effectively we *manage ourselves* and the need for *interpersonal coordination*. I'd like to expand on each of these separately.

Mental Set Toward Change—We must:

- Understand and keep our fingers on the pulse of the *real* world.
- Be flexible and respond in a timely manner.
- Think innovatively—"stay unreasonable." In other words, not settle for the status quo, but continue to question what we do, and strive for improvement.
- Search out problems and their causes, being careful not to react to symptoms.
- Develop a high comfort level with change.
- Adjust priorities to meet current needs.
- Periodically, stand back and take an objective, long view; look ahead; see how we are doing and where we are going. Consciously review what we think we have. Solutions to problems really are based on defining the right problem and involve one or more responsive solutions that bring higher value results.

Managing Ourselves

We can be most successful by emphasizing "mind control" with ourselves: Establishing overarching goals and working to them.

- *Knowing* where we are going: working to a plan to avoid perpetual firefighting. Writing down our plans and communicating them.

- Confirming that the results produced actually support our stated goals and our defined plans.
- In what we do, considering that proper motives result in the right actions. Understand and focus on the mission.
- Being honest with ourselves.
- Maintaining an updated mental database for decision making—decisions based on old, inappropriate, or incomplete data are usually the wrong decisions.
- Being results-oriented.
- Recognizing and positively channeling stress and emotions.
- Developing mental peripheral vision—being conscious of and staying dissatisfied with tunnel vision.
- We must enjoy what we do. We should periodically ask Teli Savalis' favorite question—"Who loves ya, Baby?"—The answer had better be ourselves!

Interpersonal Coordination

The term *partnership* is overused and worn out. Rather...we must

- Communicate "processes" together, dissect them, discuss them, understand them and seek out specific areas of improvement.
- Be selfless: team success depends on it.
- Trust each other and demonstrate it.
- Learn to understand and use system dynamics—how things happen—who influences events and how they get results.
- Be objective.
- Stay optimistic—optimism breeds confidence and positive results.
- Give praise easily.
- Be leaders.

As this relates to security awareness, one of our managers recently described to me how his staff addresses education. They have not used posters, newsletter articles, or trinkets with printed slogans. Their primary asset has successfully been themselves.

As he has described it to me, each of his staff members has been sensitized to and embraced a sincere, common attitude of "we are here to help." Equipped with the knowledge of requirements and an understanding of their customers' business processes, along with a large dose of common sense, each of his security administrators has been successful in developing an active awareness with the program people they support of what needs to be done, where to go to get more information, and who to contact for help.

They have come a tremendous distance in a very short time. They continue to demonstrate that the key element in increased security awareness has been their own preparation and interpersonal communication. To do this, they have had to adapt to the changing environment their customers face and have had to successfully internalize what I have discussed today.

In today's participatory management environment, the term *empower* is usually used to indicate a manager *enabling* a subordinate. In my view, this is too narrow. I believe enabling is a freeway cloverleaf proposition. We must all empower each other: multilevel, multifunctional and most importantly in our profession, multi-organizationally—among industry and government—no holds barred!

We must team as a single "we," not individual "I's." In doing so, we must take ownership of required actions to task completion and share the ownership glory of results and accomplishments with others.

Mr. Howe is the 35th President of the American Society for Industrial Security. He is the corporate vice-president for security of the Science Applications International Corporation. Mr. Howe has also served with the Central Intelligence Agency in a variety of assignments.

An Industry View

by Lawrence J. Howe

My task this afternoon is to present an industry view of the challenges ahead of us. I have approached this from the point of view of an "environmental impact statement" reflecting a theme repeated in many of the presentations at this symposium, that a change in perception now exists of a diminished threat. As a result, in many respects, the security field is looking for a new relevance. Now that the sky is not supposed to be falling, what is Chicken Little doing for work? We have based our craft on a preoccupation with an Evil Empire in which Darth Vader has just received the Nobel Peace prize.

Within the organizations we serve, there are those anxious to be free of the restraints imposed by the security safeguarding discipline. In that process, there are people who are quick to paint our breed as having been made irrelevant by changes in world-serious threats to our national well-being. We understand that it is only the nature of the threat that has changed. The theme of this discussion is to point out that we need to develop tools to deal with a world full of complex subtleties. Many of our past responses to perception of the threat have been perceived to be rigid, "by the numbers" approaches that are long on standardization but lack a flexibility to deal with issues which are not neatly resolved in absolutes.

Turning now to the present and the future, most would agree that technology and innovation have been vital elements for the United States to maintain a preeminent position in the world. These important assets should be anticipated to remain key factors in the more complex competitive environment in which we find ourselves. National defense has taken on a broader focus for which new approaches are necessary. The struggle has shifted to an economic contest in a process that began some time ago, but was overshadowed by a nuclear threat. Our "victory" over Communism has been as much, if not more, a battle won on an economic playing field where our military posture has been a primary factor in maintaining containment long enough for the economic outcome to be determined. The competition for political and economic prominence is more complex to comprehend than military confrontation. The added complexity makes it more difficult to devise clear strategies for response. In the economic sphere, there are no handy bipolar, adversarial groupings like NATO and the Warsaw Pact. The

multiple participants in the economic competition have little in the way of fixed alliances with the possible exception of the 1992 emergence of the European Economic Community (EEC). Even within the EEC, it is suggested the member states are likely to respond on matters of economic competition as separate, self-interested, economic units rather than as a block. To add to the confusion on where to focus our concerns, we are finding ourselves forming strategic economic alliances with industrial segments within nations with whom we are also in competition in other market areas. The world just does not have clearly definable bad guys anymore (with the exception of Saddam Hussein whose marketing instincts told him there was a void he could fill).

The question of the hour is how do we ensure relevance in security awareness as the national interest takes on different dimensions? First, we need some fresh thinking. I suggest that we who are identified with the security field are perceived, regrettably, as mutually supportive functionaries within a very entrenched bureaucracy. We are at risk of being indicted for being more attentive to preserving our own "rice bowls" than having something meaningful to say. Contemporary marketing strategy would suggest we need an image change. If the perception is that the world has changed, even if the perception is more generous than the reality, we need to project that we have readjusted to that change. Unless it is evident that we are mirroring a new reality, we will be dismissed out of hand, and our ability to make a positive contribution will be diminished.

What are some of the more evident complexities with which we have to deal? Clearly, state-sponsored intelligence gathering to glean U.S. high technology assets is one of our current major threats. This is all the more insidious because our "friends" are likely to be as heavily engaged in the process as our former Warsaw Pact adversaries. While the more jaundiced among us might suggest that this is not necessarily totally new, the change in scale certainly is likely to become more intense as the economic competition heats up. Additionally, the lack of clarity in U.S. policy with regard to the control of critical technology in a rapidly expanding world market is also preventing those in the security field from playing a significant role in the broader application of information security outside formal classification structure. Rapid closure needs to be made at the national policy level on the role of U.S. high technology in world trade. To date, progress in establishing a coherent national policy on critical technologies has been dismal.

The paradox of the moment is that we have a very procedurally intensive safeguarding structure for military-related assets but little in the way of measures to protect the much broader range of data and ideas that may well be the major components in our economic arsenal. Companies that engage in both national security-related work and also are involved in the commercial sector operate a two-tier security system. The very procedurally demanding nature of the Defense Industrial Security Program places a very high over-

head cost burden on contractors. Many companies find they are unable to devote much in the way of resources to proprietary information security measures because of the disproportionate demands of the compliance requirements associated with defense contracts.

It is beyond the scope of this discussion to make inquiry on the need to reappraise our national approach to classification management. For the purpose of discussion, the need to continue to afford protection to much of our military-related technology is not challenged. What is asserted is that we need to establish closure on a much broader information security posture. The present two-tier approach has us securely bolting and guarding the front door while the back door stands wide open.

Given that we may be over-protecting some assets and under-protecting others, it should be clear that changes are in order. The commercial sector will not accept, nor can they afford to adopt, some version of the present Defense Industrial Security Program (DISP) to protect a broad range of economically relevant high technology issues. What is needed is a reappraisal of the broader issue of safeguarding policy and practice to develop a consensus on the strategic importance of information security to our national economic goals. Above all, whatever program direction is devised, it is clear that it must be more relevant and cost-effective than our present approach to industrial security in the defense context.

If we who have been associated with national security-related programs in the past are going to make any contribution to protecting the much broader list of national assets involved in the new competition, we need to re-tool and do it quickly. Anything that is perceived as a regurgitation of the old litanies based on a bipolar world view dooms all of us to a richly deserved obscurity. In the presently emerging world science, counterintelligence has taken on a much broader and challenging meaning. For the United States to remain a major world force, industry must remain competitive. To succeed competitively means not only producing the best product or service at the best market price but also ensuring that the effort invested in developing these products or services bears fruit through adequate, reasonable, *tailored* safeguarding measures.

As never before, we need a close bonding of government and industry as partners in this economic battleground. There can be little doubt that the success of many of the countries which have become major competitors with the United States is because they have enjoyed a more mutually supportive linkage between government and industry than we have achieved to date. In recent years we have made substantial progress but much remains to be done. It is suggested that we begin by discarding the ones and zeros in our approach to problem solving and content ourselves with "tentatives" of many grays while the widest possible options are being explored.

Ms. Dyl, corporate security manager at Bolt Beranek and Newman Inc., has been with BBN for nine years and is currently responsible for managing government security programs for BBN and its subsidiaries. Prior to joining BBN, Ms. Dyl was a security specialist with the Defense Investigative Service where she served as the New England Region education and training specialist and as an industrial security representative. She is also an active member of the National Classification Management Society, having served on its board of directors from 1987 to 1990 and is presently the chapter chairperson for the Northeastern Region of NCMS.

Security Awareness Through TQM

by Catherine A. Dyl

Security awareness programs will have to undergo dramatic changes in the 1990s to achieve success. During the 1990 NCMS National Seminar, Jim Bagley pointed out that "*perestroika* means restructuring. There must be a restructuring in our thinking."¹ FSOs must experience a *perestroika* in their management style if they are to establish an effective security awareness program. They must become better managers in the 1990s to achieve their goals during tough economic times.

At BBN, we look towards TQM (total quality management) as our guide to management. TQM is a management approach dedicated to continuously improving product or service quality through the application of quantitative methods and human resources. A security awareness program like any other facet of operations must be properly managed. One of the basic principles to TQM is that if you build in quality, you will reduce costs because it's cheaper to build in quality than inspect out defects. Therefore, the more effective a security awareness program, the less time we must devote to self-inspections and correcting deficiencies. It's cheaper to take the time to prevent deficiencies than it is to correct them once they've occurred. In terms of our ultimate goal—protection of classified information—it makes sense that preventing deficiencies will result in goal achievement.

Application of TQM principles

W.E. Deming developed an approach to TQM known as PDCA or Plan-Do-Check-Act. During the plan phase we "state our organizational goal and identify significant process variables that affect achievement of our goal."² I think everyone agrees that our goal is to protect classified information. The issue then becomes, how do we protect classified information using existing (or diminishing) resources?

Planning Phase

The tendency during strained economic times is to reduce those security practices that aren't required by federal regulations. Cutting the security awareness program is one such practice resulting from this tunnel vision. Both government and industry are guilty of doing this. While both preach the importance of a security awareness program, we see industry reducing their security education budgets and the government reducing the number of courses taught or diluting the role of education and training specialists.

Inevitably the first to go with any budget cut is the security awareness *program*. I emphasize the word *program* because the ISM and similar regulations only require the execution of a Nondisclosure Agreement, a counterintelligence briefing, and assortment of specialty briefings. These briefings do not constitute a program. I do not advocate federal regulation of a security awareness program because such micro-management is counter-productive. However, I do urge security professionals to recognize the importance of security awareness. Security professionals must recognize the fact that compliance with federal regulations designed to protect classified information is the natural result of an effective security awareness program that motivates employees to work towards that goal.

A security awareness program must be a systematic program designed to achieve certain goals. The program should be a plan that includes orientations, recurring security education, and debriefing. Security awareness programs should use different media of communication to convey your message, ranging from newsletters and graphic posters to video. Don't forget that some of the best security briefings are conducted one-on-one.

Summarizing our planning phase, our goal is to protect classified information, and a significant variable that will help us achieve this goal is security awareness. An effective security awareness program must be established as a methodical program that will protect classified information.

The "Do" Phase

The second phase of Deming's TQM technique is the "Do" phase. In this phase we develop data to carry out the change that will improve program quality. We must identify those significant occurrences that create quality in security awareness. Security awareness programs will vary in specifics but will share certain characteristics.

Needs Assessment

For example, a security awareness program must start with a needs assessment. Security should get the technical staff involved to assess their

needs and develop workable procedures so that a viable security awareness program can be established. A security awareness program must have specific goals as determined by a needs assessment.

At BBN, many of our security awareness briefings and materials began with input from the technical staff and audit team. Both security and a representative from the targeted audience work together to determine what is needed and develop an appropriate briefing or guide aimed at job categories, programs, or various topics of interest.

Communications and Motivation

Communications and motivation are two other important facets of all security awareness programs. The purpose of security awareness programs is to inform people of the requirements and motivate them to comply. The technical and administrative support staffs must understand what they have to protect and be convinced that they should protect it. The security staff is responsible for communicating these ideas to others. Communications and motivation is an entire field unto itself; therefore, I will not dwell upon it except to say that security educators must know how to communicate. Before we can train non-security staffers on their responsibilities, we must ensure that the security educators and both government and industry auditors know how to communicate. Technical security knowledge, *i.e.*, knowing the ISM inside and outside, is only one part of security. Security educators must also know how to get others to follow the security regulations and work with the security staff in a cooperative spirit.

Teamwork

Teamwork is another important facet of developing a security awareness program. TQM teaching shows that we can do more with less through teamwork. Creating teamwork by building constructive working relationships with our customers is essential in using TQM. The ISM makes security an individual responsibility. We often use that passage in the ISM when assessing culpability for a violation. On a daily basis just how much of the security responsibilities are shared by all employees? Security must get cooperation from all employees to succeed.

With decreased resources in the 1990s, I envision a shifting of responsibilities away from the security staff and onto the technical and support staffs. You can be sure that when a company cuts overhead expenses to become more competitive in the marketplace, security budgets will be affected. At BBN, we've asked the technical staff to participate in security self-inspections. Container custodians must inventory their classified holdings and justify the need to retain them. During the next budget-cutting rounds, the system security officers will become responsible for weekly AIS inspections.

This doesn't mean that the security staff needn't perform a self-inspection. It just means that the other employees participate and become part of the security team. The security department is quick to point out that security can cut overhead costs if the technical staff helps. Security must truly become an individual responsibility and compliance become a way of thinking as budgets are trimmed.

Dee Dee Collins states on the subject that, "The security manager's job is easier when other employees, especially those outside of security, understand the program—its purpose, who it serves, and how."³ Remember that TQM involves quality improvements through the application of quantitative methods and human resources. Today's security professional must know how to use the most important of all resources—people. Involve others when developing a security awareness program. Sometimes the technical staff and top management can do a better job of selling security than the security staff because of their positions of influence and respect with their peers. At BBN, security briefings are often given jointly by a security person and an engineer. The engineer will discuss the technological aspect of a program and both will review the program's security implications.

Defining The Threat

Another step that can't be overlooked when creating a well-rounded security awareness program is to determine the threat. While some people will obey rules for the sake of obeying rules, many others will obey the rules only if there is sufficient reason to do so. Therefore, it is our job to inform people as to why they should protect classified information. We can appeal to their sense of patriotism by explaining the threat.

But what exactly is the threat today? In the past the U.S. defense industry's number one enemy was the Soviet Union and Eastern European puppets. *Perestroika* and *glasnost* have since changed our perceptions of who the enemy is. Security professionals are now in a position where they must redefine the threat. Much of our security education in the past described the hostile intelligence threat. But security awareness materials can't constantly regurgitate the same hostile intelligence information because the threat is not the same. Security awareness materials must be current to be effective. Now the question is who are the hostile intelligence services and how do they threaten the United States. Security educators in the 1990s will have to answer these questions to develop a security awareness program.

The fact that the budgets of the GRU and KGB have increased in recent years shows that intelligence gathering has not diminished during *perestroika*. Also, the recent defection of East German spies to the Soviet Union shows that some Eastern European spies are more devoted to Communism than their country. It's important for security professionals in both

government and industry to work together on sharing information regarding the new threat. Educational programs will have to be changed accordingly. Perceptions about the lessening Communist threat resulting from *perestroika* must be brought into alignment with the reality of today's threat.

Security professionals need current threat information from the government. Thus far, the only current information I've received is a reminder from the FBI that the threat still exists. It is imperative that the government do more to help industry define, communicate, and give examples of today's threat. However, it is also incumbent upon the security professional to remain aware of current events by reading news articles.

Security awareness materials must be kept current. The key is to know your audience and understand what their needs are to avoid boring, irrelevant or redundant information. Customized up-to-date materials are needed to deal with today's security complexities.

Security's goal has always been the same—to protect classified information. We've determined that a security awareness program must be based on actual threat, requires communication and motivational skills, and needs teamwork. But the 1990s will present a major obstacle in doing this; namely, money. How do we develop an effective security awareness program when security organizations are having their budgets slashed?

Management Support

One way of bridging the gap between an effective security awareness program and dwindling resources is to get management support. Management support is essential to the use of TQM principles. Security has to enlist the aid of those executives who have the greatest amount of influence on others because TQM must be implemented from the top and flow downward. Executive management must communicate and demonstrate the importance of complying with government security regulations and having an excellent security program. Furthermore, an environment in which people can grow and contribute to the national defense must be promoted by the executives. Behavior aimed at that purpose must be recognized and rewarded. Top management must lead the way to increase communications, promote teamwork, and establish a climate of cooperation.

In continuing to improve quality during the "Do" phase, we must turn our attention to another basic principle of TQM which is customer commitment. Who is the customer and what are that customer's needs? In terms of a government security program in industry, I've always believed that we have two customers. We must satisfy the government by complying with regulations, and we must assist our employees in protecting classified information.

Government and industry must cooperate and discuss objectives to achieve their goals using available resources.

There have been great strides made by both government and industry during recent years to achieve this. However, there is more work to be done. A bureaucratic system bloated with unnecessary regulations defeats efficient and honest businesses. We must determine which processes are important to our mission's success. Do we focus on security awareness programs or do we spend money on new and improved (and more expensive) containers and locking mechanisms? Furthermore, industry must continue to give support to its security program. Perhaps a joint TQM plan can be developed to improve program quality so we can determine which variables result in better security. Only through a joint effort can we reduce costs, improve program quality, and still realize our goals.

The "Check" Phase

Getting back to Deming's model of implementing TQM, we must now examine the "C" or check phase. During the check phase we observe the effects of change. Most importantly, we have to quantitatively measure the effectiveness of our security awareness program. An objective method of measurement is critical in determining the effectiveness of a security awareness program. Therefore, we must determine how to measure and evaluate our security awareness program.

"Evaluation should be based on predetermined criteria and a feedback process."⁴ The criteria used to evaluate a program should be developed by the group that developed the program's objectives to make evaluations consistent. For example, a company may decide that it needs to improve computer security because there have been an increasing number of deficiencies in that area and because the technical staff doesn't feel comfortable with their understanding of computer security practices. Therefore, the security and technical staff would develop a course and evaluation method to teach employees the rules and regulations for classified computer processing.

B. W. Tuckman identified "three primary stages of education evaluation."⁵ The first is to determine the extent to which the information provided in the course was learned. This can be done using a test or assessment instrument. Donald Kirkpatrick, in compiling material for the American Society for Training and Development, broke down this first stage into two categories. The first category pertains to student reaction since "the more favorable the reaction, the more likely one will learn."⁶ Applying Kirkpatrick's method, an evaluation to test reaction might look like this:

What did you like best about this briefing?

What did you like least about this briefing?

Comments or suggestions

The second category that Kirkpatrick uses is the "learn" phase. In the learning phase we want to measure the change in skills, knowledge and attitude that have occurred because of this course. As with the use of any statistical method, it's important to apply your measurement before and after a course of instruction. Written tests are particularly useful for security briefings since facts, rather than techniques, are being taught. Also, the use of a control group is useful for comparison purposes. A control group could consist of employees who haven't taken the computer security course but are scheduled to take it. Here's a sample evaluation:

The second stage of Tuckman's method involves "determining if, and to what degree, the information has been appropriately applied at the work place. This type of evaluation is usually conducted one to three months after completion of the training."⁷ Kirkpatrick writes that there's a difference between knowing the principles and using them. Therefore, we must measure on-the-job behavior changes resulting from the course. This should be measured by the student's superiors and subordinates, as well as the student himself, before and after taking the course. Also, use a control group for comparison.

The evaluation should ask what changes have occurred and who is responsible for the changes. Specifically ask the respondents what they think is more effectively done and what they think is less effectively done.

The final stage in the Tuckman or Kirkpatrick method of evaluating training is of great value during the final or "Act" phase of the Deming model of TQM as discussed in section 12.

The third stage of the Tuckman model involves measuring the effect on the organization, and is "usually conducted six months to one year after training and thereafter on an intermittent basis."⁸ This "results"-oriented stage of evaluation measures compliance or number of deficiencies before and after the course. The specific method of measurement can be internal audits and government inspections. However, Kirkpatrick warns that the method of measurement must carefully examine other variables that affect results. For

example, has there been a change in staffing, workloads, regulations, amount of classified computer processing, *etc.*?

A security awareness program is then modified based on the results of the evaluation. TQM is based on continual improvement to prevent flaws. Therefore, we constantly measure the effects to process change, and we modify accordingly to improve overall quality.

The "Act" Phase

The final phase of the Deming model is the "A" or Act phase. In this phase we continue to assess the effects of our change to determine if and why our security awareness program improved. By doing this we can somewhat standardize our methods for implementing our security awareness program and evaluations processes. However, it is important to note that this degree of standardization does not imply that the program is stagnant. In fact, TQM requires constant improvements.

Security Awareness at BBN

The following is a general outline of BBN's security awareness program for this fiscal year using the TQM approach to form a program plan.

I. Goal

Protect classified information through an improving security awareness program.

II. Needs Assessment

A. Convince employees that the threat still exists so they will be motivated to continue compliance. This need was identified in response to many questions from the technical staff regarding the German reunification and effects to *perestroika* on security.

B. Educate the staff on the use of secure telecommunications. The rapid increase in this area has created an education gap as demonstrated by deficiencies in a recent government inspection. Also, the use of secure communications is relatively new to most BBN employees.

C. Reduce violations by improving employee understanding of classification guidelines. BBN has acquired contracts with different user agencies in technical areas that are state-of-the-art. Therefore, there is little classification experience with the information developed under these new contracts. As a result there have been many classification is-

sues. Target program managers with new programs to discuss security issues and jointly prepare presentations.

III. Plan

A. Orientation

1. Discuss security basics and individual responsibilities
2. Adjust hostile intelligence threat briefing to accurately describe today's threat
3. Determine employees' job category to gear briefing towards their needs
4. Discuss telecommunications capabilities, threat and security practices.
5. Hand-outs: SPP, BBN Basic Security Guide, Counterintelligence Briefing, Espionage Laws

B. Recurring

1. Presentations: Survey department managers to determine their needs (largely departments with classification problems). Resources allow for one program presentation each month.
2. Posters: Change posters quarterly and use posters that remind employees of the continuing threat
3. Newsletters: Quarterly newsletters to describe today's hostile intelligence threat, identify problems discovered in internal audits, describe regulations changes, announce kudos for helping security, inform of government inspection results

B. Miscellaneous

Update SPP in 1991 to reflect new ISM changes. Have the CEO prepare the foreword.

C. Evaluation

Conduct evaluations after every presentation, newsletter, *etc.* Conduct overall evaluations every six months to determine overall security awareness program effectiveness.

D. Revise security awareness program appropriately

Again, this is just a general outline of BBN's security awareness program. Yours may look very different, but hopefully all security awareness programs will have at least one thing in common—management planning. TQM is only one method of management. The key is that a security awareness program must have a plan of action with stated goals and a method of evaluation to monitor effectiveness. The program must be dynamic so as to constantly change according to the evaluations so that the program will be continually improving. As the security awareness program improves, you will see that resources will be used more effectively. Deming writes that the more quality you build into a system, the less it costs.

Summary

TQM as applied to government security in the 1990s can be summarized as follows. Security's goal is to protect classified information with existing resources. To achieve that goal we must have an effective security awareness program. Effectiveness of the security awareness program is measured, thereby creating revision to sustain continual improvement.

This week's seminar is a great start for security professionals to learn marketing, teaching, and management skills that can be applied to security awareness programs. While the specifics of any security awareness program will vary to meet organizational cultures, the techniques learned this week will prove useful. In the difficult economic time ahead, security professionals must employ better management techniques and planning to maintain a good security program by striving to improve the quality of their security awareness program.

Footnotes

1. Bagley, J. (1990). *Perestroika - Technology Transfer - Reality*, NCMS Bulletin, Volume XXIV No. 4 July - August 1990.
2. Moen, R.D., & Nolan, T.W. (September 1987). Process improvement: A step-by-step approach to analyzing and improving a process. *Quality Progress*, 20(9), 62-68A quoted in A. Houston and S.L. Dockstader. (1988) *A Total Quality Management Process Improvement Model*, Navy Personnel Research and Development Center, San Diego, CA.
3. Collins, D.R. (1988). *Motivation and Management*, Lecture given at the NCMS National Seminar, Redondo Beach, CA, July 1989.
4. Department of Defense (P & L)(1989). *Total Quality Management, An Education and Training Strategy for Total Quality Management in the Department of Defense*. Washington, DC
5. Tuckman, B.W. (1979). *Evaluating Instructional Programs*, Boston, MA: Allyn and Baron, 16, quoted in Department of Defense (1989). *Total Quality Management. An Education and Training Strategy for Total Quality Management in the DoD*, Washington, DC
6. Kirkpatrick, D.L. (1985), *Evaluating Training Programs*, Journal of the American Society for Training and Development.
7. Kirkpatrick, D.L. (1985), *Evaluating Training Programs*, Journal of the American Society for Training and Development.
8. Kirkpatrick, D.L. (1985), *Evaluating Training Programs*, Journal of the American Society for Training and Development.

The Executive View and Implications for Practice

Executive View

James A. Abrahamson, Executive Vice-President, Corporate Development,
Hughes Aircraft Company

James E. Freeze, President, The Freeze Corporation

Implications

Harry A. Volz, Director of Security & Transportation, Grumman Corporation

William B. Bader, Senior Vice-President, Policy Group, SRI International

Maynard C. Anderson, Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

Mr. Abrahamson is executive vice-president for corporate development of Hughes Aircraft Company. Mr. Abrahamson retired with the rank of lieutenant general after 33 years of active duty with the Air Force. He is widely recognized as a leader in several national military and space programs, most notably as Director of the Strategic Defense Initiative Office of the Secretary of Defense.

Security Awareness: A View From the Top

A Corporate Perspective

by James A. Abrahamson

Introduction

I am grateful and pleased to join you in this symposium and to have the opportunity to address you on a topic of such importance.

Having had a fair amount of experience with military and technology security matters over the years has made one thing very clear to me: A defense industry company doing business globally must have in place extremely strong security arrangements to protect its critical technologies from foreign espionage activities.

Today I want to focus just on two key elements of such arrangements—a program aimed at making all employees fully aware of the foreign espionage threat and development of a program designed to monitor, on a continuous basis, employee preparedness to meet the threat. Let me begin with employee awareness.

The Employee Awareness Program

Despite the warming of relations with the Eastern Bloc, U.S. defense industry companies operating in today's global business environment continue to face a very serious threat of foreign espionage. For one thing, shrinking defense budgets have resulted in such ferocious competition that we can expect a growing number of our competitors to reply on their means of making sure our business leaders fully understand the security risks confronting their organizations.

The greatest of such risks are posed, of course, not only by friendly nation competitors, but by our traditional adversaries. Because of the shrinking defense budgets and intensifying competition that I mentioned earlier, U.S. defense contractors are undertaking a global search for new markets both

military and commercial. Further, because of the dramatic and ongoing shifts in Cold War relationships, U.S. companies will have a growing number of dealings or involvements in markets that have previously been off limits. And these ventures will very likely increase our vulnerability to covert activities of the nations that are still unfriendly to us.

Many of these unfriendly nations large and small are capable of mounting effective espionage operations whenever they commit themselves to pursuing our critical defense technologies, or even our military hardware. For example, our embargo against Iran failed to keep that nation from acquiring replacement parts for the U.S.-built aircraft Iran was using in the war against Iraq. Iran got vital parts by developing an agent network that included coopting members of the military.

As threats of such espionage multiply in the new global operating environment, our defense industry will more and more find it a balancing act to sell products without giving away secrets. We will need to make our people wholly alert to the dangers that characterize this new environment—so they'll be able to protect technologies that are critical not only to military security and defense industry readiness, but also to our nation's competitive position in the global marketplace. Such technologies are nothing less than the foundation of our nation's power among other nations—for today a country's position in technology is as much a gauge of its comparative strength as territorial holdings were in former times.

To help protect our critical technologies at Hughes Aircraft Company, we have set up an innovative foreign counterintelligence awareness program.

Our program reflects a change in attitude toward the business of security. Locks and guards (no matter how sophisticated and well-trained) cannot guarantee the security of the hundreds of thousands of classified documents that must be protected every day. Today's spies are powerfully motivated—by money, revenge, perhaps a desire for recognition—and they are skilled in their craft as well. There is no system of physical security that cannot be evaded or penetrated by one of these spies at some time.

So today, security has taken on a new dimension. Our task begins long before we must catch spies. It begins at stopping people from becoming spies. To move toward "complete security" we need more than state-of-the-art hardware. We also need "software"—the informed awareness of our employees.

At Hughes we reach out to heighten employee awareness of foreign intelligence activities and to offer help before it's too late. We've developed a unique, multi-phased program designed to show employees that the threat posed

by foreign intelligence services is real—and that it endangers everyone in the defense engineering community.

We invite intelligence and law enforcement experts to Hughes to brief employees on foreign counterintelligence issues. These experts provide critical information about procedures that protect employees, their co-workers and defense-related technologies from foreign intelligence activities. Our goal is to create a work force that is not only aware of the danger, but knows how to deal with it.



Roger Denk, GEN Abrahamson, ADM West, and GEN Freeze

Our program also aims at giving employees clear and graphic descriptions of the consequences of espionage. These are not new-found wealth and excitement. Rather, they are fear, despair and prison. Using a variety of communications resources, we are generating a flow of security-related information in the work place—and we are also boosting the priority of security matters in the consciousness of our employees.

Finally, we supplement our awareness effort with confidential employee assistance programs. These programs that supply counseling about family matters, financial management, and alcohol and drug abuse situations can help employees solve a problem before they become vulnerable to recruitment by a foreign agent.

help employees solve a problem before they become vulnerable to recruitment by a foreign agent.

The greatest guarantee of our security is our employees. The Hughes foreign counterintelligence awareness program is dedicated to helping employees protect themselves, their company, and the technology upon which the free world depends.

I'm convinced, then, that U.S. defense industry companies must have employee awareness programs. However, given the serious and accelerating threat posed by foreign intelligence operations, I'm also convinced that the United States needs an overarching *national* awareness program.

We need a single central government program charged with overseeing and ensuring the general uniformity of awareness efforts of defense contractors and government organizations. This program should have responsibility for such activities as establishing guidelines for awareness programs, supplying educational materials and procedures for implementation, and providing current assessments of various security environments and threats.

While a high-quality, effective awareness program is a crucial element of the security arrangements needed by U.S. defense contractors, I suggest another crucial element is development of a program for monitoring the security reliability of employees on a continuing basis. Such a Continuing Assessment Program, or CAP, is the second subject I want to talk about today.

The Continuing Assessment Program

As you know personnel security procedures established over the past 30 years center on a clearance—a certification at a point in time that a person can be allowed access to classified materials or functions. Such clearances are granted, rescinded or denied on the basis of the loyalty, character, associations and reputation of an employee.

In the case of the CAP, these evaluations would be conducted not just periodically, but on a continuing basis. The CAP would achieve continuing assessment by making periodic evaluations the responsibility of first line supervisors who have day-to-day contact with cleared employees under their direction. These supervisors are in the best position to observe actions and attributes of employees that may point to a potential security breakdown. As history shows, these actions and attributes include everything from drug dependency and sexual misconduct to an obsession like an excessive need for recognition, status or adventure.

What about the current state of continuing assessment programs in defense industry companies? Such programs are, in their general outlines at

least, required of defense industry contractors by DOD. My message today is that contractors *should* consider developing specific procedures for implementing this concept.

Let's look more closely at the concept of continuing assessment. Why does assessment need to be continuous? You certainly can't rely just on an initial clearance evaluation when you're concerned about someone's suitability to protect classified data. Even after government agencies spend great amounts of time and money on investigations, they still grant clearance status to 99 percent of applicants. The problem with trusting solely to these initial evaluations, of course, is that situations and people change over time, so that past behavior is no indicator of future loyalty.

Expanding the strategy to include periodic reinvestigations is clearly an improvement because this enables us to detect adverse changes that have emerged since the last investigation; however, if such reinvestigations are infrequent, extensive compromises may still occur.

In fact, according to a security research report by the Rand Corporation, even *regular* periodic reinvestigations can't do a reliable job of identifying high risk employees. The only satisfactory security strategy, says Rand, is *continuous* monitoring of employee job performance and personal behavior.

Reporting adverse information is the first line of defense in preventing espionage activity. According to the *Industrial Security Manual*, a contractor must report all information suggesting that the conduct or character of a cleared employee "may not be clearly consistent with the national interest." This includes information about: criminal activities; bizarre or notoriously disgraceful conduct; treatment for mental or emotional disorders; excessive use of intoxicants; use of illegal, controlled substances such as marijuana, heroin, cocaine and hashish; and excessive indebtedness or recurring financial difficulties. Only information that has been confirmed by the contractor as fact should be reported formally by the facility security officer.

The responsibility for acting upon adverse information rests on and extends beyond managers and supervisors. Continuing assessment programs, if instituted, must ensure close coordination among managers, security officials and the personnel, medical and legal staffs of the organization to guarantee that all pertinent information is considered in the security program.

In addition, management must develop programs aimed at counseling and otherwise assisting employees in security-sensitive positions who are having personal difficulties—for instance, emotional, medical, or financial problems. Employee assistance is a critical element in effective continuing assessment

programs. It can minimize negativism by emphasizing the fixing of problems rather than ferreting out and reporting of problems.

Employee assistance efforts can solve what might be called the needle-in-the-haystack problem. It's virtually impossible to tell which of your employees with personal problems will someday become involved in espionage because personal problems of potential spies look like personal problems of anybody else. You don't have to identify this needle in the haystack to deal with it, if your company has an assistance program aimed at all employees with personal problems. The assistance program offers each employee opportunities to get support and assistance from supervisors and counselors before problems become desperate, unsharable and conducive to illegal behavior like espionage.

Further, having a good assistance program can make it easier to report adverse information when required. Suppose a problem employee has been given every opportunity to straighten things out, but he or she fails to do so, the reporting of adverse information or disciplinary action follow. An assistance program can be a litmus for distinguishing employees who are willing and able to handle their problems responsibly from those employees who are not.

Another step to consider is to integrate security assessment criteria into the annual performance appraisal process that is already in place in companies. Managers and supervisors could then measure an employee's reliability to security matters using the same type of evaluation procedures that are now used to measure job performance. The effort would be to obtain a dynamic profile of the employee's security reliability over time.

Conclusion

In designing and implementing a Continuing Assessment Program, we must not overlook the fact that such a program is already in place. Foreign intelligence services are actively and continually assessing our employees for suitability and reliability to handle the transfer of needed information. Failure to use the program already in place can only lead to future security disasters. Our most important weapons against espionage are awareness and continuing assessment program.

General Freeze is president of The Freeze Corporation which provides management, intelligence and electronic warfare threat analysis, and offers security-related services to both government and corporate clients. Prior to assuming his present position, he served 32 years in the United States Army.

A View From The Top

by Major General James E. Freeze
United States Army, Retired

My colleagues and I have been asked to address the role and importance of security awareness to broader corporate objectives and discuss our views related to the most promising strategies for achieving security awareness. Having accepted that mission and performed a simplified mission analysis, I have chosen to pursue the matter in two phases exactly as it is stated.

First I want to talk to you about my view of the relationship, or role and importance, of security awareness to broader corporate objectives. Then I'll provide you my thoughts on how to establish and *maintain* a high level of security awareness in an organization.

Role And Importance To Broader Corporate Objectives

With reference to the relationship of security awareness to broader corporate objectives, I think it's essential that we have a common understanding of the term *broader corporate objectives*. For our purposes today, I submit that common understanding can be capsulized by the term P2. In this instance, P2 breaks to perpetuation and profit—the perpetuation of the firm and the profit motive. Are not those truly the ultimate broad objectives of any corporate entity? Many years ago one of this nation's corporate leaders stated: "The purpose of business is business." Read that as perpetuation of the firm.

Profit, our second P in P2, is certainly a commonly accepted corporate objective in our society. And the two P's support one another. Without profit, there is low to no probability of perpetuation of the firm; and without perpetuation of the firm, there surely will be no profit.

So accept my thesis, for purposes of this presentation at least, that the term *broader corporate objectives* means perpetuation of the firm and making a reasonable profit. In fact, we can say that profit is prime since few firms continue to operate—or perpetuate—very long when losing money.

That being the case, we can ask ourselves how do you make a profit? And we respond with answers like, "provide a good product or service at

reasonable price and optimize volume sales." Or we say, "obtain an advantage over your competitors." Now in either case, there are elements of information related to our success which are of value to the firm. If we provide that good product or service at a reasonable price, we must have a strategy. We may choose to make a better product or do a better job than the competition. We may have a method for reducing our cost of production or cost of providing the service. Or we may choose to reduce our incremental profit. Now, whichever strategy we might choose is an element of information we should keep from our competitors because it provides us an advantage. We need that advantage to make the profit to perpetuate the firm, to achieve our broad corporate objectives. *Security awareness* is an essential factor in keeping our strategy from our competitors.

"Oh," you say, "he worked hard to get there."—Well, now I want to bring it to where most of you live: DoD and the defense industry. I'm preaching to the choir when I tell those of you in DoD that security awareness is essential to U.S. national interests. If you don't know and accept that as fact, shame on you. History is replete with examples of how this nation has been ripped off by friend and foe alike simply because of inadequate security awareness. And I assure you, my friends, *perestroika*, the demise of Communist regimes in eastern Europe, and all this talk about this euphemistic something called a "new world order" does not mean the end of—or even a reduction in—intelligence collection against the United States. In point of fact, I fully expect greater intelligence collection efforts against us. The targets may change to some degree, but I believe the level of effort may well increase with broadened opportunities for collection.

And what does that diatribe have to do with the importance of security awareness to those broader corporate objectives of perpetuation and profit? Simply this: Firms that leak like sieves are going to find that their profits dry up.

In some instances, the information we want to protect may not be national security-related. It could be proprietary in nature. It could involve new product development, a new style line, a modification to an existing product line. Any of those could provide an advantage over the competition and conceivably increase profits. And, of course, there is the ultimate proprietary secret—the proposal. Corporations do not spend tens or hundreds of thousands of dollars developing a proposal only to have its technical and cost data obtained by a competitor. Acquisition of such data by a competitor certainly is antithetical to broad corporate objectives. Security awareness can and does play a vital role in precluding that acquisition.

And that is my bottom line. *Security awareness is of vital importance to those broader corporate objectives of perpetuation of the firm and profitability. It truly provides value added.*

Strategies For Achieving Security Awareness

So how do we achieve security awareness? Well, I assure you it doesn't simply fall on us from the sky. We achieve it through a studied, structured and disciplined approach involving the tireless pursuit of innovative and imaginative actions. We achieve it by convincing the work force of its value to them as individuals, to the firm, and, if applicable, to the nation. We achieve it with and through the support of senior management.

Early on in developing our studied, structured and disciplined approach—our plan, if you will—we must decide and dedicate ourselves to the proposition that our security awareness program is not going to be a *paper tiger*—not just something to get us by the next checklist-type inspection. We need to determine that it's going to be more than an initial job entry security briefing and annual security lectures supplemented by a poster here and there mentioning security awareness. If we're not prepared for total immersion, then our security awareness program is destined to simply be that paper tiger.

And senior management has to sign up for the concept of total immersion. It's going to cost a little money—not a lot—but some. It's going to require a few personnel spaces and a budget for procuring training aids, educational materials, white propaganda, and for inviting guest speakers on occasion. It's going to require diversion of some time—not much, but some time—of the members of the work force from their normal line and staff functions to attend and/or participate in security awareness education, training, and possible planning and publicity activities. And senior management must accept, sign up to, and personally support that diversion of resources and the total program.

Further, senior management must be prepared to be personally involved in the program. Senior managers must be seen and heard by the work force espousing their understanding of, and support for, the security awareness program. In fact, senior managers should play a major part in explaining to the work force the importance of security awareness and the relationship of security awareness to employee job security.

In addition to formal *pitches* to the work force on the subject, senior managers should optimize opportunities for E-T-E (that's a Freezonian acronym for eyeball-to-eyeball) contact with employees. They should visit them at their work place; chat with them in the cafeteria; meet them at the door in the morning; or even wander through the parking lot as they are coming and going. During these E-T-E opportunities, the senior manager should include security awareness as a discussion topic. He or she should demonstrate an understanding of security awareness and of the need for the

program, and should enlist comments and suggestions from the employees related to its conduct and possible improvement.

And what of the work force *per se*? It is those men and women who will ultimately reflect the success or failure of the program because they are the product of the program. Dedication, money, management support, and machines comprise the program, but the people in the work force ultimately "make it happen." They must be convinced of the need for, and value of, security awareness. They must understand the threat and their role in countering that threat. And they must be sold the program in a class fashion. Sloppy briefings by slovenly briefers, using esoteric examples, do not sell a program. We want a class act to sell a class program. Many of the federal agencies are prepared to provide speakers to assist you. There are superb training videos available. Ensure that education and training materials are relatively current. You can really turn off a group by showing an 8- or 10-year-old film.

We want to involve the work force in program planning. Establish a Security Awareness Working Group. Assign them such tasks as recommending themes for the program; conducting small security awareness seminars in their respective departments or functional areas; planning and carrying on a facility Security Awareness Day or Week, with displays, special speakers, maybe a special meal in the cafeteria, or even a catered picnic—the tireless pursuit of innovative and imaginative actions.

So there you have it, my friends—my strategy for achieving security awareness. It's people-oriented, because people make it happen. The strategy involves studied, structured and disciplined planning, and implementation of that planning; it requires the support and participation of top-level management; and it is focused on involvement of the work force in planning and execution of the program, in recognition of the fact that the members of that work force are the product of the program. *They make it happen.*

Mr. Volz is the Director, Security and Transportation, Corporate Services Division, of the Grumman Corporation. He joined Grumman in 1955 and transferred to the Director of Security's staff in 1958. He has served Grumman in a variety of increasingly responsible positions. He has also been recognized many times for his outstanding work with the Boy Scouts of America and other community service.

Implications: The National Industrial Security Program

by Harry A. Volz

The title of this symposium is "Security Awareness: The Challenge of the 1990s." So far we've had lectures on approach, and attitudes, appeals, methods, traditions, professionalism, the TQM. What I want to talk about is not any of those things, but what will be an important item of content, an element of the curriculum of the '90s, the NISP. You opened the door for me, so now I get a chance to talk a little bit about something I have talked about a great deal lately.

You gave us enough evidence in your presentations and discussions. There is a *need* to discuss the NISP, for instance, with questions and comments like these: We *need* to do better than we have been doing. We *need* to avoid those things that are out-of-date. We *need* to take another look at special access programs. We *need* to recognize the impact from the changes in the Warsaw Pact. We *need* to protect information of value. There is a *proliferation of requirements*. Do we *do it right*? These are questions in your minds. We *need* to talk about sensitive, but unclassified information, about TQM. We *need* to reduce the number of documents. We *need* to examine the public perception and opinion about our current programs. We *need* to know where the threat is. We *need* to evaluate the difference between centralization and decentralization. What are *minimum standards*? Is there a *system for delivery*. One of you remarked that there is a need for a **National Industrial Security Policy**. Note the acronym! We have to be aware of technical terrorism. Perhaps we should look at the real threat that we call TEMPEST. If we are able to deal with all of the above, and more, we will have the NISP.

What's the NISP?—the National Industrial Security Program? People have been saying it in the last few days, as if one needs only to say it and all problems go away. It is like a magic word written on a rock by the roadside. But the NISP is still only a concept. We have spent almost three years selling a concept—a good concept. Industry and government, both working together all those years. As a result, President Bush asked the government

people involved in his NSR, "Is the NISP feasible?" The answer came back, "Yes, it is and it is desirable," and he said, "*Do it*, with industry." Now it must be done. But what is it that we are going to do? Somebody asked last night or at least said last night, "Are we sure about constant commitment? And, what is the program?"

The NISP, in simple words, is a program that will improve and enhance the protection of significant technology and classified information. Recall that somebody asked, "What about unclassified, but sensitive?" It is threat-driven, which means we have to know the threat. It has baseline uniform standards; it is applicable to all participants, consistently; it is cost effective; and it is co-developed and maintained. It is a partnership, something we used to smile at and, now, we are serious about. The NISP has been marketed and sold as a concept to people like Bob Atwood, Reggie Bartholomew from State, John Betti, Steve Garfinkel, Bob Howard from OMB, whose representatives stated that if the NISP occurs and survives, while they don't classify information and don't put down the security rules, they will make participation in the NISP a requirement for funding. The list includes Dave Kitchen from the NSC, Ed McCallun from Energy, Tom Murrin from Commerce, Don Pilling from NSC, Nick Rostow, Judge Sessions, Admiral Truly and anybody else who would listen in the hallways.

Does it have support from industry? We have had management endorsements from Aero-jet General, Aerospace, the Harris Corporation, Grumman, AT&T, General Electric, Teldyne. Run through the directory for the aerospace industry and you will find endorsers.

The program is to meet both current and emerging threats. We have just heard the kind of threats that are coming. That's the kind of thing that the NISP will meet. What are some of the elements of NISP that relate to things that were addressed during the discussion sessions this week? Under information security, there are task forces being formed about classified material control, classification management, AIS, communications security, system security engineering, and the protection of independent research and development information. Under personnel security—background investigations—a single scope BI, personnel reliability, classified visits. All elements that we now find in existing programs, plus technology transfer and treaty implications, are all part of the NISP. That is why Maynard frequently responded when someone asked a question with, "You have the NISP." And you will have the NISP! The task forces have a big job before them. The goals that have been established by the President indicate that Maynard must have a progress report by the first of September. That might not be easy to do. All of those boxes on all those charts that we have (some that pertain to industry and some to government) will need to be blended, all need to be filled, all need to be accomplished, in some kind of meaningful fashion by the first of

September. The *whole* program cannot possibly be developed by then. But some kind of meaningful development must occur between now and then.

One thing we expect to do during that period is conduct a regulatory review. We have looked at how many regulations there are. There are more than 600 regulations that need to be looked at. We need to see which can be changed, which can be blended, which can be superseded so that we have a single set of rules when we have finished. We need to accomplish uniform policy development as well as something that OMB jumped on when we talked about it; some kind of a system by which we can identify costs. When the facts receive wider distribution, you are going to see a number for 1989 of expenditures at an estimated 13.8 billion dollars. For industrial security that is a lot of money. Suppose only 20 percent of it could be recovered and used more wisely. For instance, suppose we add it to the budget that has to do with training—things we've been talking about the past couple of days. This doesn't mean that we have ever said that we were going to save a great deal of money. What we have said was that we were going to avoid unnecessary costs and use the money more wisely, elsewhere.

There will be baseline standards for the NISP. In addition, we have proposed layering, so that there are separate levels, if you will, for areas like SAPS, energy-related items and for SCI. That does not mean that we can make the same mistakes we made with the FAR (Federal Acquisition Regulations) where we left room for implementing instructions. We expect the same kind of goals or standards across each of the layers, so no matter which facilities are in operation, we will be able to recognize the program as a single program. All of these elements will be part of the NISP. When we are finished, there will not be a thousand separate programs as there are now.

The response that came back from the President's request for an NSR states that the development of a single, coherent and integrated industrial security program should be explored to determine the extent of cost savings for industry and government while improving protection of our national security interests. The response came back with a cover letter from Secretary Atwood, from Admiral Watkins, and from Judge Webster. The response says the globalization of industry, coupled with increased economic competition and the dramatic strategic developments in East and West relations, will lead to new and different threats from all of the new adversaries. "We agree it's a time for collective effort by government and industry to establish a single, integrated and cohesive security program."

In his response to the report on the NISP, President Bush concurred with plans to establish an interagency task force to develop the elements of the program *and* he stated that he was encouraged by plans to *include industry* in the development of a national program.

That is the charter we now have, government and industry together. That is the major item that should appear in the curriculum in the '90s for your programs for education and for training. First, to explain what the NISP is. What we need to do is have some kind of centralized source for the proper display or disbursement of information on the NISP, so everybody understands what it really is. As elements are developed, we must have train-the-trainer sessions. We need to train the whole of industry in a whole new program. Remember, *this is not a modified DISP*. This is a brand new system! When we are finished we must train those people who must evaluate performance on the program. There isn't anybody who is trained right now to do that. It is going to be a different kind of program. A kind of program that is somewhat more difficult to evaluate. We hope that we will be able to do that as part of the effort here. Everything starts now because it is still a concept. But it is like a new-born baby. We must start teaching it how to walk, we must feed it so it grows, and we must develop a mind set in it so it meets the challenges that are going to come to all of us in the '90s.

Dr. Bader is a senior vice-president of SRI International's Policy Division, which provides research and consulting services to public and corporate policymakers. He is a former Naval officer, and later served as a senior staff member of the Senate Foreign Relations Committee. Dr. Bader has authored a number of publications in the fields of national security, arms control, foreign affairs, and government policy.

The New Global Environment in Defense Industry

by William B. Bader

I've listened to some of your proceedings and read several reports by Dr. Mimi Stearns, a very good sociologist and political scientist who's enormously impressed with the intent and importance of these proceedings. So I think I have a sense of the problem that you are facing and I trust that I am up to the challenge of trying to gauge the technological and societal trends that will define a new environment for the 1990s—one in which security issues will be extremely important.

A new generation of scientists, engineers, and management consultants will create the new security consciousness in the course of their daily work. Every laboratory, cubicle, and office that contains networked or modemed computer equipment will be an experiment in security awareness. And SRI is a particularly interesting place for that kind of experiment. With an organization that has about 2,600 scientists, engineers, social scientists, and management consultants, it features some rather remarkable diversity. The population can be characterized on a spectrum that ranges from a high level of security awareness to a low one.

A large segment of our employee population has a high level of security awareness. That segment consists of the engineers who are part of the cleared (to perform classified government work) community in every sense of the word. They work in many very major classified programs. At the other end of the spectrum is a new group. The new group tends to be multinational, ethnically diverse individuals with few ties to the United States except in their work pattern. This group is similar to the increasing number of management consultants and people who work with big international firms that have become more global and more multinational in their activities and scope.

Probably a quarter to half the people who work with me (this number excludes people cleared for classified work) would find the rhetoric, if not the content, of this meeting somewhere between ludicrous and amusing because it doesn't fit with the world as they see it, and it doesn't fit with the experience they've had. One of the major challenges we face in increasing

security awareness is in the refinement of the rhetoric and in the development of a dialogue with these new practitioners.

Let me just say a few things quickly about that environment as I see it because how we all address what needs to be done and how we think about these issues is important. Let me first mention something about my own background. I formed the way I perceive the world, and how I perceive security issues and security awareness, as a LTJG in Japan in the 1950s and also as a CIA officer in the 1960s. As I look back on it, nostalgically, the environment was remarkably predictable and manageable—something we really don't have today.

Today, we're dealing in an arena in which sovereign nations compete to gain advantage in ways other than the traditional means of international trade. Today large corporations operate as world players and that serious difference creates a problem. Fifty of the global corporations we track at SRI have 40% of their sales outside their home countries. Xerox reports that 50% of its employees and 50% of its sales are outside the United States. Of Philips's assets, 60% are in Europe, 30% in North American and South American, 10% in Asia and Pacific. IBM employs 40% of its employees outside the United States. Whirlpool employs 43,000 people in 45 countries. What we're really doing now is competing in an increasingly borderless business world in which a company's national identity may be really difficult to define. The ambiguity creates enormous problems for us concerning the national identities of company X or company Y.

Of course, at the same time, governments are opening their borders to participate in these global economics. As you probably all know, foreign investment now has increasingly overshadowed trade flows. Foreign exchange transactions are running on a daily basis between \$325 billion and \$375 billion, while trade volume is some \$70 billion. You can see there's a big difference. So what does it mean?

It means that foreign direct investment all around the world has been growing at the rate of about 20% annually—four times faster than trade. Foreign direct investment is reshaping the whole international business structure. For example, the Japanese FDI (or foreign direct investment) in the United States has dramatically altered the structures of the U.S. automobile industry, machine tool industry, and the financial service industries. From the skyline of Los Angeles to the Rockefeller Center in New York, there are many indications of substantial investment by the Japanese, including what the Japanese may or may not do to the U.S. entertainment industry. What are the implications of this foreign direct investment throughout the world and, most particularly, of the foreign investment in the United States? We have to begin to wonder whether the nation-state is, in fact, economically and competitively the relevant unit of analysis.

How about your world here, which is often associated with the defense industry? The defense industry is becoming smaller, more consolidated, and more global in nature. Players will seek international affiliations, which we're now seeing, let's say, between General Dynamics and Mitsubishi. We'll eventually see a few large, major diversified, and very, very global firms in the United States, France, Germany, the United Kingdom, and Japan. These firms will be the survivors of what is very obviously going to be a shakeout in the defense industry. It will have very strong implications for all of us, and particularly for you. A dramatic increase in international partnerships and consortia is going to take place. Some of them are particularly noteworthy and I think worrisome because they have implications for information flow, information management, and competitive advantage. I'll just name a few. Lockheed and Aero-Spatiale, General Dynamics and British Aerospace, the U.S.-French CFM International, which is General Electric and SNECMA; the French Aircraft Engine Manufacture; and McDonnell Douglas and Samson. Others involve non-U.S. companies and have some of the same worrisome implications. The consolidation between Daimler-Benz and Mitsubishi has a truly haunting antecedent in the axis alliance of World War II.

All this comes at a time in the world when the U.S. defense industry moves into the 1990s with many more problems than those brought by smaller defense budgets. Just one note for the defense industry world: The percent of debt to equity among the 10 defense companies in the S&P Aerospace Index has more than doubled in the past seven years. The U.S. defense industry at this stage is becoming hungry for foreign alliances and investment. Defense companies are exceedingly vulnerable to the temptation to traffic in information and in data—and not necessarily the information and data of the 1950s, but the essential information and data in today's world that defines whether we are going to be, as a nation-state, competitive in this market place.

The next factor I'd like to discuss is sociological in nature. The process and product of security awareness programs in the Defense Department and the defense industries will become much more complicated and ambiguous because of the presence of foreign nationals in our facilities. Foreign nationals will become more common not only in our facilities, but in our laboratories, at our dinner tables, and increasingly in our bedrooms. Statistics indicate that the population at U.S. universities and graduate schools is increasingly foreign. At some graduate schools in the United States 60-65% of the graduate students in physics and in engineering come from another country. These people will be coming into our industries, including our defense industry.

And what does that mean? At a place like SRI we have a mixed population. You go into one laboratory and you find a Czech. In the next laboratory the scientist you find is Chinese. The situation generates a real problem of

managing these constituencies within the new environments we're creating. We have situations now at SRI where the poor chaps over in the cleared community receive notices that you may not go to the dining room for the next 2 1/2 days because of visiting Czechs or Chinese. The demographics are changing in our world, and the security world has to adjust.

Now let me turn to the implications of all this and to some of the recommendations inspired by our examination of national economics, strategic alliances, and cultural and national diversity. But first, I think we ought to acknowledge that whatever the demographic, economic, and competitive changes have wrought, a more important factor is at work. Information, data, and analysis are—and will remain—the most powerful engines and tools of economic security and power. The management of these precious resources is our biggest task. I think when we're trying to understand this environment and operate within it, we must keep our eye on information, data and analysis: their use, their traffic, and their essential nature to the competitive edge.

I think we ought to acknowledge at the same time that enhanced security awareness in the 1990s will be the result of a partnership, discussion, and in-



Maynard Anderson, William Bader, and Harry Volz

teraction at all levels: in corporations and businesses. Our efforts will be fruitless if they depend on administrative, legislative, statutory fiat. Partnership and discussion within your company is the trend, and it has to be the trend. No other way will work. At a time of constrained resources for security programs and for security education, we should take advantage of that reality. And I think that we are going to have to see more voluntary and more proactive involvement at all levels of your organizations.

We must make an attempt to educate and to convince people that some new words are relevant and important in this process. Let me give you one that you might think is absolutely heretical in the world that we now live in. The word is *ethics*. I believe that in the 1990s the true enemies of this state in terms of our economic and national security will be the Boesky's and the Millikens of the world rather than the Walkers. Individuals who are prepared to traffic in information and inside knowledge, whether they have to do with technologies or market trading, are a threat to our nation in a way that is much less obvious than the traditional security risk. No ethics and no standards existed among the major operators in what is now known as the Decade of Greed: the 1980s. In the security world, we need to work for ethics and ethical standards: personal standards, professional standards. We need to understand competitive advantage, to understand that you can damage the security of the United States or the economic security of the United States if you make deals, if you pass technology—if you do things that are damaging in an ethical sense.

I think these are the major forces, and I hope that you take away from these proceedings the desire to implement these kinds of attitudes and approaches in your own organizations. I'm not saying that you shouldn't have procedures and rules. I am saying that a more basic dimension is important.

Anyone in the information industry these days faces tough decisions. One of my programs at SRI takes information about emerging technologies from all over the world and creates documents called technology profiles. I have profiles of everything from advanced silicone microelectronics to biocatalysis; from fiber-optic sensors to neural networks. And what do I do with this technology information? I sell it all around the world. I sell it to businesses. I sell it to Mitsubishi. I sell it to whoever is prepared to pay for it. This is technology information. Is it a technology leak? Is it a dangerous loss of information as far as the American competitive position is concerned at this stage? In the last analysis, it is going to depend on all of us who are in this business of understanding the usefulness of data, information, and analysis to be responsible in terms of our national interest about what goes into those packages. That's where I think attitudes must change. We need more interaction. We need more mutual education. And we need a hell of a lot more sense of ethics and responsibility on the part of individuals who are dealing with information in this world.

Delivering the Right Message

by Maynard C. Anderson

Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

While other areas of the world pose challenges because of changes, our concentration has naturally turned toward those areas where change will continue and political instability will probably be characteristic. We find that the countries of Eastern-Central Europe are no longer part of the "Soviet Bloc" and must be dealt with on an individual basis. Eastern Europe is important to us. It's important to Americans whether these geopolitical matters pertain or not, because of the ethnic and historical ties to the region. That is something we didn't talk much about this week, but it's a factor. The peoples of those regions have warm feelings toward the United States. Humanitarian concerns become more personal.

Events have been moving in the American direction towards democratization and toward free market economics. We just heard some vivid examples of it this morning. There is a future possibility of Eastern European states merging into an all-European framework that might even include the Soviet Union and the United States. I suppose we have some precedent in the Helsinki process, the Conference on Security and Cooperation in Europe.

What is the awareness lesson of all that? I suppose that all of these things affect major United States interests. As we decide how to convey to our cleared populations their new responsibilities, those changes have to be understood.

We have learned this week that training is available, but not taken advantage of. There is uneven availability and application. And the impact of training programs for achieving awareness is somewhat uncertain.

Public opinion seems to be in support of our efforts that contribute to the national security in general. We must achieve and maintain the support of our constituencies.

While our role in the midst of uncertainties and changes is not clear, our message has to be current and our message has to be objective. We need to persuade people to take the actions that are necessary. The message must be understandable intellectually and believable emotionally. And I think awareness must be transparent. I think we must get to the point where we are aware, but we don't know it. I think we have to achieve that in all elements of security, particularly in the way the times are changing. Awareness is a

product. It is the result of training and education, but more than that, it is the result of intent and capability.

And a delta does continue to exist between policy and implementation. Sometimes I look at what goes on in the field and I don't recognize its relationship to what we wrote and distributed as policy. I don't recognize what we agreed to in Washington. We need to make sure that what gets to the end of the pipeline is delivered in clear, understandable language that doesn't leave any ambiguity.

I suppose the proper combination between what Bill DeGenaro called vision and reality will result in utility. We need to ensure that our system is some kind of compromise between dreams and reality. There is nothing wrong with dreaming, but you need to get it down to where it is useable, and that's the utility.

We pity the person who doesn't believe in humor. Humor incisively targets an issue. There is a funny story for every aspect of human behavior and there are many ways to look at that. There was an elderly Jewish gentleman who ate at the same restaurant in New York every night. He came in every night for 22 years. He had the same meal. One night he sat down and the waiter brought him his soup. He called the waiter back and said, "Taste the soup." The waiter said, "I don't have to taste the soup. I bring you this soup every night for 22 years." He said, "Taste the soup." "All right, I'll taste the soup, where is the spoon?" He said, "Ah-ha!" There is a message to humor.

The other story that brings it out more clearly perhaps is told by a friend of mine who was a high school drop-out but who now has a lot of advanced degrees and makes his living teaching. He was once waiting on tables in Altoona, Pennsylvania, at the Holiday Inn. After a banquet one night a very distinguished gentleman got up to address the audience and said, "I'm the sales manager for Alpo dog food. I want to know who has the best packaging in the industry." Everyone was silent. He repeated, "You didn't hear me. Who has the best packaging in the industry?" The audience finally got the message and replied, "We do, we do." He asked, "Who has the best sales force in the industry?" "We do, we do." "Who has the best sales technique in the industry?" And they said, "We do, we do." Then he asked, "Then why are sales down?" From the midst of the audience a small voice said, "Because the dogs don't like it." There's a lesson there. We need to make sure that what we have to sell is likeable.

Establishment of security in hearts and minds is necessary. Employee assistance programs are a wonderful forum for awareness; but they normally can't be mixed with security. It's a very dangerous situation. We cannot infringe on anyone's right to rehabilitation; we are prohibited from doing that by statute. But it's a wonderful opportunity for awareness, because who is

more "aware" than an employee who was responsible for some failure, but who now understands what's necessary, and who is able to achieve continuing awareness from the recollection that sometimes things go wrong. Often the greatest proselyte of anti-smoking is the former smoker. We need to look at the opportunities in that kind of process.

Have we been victims of trusting the system? I think so. People have relied on the system to work. People make the system work. Change does not abide complacency. We need to realign our priorities. I love to hear Jim Freeze talk. He reminded me this morning about a saying that is going around in Washington, now attributed to Mark Russell: "Hypocrisy is the vaseline of political intercourse." There was no hypocrisy in his speech—it was straightforward. But I want to add something. You said "P-2", Jim, (perpetuation and profit). I think you ought to think about "P-3", perpetuation, profit and people. Because that's really what's going to make your company work and that's what really is going to make government units work. And I think P-2 and P-3 make it necessary to change the rhetoric of security. I think it reminds us, as this conference has, that we talk too much to each other. We've had other kinds of people come and talk to us and that demonstrates that awareness is a global issue.

There are increasing foreign national presences, there are foreign national investments in the United States. We need to ask who we are sharing this critical information with? Ethics and standards and judgment will determine not only what we will share, but who we will share it with, and how we will share it.

There are four characteristics that describe the needs highlighted by this conference that I think are the most significant: responsibility, accountability, innovation, and creativity. I think if we remember the need for those qualities in our programs, we probably will have some very successful efforts in our own organizations.

Let me take this opportunity to say thank you to the Personnel Security Research Education Center and its staff and the Defense Security Institute and its staff for what I think has been a very productive time in Monterey.

Closing Remarks

R. Everett Gravelle, Director
Department of Defense Security Institute

For those of you who have suspected that I'm a risk-taker, you've now had that suspicion confirmed since I'm following Maynard Anderson and I'm going to allow Roger Denk to go after me. Very risky indeed. For me personally this has been a stimulating and interesting two and a half days. It has certainly served to clarify and to validate some of the ideas about security awareness that I have, and it's challenged some of the others. It's been a very good learning opportunity. If this experience has served to stimulate your thinking and given you cause to reflect that we may not all share a common understanding or agreement about just what security awareness and education is, or even *should* be, then I think we can conclude this symposium has had some success.

It's been said that sometimes the first step to solving a problem is to admire it. I submit to you that we don't have a problem in security awareness, because the word *problem* usually implies that there are answers or solutions. I think that what we have with security awareness is a series of challenges. We don't seek solutions or answers to challenges. Instead we devise strategies. Now that may sound like I'm splitting hairs semantically, but I assure you that that's not my intent. Whether you view security awareness as an activity or state of mind, behavior, outcome or a result, there is one constant, and that is that in all of those concepts, human activity is involved. And with human activity and interaction, we don't really have answers or solutions; we have theories and we have strategies.

For the last few days we've looked at security awareness from a variety of viewpoints, and we have truly admired the challenges. Now I think it's time that we go about the serious business of developing strategies to deal with these challenges. During these proceedings there have been a series of words that have tended to underpin our discussions, and Maynard certainly mentioned four very important ones. They have recurred again and again throughout our dialogues, and I think these words best represent the challenges that we face. I'm going to give you my personal list. Here they are: expectations, goals, objectives, effectiveness, quality (certainly a recurring theme), results, measurement, sanctions, rewards, oversight, and accountability.

Up until now I think our concerns about these issues have been, for the most part, either ill-defined or unstated. Borrowing from Bill DeGenaro's vocabulary, I would say that we lacked a "vision" as far as security aware-

ness is concerned. In the Department of Defense, for security programs, we have two primary methods of expressing our visions: one is by promulgation of policy by directives, regulations, and manuals. And the other is by speeches presented by Maynard Anderson. To the extent that this symposium has helped us to focus on the fact that perhaps our vision is not clear, its timing may be particularly appropriate.

Maynard has predicted that we will probably see a new Personnel Security Executive Order in the next two years. At ISOO Steve Garfinkel and his staff are in the final stages of development of ISOO Directive #2, which will deal with security education. At OSD we are in the process of revising the 5200.1-R (The Information Security Program Regulation) and the 5200.2-R (The Personnel Security Program Regulation) and, as we heard at great length from Harry Volz, the NISP certainly has a clean slate, so there is much to be developed in that arena.

I think lastly, but certainly not least, there is the Institute's implementing regulation which some of my government colleagues have seen, and most of you in industry have not seen. That document is in the queue for final coordination. I can assure you that it *does* address the vast majority of security awareness and education issues and concerns that we have discussed here these last few days. We have already informally coordinated our first draft with the components, and our revised draft incorporating their feedback is now in staffing at OSD. Now if pressed for a diplomatic assessment of our first draft, I suspect that some of my colleagues in the services might say, "Too visionary." And they may be right. But now having attended this symposium, they just may rethink their positions—at least I hope they will. The development and refinement of a vision is certainly not an easy or a finite process. What I am happy to report to you is that we have already taken the first steps towards that goal and this symposium has confirmed that our compass heading is true.

One final note before Roger Denk takes over this lectern to wrap up the proceedings. During yesterday's panel discussion Larry Howe noted, "There is not a sufficient buy-in by either government or industry." I can't recall whether or not Larry was specifically talking about security awareness, but in any case I think the description fits. And I offer this to you: When we meet in the year 2000, I hope that we can look back on Larry's observation and say, "It may have been accurate for the 1970s and the 1980s, but it just wasn't so in the 1990s." Thank you.

Closing Remarks

Roger Denk, Director
Defense Personnel Security Research and Education Center

I want to thank each of the individuals who spoke here for their candid and thought-provoking remarks. We covered a great deal of ground since we began this symposium two and a half days ago. I said at that time this was not to be a problem-solving or policy recommendation effort. However, you might feel that some of the issues raised and discussed amongst us will assist you in solving problems or policy. Regardless, I think that we all benefited from what we heard and said here.

To each of you who made the effort to come here in this tight budgetary time—thank you as well. We hope that the contacts you made here will enable you to share ideas and concerns with other professionals in this field. And thank you for your comments and questions to the speakers in the panels. Without this give and take, we would have a much less successful symposium.

Before I conclude, I wish to give special recognition to Jim Riedel at the Defense Personnel Security Research and Education Center who conceived, designed, planned, and administered this symposium. We owe a tremendous debt to him for this accomplishment. With the assistance of the participating staff at PERSEREC and at DODSI, we will be producing a set of proceedings which will be edited and published by Lynn Fischer at DODSI. The proceedings will be available in the next several months and it will be mailed to each of the participants. Again, on behalf of PERSEREC and DODSI, let me thank you for coming and participating in this symposium. I hope it has given substance to the issues of security awareness and the challenge of the 1990s.

Thank you and have a safe journey home.

An Immediate Assessment: The Evaluation of the Symposium by Participants

by Suzanne Wood

At the end of the symposium, participants were asked to fill out evaluation forms. Forty-seven percent of the participants eventually returned the forms. The grade ratings are summarized in the charts that follow.

Many of the forms included written observations in addition to the ratings. Several respondents wrote only brief comments, such as "Excellent meeting/formula!" and "Keep it going!" Others wrote lengthier and mostly complimentary summary remarks, such as "Excellent, stimulating and a good learning experience" and "Probably one of the best symposiums I've ever attended."

Several themes emerged from other longer written comments on the evaluation forms and from the 15 letters of thanks received after the symposium. We summarize these themes below, with no effort at strict quantification.

Content

The vast majority of participants appreciated the breadth, scope and yet tight focus of the ideas presented, and they enjoyed the wide array of people at the symposium. Many mentioned the advantages of having a good mix of government and industry representatives, and several commented on the refreshing and provocative introduction of presentations from the advertising, training, and evaluation arenas.

A few suggested that the symposium was too philosophical in scope and that it should have been pegged at a more practical level. However, the majority felt that the symposium provided an excellent way of communicating information in the context of the stated goal of the symposium, which was to stimulate and broaden the thinking of security professionals. The symposium allowed the participants to reflect on many aspects of security awareness and to take time to look at the field "through different lenses," as one person put it.

Format

Most of the participants liked the variety of speakers and topics. And most liked the presentation organization, *i.e.*, single speakers, or panels with

moderators. However, a few complained that some speakers ate up the period allotted, thus minimizing time for audience participation. Several would have preferred that small brainstorming groups be held after the major presentations so that participants could exchange ideas and thus make a more significant personal contribution to the proceedings.

Many mentioned their appreciation of the opportunity at the symposium to come together as a professional community and to network with their counterparts and colleagues in industry, government, and the military.

Speakers

Most described the speakers as being "excellent" overall. However, a few said there was some unevenness among the speakers. Some presenters were simply not as effective as others: the topic was not always addressed directly, and presentations were not always sharply prepared.

While a few participants felt that speakers should have a basic knowledge of the security field, others saw a great advantage to bringing in outsiders who may not have that knowledge but whose perspectives were fresh and stimulating.

Administration/management

The overwhelming opinion was that the administration of the symposium was done very well. As one participant put it, the symposium was "put together with great thought and presented with great success."

Two people suggested that at future symposia paper copies of presentation slides should be provided, if possible, for participants at the time of the presentation.

Facilities/audiovisual

A handful of participants commented on the occasional failures in the professional audiovisual service's equipment, although one person forgivingly urged the organizers not to get "hung up on minor problems such as AV." Two people complained about the meeting room itself ("noisy," "too dark for notetaking," "cold in the morning.") Under the category of "first of its type" for critical comments about conferences sponsored by the Department of Defense, one weary attendee complained that he was kept up all night by barking seals.

Recommendations

Several participants suggested continuing such conferences annually in order to build on this foundation. One suggested that industry might host (and fund) any such follow-on meetings.

While the broad goal of the symposium was clearly stated in invitation materials, a few participants said they would have preferred a more "doer"-level symposium, aimed at staff rather than directors, where more practical topics could have been discussed. Perhaps such hands-on workshops might be offered in the future in a different context.

Evaluations



Speakers

James A. Abrahamson
Exec Vice-President, Corporate Dev
Hughes Aircraft Company
7200 Hughes Terrace
P.O. Box 45066
Los Angeles CA 90045-0066
(213) 568-6600 FX 649-3155

Maynard C. Anderson
Assistant Deputy Under Secretary
of Defense (CI&S)
Room 2E812, The Pentagon
Washington DC 20301
(703) 695-6607 AV 225-6607
FX 614-8976

Dr. William B. Bader
Senior Vice-President, Policy Group
SRI International
333 Ravenswood Avenue
Menlo Park CA 94025
(415) 859-3078

Dr. Robert Bailey
Executive Vice-President:
Director of Marketing Services
BBDO
410 N. Michigan Avenue
Chicago IL 60611
(312) 337-7860 FX 337-6871

Dr. Robert O. Brinkerhoff
Department of Education Leadership
Western Michigan University
Kalamazoo MI 49008
(616) 387-3881

Fred Capps
National DECA Coordinator
Federal Bureau of Investigation
10th & Pennsylvania Ave., N.W.
Washington DC 20535
(202) 324-2566

Deborah Russell Collins
Security Consultant
Collins Consulting Group
Mgr, Sec. Admin & Training, ESL/TRW
1360 Josselyn Canyon Road, #44
Monterey CA 93940-6433
(408) 743-6009 FX 743-6345

William E. DeGenaro
Director of Business Research
& Analysis
3M Corporate Marketing Services
3M Center Building 225-3S-05
St. Paul MN 55144-1000
(612) 733-8974

Dr. Roger P. Denk
Defense Personnel Security
Research and Education Center
99 Pacific Street, Bldg 455-E
Monterey CA 93940
(408) 646-2448 AV 878-2448
FX (408) 646-2041

Catherine A. Dyl
Corporate Security Manager
Bolt Beranek and Newman Inc.
70 Fawcett St.
Cambridge MA 02148
(617) 873-3291 FX 547-8918

Dr. Richard S. Elster
Dean of Instruction
Code 06, Naval Postgraduate School
Monterey CA 93943
(408) 646-2161 AV 878-2161
FX 646-3407

James E. Freeze, MG US Army (Ret)
President, The Freeze Corporation
5415-D Backlick Road
Springfield VA 22151
(703) 941-5065 FX 941-1586

Steven Garfinkel
Director, Information Security
Oversight Office
750 17th St., N.W.
Suite 530
Washington DC 20006
(202) 634-6150 FX 634-6131

Joseph A. Grau
Chief, Information Security Division
DOD Security Institute
c/o DGSC
Richmond VA 23297-5091
(804) 275-3816 AV 695-3816
FX 275-5239

R. Everett Gravelle
Director, DOD Security Institute
c/o DGSC
Richmond VA 23297-5091
(804) 275-3012 AV 695-3012
FX 275-5239

Ernest V. Haag
Western Operations Manager
HumRRO International Inc.
99 Pacific Street, Bldg 400-C
Monterey CA 93940
(408) 647-9975

Dr. Henry M. Halff
Chief Scientist
Halff Resources, Inc.
4918 33rd Road North
Arlington VA 22207
(703) 237-0984 FX 534-2089

Lawrence J. Howe
Corporate Vice-Pres., Dir of Security
Science Applications International
Corporation (SAIC)
10260 Campus Point Drive
San Diego CA 92121
(619) 552-4745 FX 552-4797

Brig Gen Frank K. Martin
The Air Force Chief of Security Police
Air Force Office of Security Police
Kirtland Air Force Base NM 87117-6001
(505) 844-1315 AV 244-1315
FX 846-1360

Willis J. Reilly
Deputy Director of Security
Central Intelligence Agency
Washington DC 20505
(703) 482-7852

Dr. James A. Riedel
Research Scientist
Defense Personnel Security
Research and Education Center
99 Pacific St., Bldg. 455-E
Monterey CA 93940
(408) 646-2448 AV 878-2448
FX 646-2041

Dr. Stuart Robertshaw
Corporate Executive Officer
National Association for the
Humor Impaired
400 S. 15th Street, Suite 201
La Crosse WI 54601
(608) 785-8442

Jed Selter
Senior Mgr, Security & Fire Protection
The Boeing Company
MS 7E-79
P.O. Box 3707
Seattle WA 98124-2207
(206) 393-8232 FX 477-1449

Dr. Tom W. Smith
Director, General Social Survey
National Opinion Research Center
1155 East 60th Street
Chicago IL 60637
(312) 753-7500 FX 753-7886

L. Britt Snider
General Counsel
Senate Select Committee on Intelligence
Room 211
Senate Hart Office Building
Washington DC 20510
(202) 229-1700

Harry A. Volz
Director, Security and Transportation
Grumman Corporation
Mail Stop A02-16
Bethpage NY 11714-3586
(516) 575-3933 FX 575-6938

RADM Ralph W. West, Jr.
Superintendent
Naval Postgraduate School
Monterey CA 93943
(408) 646-2511 AV 878-2511

Participants

Thomas J. Adams, Manager
Special Access Security, B/581
Lockheed Missiles and Space Company
1111 Lockheed Way
Sunnyvale CA 94089-3504
(408) 756-2721

Norman Ansley
Chief, Polygraph & Personnel
Security Research, M503
National Security Agency
9800 Savage Road
Ft. George Meade MD 20755-6000
(301) 859-6949

R. C. Averill
Manager, Government Security
O/27-11, B/575
Lockheed Missiles and Space Company
1111 Lockheed Way
Sunnyvale CA 94089-3504
(408) 756-4388

Gordon Barland
Director of Research
DoD Polygraph Institute
Building 3165
Fort McClellan AL 32605-5114
(205) 848-3803 AV 865-3915

John W. Bates
Security Officer
Security Department
Naval Air Test Center
Naval Air Station
Patuxent River MD 20670-5425
(301) 863-3277 AV 326-3277
FX 863-4402

Ronald H. Beatty
Corporate Director, Security
Rockwell International Corporation
2230 E. Imperial Blvd.
El Segundo CA 90245
(213) 647-5285 FAX 647-5428

David Bender
Director of Intelligence
Engineering Research Group
SRI International
1611 N. Kent St.
Arlington VA 22209
(703) 247-8516 FAX 247-8569

C. Michael Berry
Chairman, Security Management Dept.
Department of Defense Security Institute
c/o Defense General Supply Center
Richmond VA 23297-5091
(804) 275-4894 AV 695-4894
FX 275-5239

Edgar N. Best
Staff Vice President, Corporate Security
Hughes Aircraft Company
7200 Hughes Terrace
P.O. Box 45066
Los Angeles CA 90045-0066
(213) 568-6688 FX 649-2806

Richard A. Black
Director, Corporate Security
SRI International
333 Ravenswood Ave.
Menlo Park CA 94025
(415) 859-3875 FX 859-5766

Mr. Richard H. Blay
Director, Security and Fire Protection
The Boeing Company
P.O. Box 3707 (M/S 7E-70)
Seattle WA 98124-2207
(206) 393-8230 FX 477-1449

Victor Brown
FCI Faculty
Defense Intelligence College
(Attn: DIC-2A)
Washington DC 20340-5485
(202) 373-3897 AV 243-3897

Robert E. Burgener
Director of Security
Booz-Allen & Hamilton, Inc.
4330 East West Highway
Bethesda MD 20814-4455
(301) 951-2004 FAX 951-2255

Michael H. Capps
Attn: M503
Ft. Meade MD 20755-6000
(301) 859-6949 AV 235-0111, x6949

Ralph M. Carney
Program Manager
Defense Personnel Security Research
and Education Center
99 Pacific St., Bldg. 455-E
Monterey CA 93940-2481

Joe Carrow
Director, Security
McDonnell Douglas Space Systems Co.
5301 Bolsa Ave., MS 121E
Huntington Beach CA 92647-2048
(714) 896-2123 FX 896-1946

Jack A. Chatowski
Manager of Government Security
TRW S&D Sector
One Space Park, MS/S, Rm 2836
Redondo Beach CA 90278
(213) 812-4785 FX 812-7111

Captain David T. Cheatham
HQ USAF/XOOSE (OPSEC)
Room BF938B, The Pentagon
Washington DC 20330-5054
(703) 697-9390 AV 227-9390
FX 227-8715

Colonel Charles R. Cleveland
Director, Security & Counterintelligence
Defense Intelligence Agency
Room 2A540, The Pentagon
Washington DC 20340-1248
(703) 695-0407 AV 225-0407

Kent S. Crawford
Project Manager
Defense Personnel Security Research
Education Center
99 Pacific St., Bldg. 455-E
Monterey CA 93940-2481

Harold Daniels
Director, Baltimore Office
ITT Aerospace/Communications Division
800 International Drive, Suite 110
Linthicum MD 21090-2224
(301) 850-0608 FAX 850-0617

Edward J. DeMattee
Chief, Industrial Security
Martin Marietta, Simulation Systems
P.O. Box 62186
Colorado Springs CO 80962
(719) 380-2310 FX 380-0399

Jacquie K. DePetrus
Security Supervisor, FSO
Systems Control Technology, Inc.
2300 Geng Road
P.O. Box 10180
Palo Alto CA 94303
(415) 494-2233 #566 FAX 496-6595

Carol F. Donner
Regional Security Director
General Research Corporation
P.O. Box 6770
Santa Barbara CA 93160-6770
(805) 964-7724 FX 967-7094

G. R. Eisele
Director, Center for Personnel Security
Assurance, Research and Analysis
Oak Ridge Assoc Univ - Med Sciences Div
P.O. Box 117
Oak Ridge TN 37831-0117
(615) 576-2208 FX 576-3194

Thomas E. Ewald
Deputy Director, Investigations
Defense Investigative Service (V0100)
1900 Half Street, S.W.
Washington DC 20324-1700
(202) 475-1331 AV 335-1331
FX 475-7599

Lynn F. Fischer
Chief, Security Awareness Division
Department of Defense Security Institute
c/o Defense General Supply Center
Richmond VA 23297-5091
(804) 275-3824 AV 695-3824
FX 275-5239

Edwin W. Forrest (Code 21B22)
Security Education Specialist
CNO (OP-09N2)
Bldg 111, Sicard St.
Washington Navy Yard
Washington DC 20388-5021
(202) 433-8858 AV 288-8858
FX 433-8849

Colonel Marvin T. Furusho
Deputy for Sec and Investigative Pgms
SAF/AAZ
Room 5D966, The Pentagon
Washington DC 20330-1000
(703) 693-2017 AV 223-2017
FX 693-2059

Lynn Gebrowsky
Security Specialist
Defense Programs
U.S. Department of Energy
Washington DC 20545
(301) 353-3200 FX 353-4164

Kevin P. Giblin
Supervisory Intelligence Research Spec
FBI Headquarters, JEH Bldg.
10th & Pennsylvania Ave.
Washington DC 20535
(202) 324-2260 FX 324-3000

John R. Goral
Chief, Personnel Security Data
& Special Studies
Defense Manpower Data Center
99 Pacific St., Suite 155A
Monterey CA 93940-2453
(408) 655-0400 AV 878-2951

R. R. Gorena
Asst for Information & Personnel
Security Policy
Department of the Navy (OP-09N2)
Washington Navy Yard
Washington DC 20388-5021
(202) 433-8841 AV 288-8841
FX 433-8849

David R. Granish
Special Agent
Federal Bureau of Investigation
11000 Wilshire Blvd
Los Angeles CA 90024
(213) 477-6565 x2248

J. E. Guibord
Security Director
Loral Aerospace
2324 Port Carlisle
Newport Beach CA 92660
(714) 644-2677

Martin V. Hale
Section Chief
Federal Bureau of Investigation
10th & Pennsylvania Ave., N.W.
Washington DC 20535
(202) 324-4901 FAX 324-4705

Helmut Hawkins
Research Coordinator
c/o Mr. Maynard Anderson
DUSD (CI&S)
Room 2E812, The Pentagon
Washington DC 20301
(202) 693-6497
AV 223-6497 FX 693-6498

James A. Hendrick
Program Manager
Defense Evaluation Support Activity
5201 Leesburg Pike, Suite 503
Falls Church VA 22041
(703) 685-1431 FX 685-1415

Neal Henshall
Manager, Special Services
AIL Systems, Inc.
Commack Road
Deer Park NY 11729
(516) 595-4100 FX 595-4368

Lt Col Neil S. Hibler
Command Clinical Psychologist
HQ AFOSI/IVB
Bolling AFB DC 20332-6001
(202) 767-5287 AV 297-5287
FX 767-6554

Robert A. Highbarger
Director of International Support
Cray Research, Inc.
14440 Cherry Lane Ct., Suite 218
Laurel MD 20707
(301) 490-1800 FX 490-3601

Thomas D. Howard, Jr.
Deputy for Security Policy
Office of the Asst. Secy of the Army
(Manpower & Reserve Affairs)
Room 2E591, The Pentagon
Washington DC 20301
(703) 695-0260 AV 225-0260

George Jackson
Security Specialist
NISRO MIDPAC
Box 76
Pearl Harbor HI 96860-7200
(808) 487-8797 AV 315-471-8473
FX 474-3243

Dan Jacobson
Director, Department of the Navy
Central Adjudication Facility
Washington DC 20388-5029
(202) 433-8870 AV 288-8870
FX (202) 433-8875

George F. Jelen
Director of Operations Security
National Security Agency
Ft. George G. Meade MD 20755-6000
(301) 688-7454 AV 235-7454

Stephen L. Jenks
Special Agent, DECA Coordinator
Federal Bureau of Investigation
P.O. Box 1733
Palo Alto CA 94301
(415) 326-4930 FAX 326-4932

Norman E. Johnson
Defense Investigative Service
Northwestern Regional Director
of Industrial Security
Bldg 35
Presidio of San Francisco CA 94129-7700
(415) 561-3235 AV 586-3235
FX 563-4738

Owen B. Johnson
Deputy Director
Office of Safeguards and Security
U.S. Department of Energy
Washington DC 20545
(301) 353-3203 FX 353-4164

ATTN: IASEC-C (Connie B. Johnston)
Commander
USA INSCOM
Ft. Belvoir VA 22060-5370
(703) 706-2621 AV 229-2621
FX 355-7881

Phil Joseph
Administrator, Security Education/Training
C-401 MS13-3
McDonnell Douglas Electronic Systems Co.
5301 Bolsa Ave.
Huntington Beach CA 92647
(714) 896-4339/2515 FX 896-1313

John M. Justice
Special Agent
Federal Bureau of Investigation
11000 Wilshire Blvd.
Los Angeles CA 90024
(213) 477-6565

David B. Kendrick
Supervisor, Security Administration
E Systems, Inc.
P.O. Box 660023
Dallas TX 75226-0023
(214) 272-0515 x 5776 FX 272-8144

James E. Kenney
Director of Security
Unisys Defense Systems
8201 Greensboro Drive, Suite 1100
McLean VA 22102
(703) 847-3410 FX 847-3782/3298

P. J. Kimball
Director, Security and Emergency Services
Lockheed Missiles and Space Company
1111 Lockheed Way
Sunnyvale CA 94089-3504
(408) 742-3211

Waymouth G. Knight
Director, Corporate and
Special Programs Security
Space Applications Corporation
901 Follin Lane, Suite 400
Vienna VA 22180
(703) 255-5200 X216 FX 255-3667

Philip C. Krebs
Security Manager
Department of the Navy
Navy International Programs Office
Washington DC 20350-5000
(202) 692-4706 AV 222-4706
FX 766-5633

Farrell J. Kunz
Director of Corporate Security
Honeywell, Inc.
Honeywell Plaza
Minneapolis MN 55408
(612) 870-6711 FX 870-6231

Bernard A. Lamoureux
Corporate Director of Security
Lockheed Corporation
4500 Park Granada Blvd.
Calabasas CA 91399-0510
(818) 712-2402 FAX 712-2329

Robert F. Lang
Director, Research Security
Georgia Institute of Technology
Research Security Department
Atlanta GA 30332-0800
(404) 894-4822 FX 894-3819

William F. Lavallee
Director, Security and Safety
LTV Aircraft Products Group
P.O. Box 655907
Dallas TX 75265-5907
(214) 266-2400 FX 266-5761

M. Francina Lester
Industrial Security Supervisor
University of Dayton
Attn: Industrial Security KL 521
300 College Park
Dayton OH 45469-0103
(513) 229-2115 FAX 229-3433

James P. Linn
Asst Vice President, Corporate Mgr
DoD Security Programs
Science Applications International Corp
10260 Campus Point Drive
San Diego CA 92121
(619) 546-6701 FX 546-6777

Walter T. Lloyd
Manager, Special Programs Security
Hughes Aircraft Company, M/S B124
7200 Hughes Terrace
Los Angeles CA 90045-0066
(213) 337-0274 FX 649-2806

Thomas M. Locke
Communications Security Officer
National Security Agency
9800 Savage Rd.
Ft. George G. Meade MD 20755-6000
(301) 688-6098 AV 235-6098

Thomas K. MacKinney
Director, Security & Admin Services
Aerojet General Corporation
100 Blue Ravin Rd.
Folsom CA 95630
(916) 351-8645 FAX 351-8666

Donald L. Madison
Manager, Special Program Security
Lockheed Missiles & Space Company, Inc
0/27-12 B/104
1111 Lockheed Way
Sunnyvale CA 94089-3504

ATTN: APIN-SC (Robert J. Marouchoc)
Chief, Information Security
& Counterintelligence
HQ, US Army Pacific (USARPAC)
Fort Shafter HI 96858-5100
(808) 438-1743 FX 438-6302

Thomas R. Martin
Program Analyst
Information Security Oversight Office
750 17th Street, N.W.
Suite 530
Washington DC 20006
(202) 634-6139 FX 634-6131

Lynn E. Mattice
Corporate Director of Security
Northrop Corporation
Corporate Headquarters
1840 Century Park East
Los Angeles CA 90067-2199
(213) 201-3257 FAX 553-2076

Robert H. McCamish
Chief, INFOSEC Field Evaluation
National Security Agency
9800 Savage Road
Ft. George G. Meade MD 20755-6000
(301) 688-6025

Robert J. McCormick
Administrative Assistant to the
Secretary of the Air Force
SAF/AA
Washington DC 20330-1000
(703) 695-9492 AV 225-9492

Richard L. McGuire
Director of Security
Grumman Corporation
Mail Stop A02-16
Bethpage NY 11714
(516) 346-2301 FX 575-6938

Michael H. McMillan
Deputy Assistant Director for Security
Office of Security
On-Site Inspection Agency
Washington DC 20041-0498
(703) 742-4520 (800) 283-2179

Joseph R. Mellitt
Manager, Awareness, Internat'l Security
Hughes Aircraft Company, M/S B120
7200 Hughes Terrace
P.O. Box 45066
Los Angeles CA 90045-0066
(213) 568-6692 FX 649-2806

Stan T. Miller
Director of Security
Teledyne Brown Engineering
P.O. Box 070007
Huntsville AL 35807-7007
(205) 726-1277 FX 726-2951

Daniel J. Muscat
Manager, Security & Plant Protection
Smiths Industries Aerospace
& Defense Systems, Inc.
4141 Eastern Ave, S.E.
Grand Rapids MI 49518-8727
(616) 241-7607 FX 241-7533

R. Gary Myers
Director, Group Sensitive Programs &
Deputy Director, Security
SRI International
333 Ravenswood Ave.
Menlo Park CA 94025
(415) 859-3190 FX 859-4222

Francis K. Nekoba, Col, USAF
Director, Security & Communication Mgmt
HQ USAF/INS
Bldg. 520
Bolling AFB
Washington DC 20332-5000
(202) 767-9241 AV 297-9241

Peter R. Nelson
Assistant for Personnel Security
ODUSD(SP) CI&IP)
Room 3C267, The Pentagon
Washington DC 20301-2200
(703) 697-3969 AV 227-4917
FX (703) 430-1497

Michael S. Nicholson
Manager, Corporate Security
Westinghouse Electric Corporation
11 Stanwix St.
Pittsburgh PA 15222
(412) 642-3097 FX 642-3871

Paul F. Nordberg
Director of Security, Safety and Health
Martin Marietta Astronautics Group
P.O. Box 179
Denver CO 80201
(303) 977-3181 FX 971-4900

Peggi A. Parks
Facility Security Manager
E-Systems, Inc.
CAPA Division
Suite 200, 10530 Rosehaven St
Fairfax VA 22030
(703) 352-0300 FAX 691-3067

George Paseur
Director of Information Security
HQ, Air Force Office of Security Police
Kirtland AFB NM 87117-6001
(505) 844-3322 AV 244-3322
FX 844-9448

James D. Passarelli
Supervisory Security Specialist
DA ODCSINT
HQ DA (DAMI-CIS)
Washington DC 20310-1051
(703) 695-8924 AV 225-8924
FX 697-7993

Janice L. Peth
Government Security
Loral Western Development Labs
3200 Zanker Road, M/S D09
San Jose CA 95161-9041
(408) 473-7481 FX 473-7926

Mr. Albert E. Philippon
Director, Information Security
HQ Strategic Air Command
HQ SAC/SPI
Offutt AFB NE 68113-5000
(402) 294-5224 AV 271-6868
FX 271-7628

Ray Pollari
Director, Counterintelligence &
Investigative Programs, ODUSD(P)
Room 3C260, The Pentagon
Washington DC 20301-2000
(202) 697-9678 AV 227-9678

William H. Pretto
Director of Security
Lockheed Advanced Development Company
Attn: Dept. 2170, Bldg. 63, Plant A-I
P.O. Box 551
Burbank CA 91520
(818) 847-7461 FX 847-1959

Attn: Mr. George Riddick (Code 24)
Asst Dir, Training, Antiterrorism
& Security Forces
Commander, Naval Investigative Command
Building 111, Washington Navy Yard
Washington DC 20388-5024
(202) 433-9119 AV 288-9119
FAX 433-9079

William T. Riebel
Deputy ADCSOPS-CI
Commander, INSCOM
Attn: IAOPS-CI-D
Ft. Belvoir VA 22060-5370
(703) 706-1038

Russell J. Riedell, Jr.
Security Specialist
Defense Mapping Agency
8613 Lee Highway
Fairfax VA 22031-2137
(703) 285-9171 AV 356-9171
FX 285-9374

Major Bolivar V. Rivera
Chief, Security Education Branch
HQ AFOSP/SPIB
Kirtland AFB NM 87117-6001
(505) 844-9446 AV 244-9446

Joyce I. Robertson
Senior Classification Management Spec
Bell Helicopter Textron, Inc.
P.O. Box 482
Fort Worth TX 76101
(817) 280-4124 FX 280-8450

H. James Rogan
Manager, Corporate Information Security
Northrop Corporation, 121CC
Corporate Headquarters
1840 Century Park East
Los Angeles CA 90067
(213) 201-3319 FX 553-2076

Robert B. Safreed
Director of Security
TRW S&D Sector
One Space Park, Bldg. 144/Rm. 1420
Redondo Beach CA 90278
(213) 813-6500 FAX 813-3329

Theodore R. Sarbin
Senior Researcher
Defense Personnel Security Research
Education Center
99 Pacific St., Bldg. 455-E
Monterey CA 93940-2481

Augustina K. Scardina
Instructor, Industrial Security Dept
Dept of Defense Security Institute
c/o Defense General Supply Center
Richmond VA 23297-5091
(804) 275-5308 AV 695-5308
FX 275-5239

Richard D. Semmel
Chief, Information Security
HQ AFLC/SPI
Wright-Patterson AFB OH 45433-5001
(513) 257-9854 AV 787-9854
FAX 787-3337/8

Barbara A. Sheckells
SSO Navy Representative
Naval Intell Sec Awareness Committee
Naval Intelligence Command
4600 Silver Hill Road (NIC-43)
Washington DC 20389-5000
(202) 763-3576/9 AV 293-3576

Charles R. Smith
Corporate Security Manager
Vitro Corporation
14000 Georgia Ave.
Silver Spring MD 20906-2972
(301) 231-2604 FX 231-2277

Susan Snyder
Manager, Information Security
Honeywell Systems & Research Center
3660 Technology Drive
Minneapolis MN 55418
(612) 782-7222 FAX 782-7438

Debra Stacy
Security Administrator
ESL, Inc.
495 Java Drive
Sunnyvale CA 94088-3510
(408) 743-6355

Attn: Ms. Laura Stanley (GH)
Director, Information Security
Programs Division
Commander, Naval Security Group
Command
3801 Nebraska Ave.
Washington DC 20393-5212
(202) 282-0282 FX 282-2605

Marian Stearns
Vice President, Health and Human
Resources Research Division
SRI International
333 Ravenswood Ave.
Menlo Park CA 94025
(415) 859-3997

Patricia R. Stentz
Security Education Officer
Defense Intelligence Agency
Attn: OSC-3 (Security Education)
3100 Clarendon Blvd
Arlington VA 22201-5320
(703) 284-1309 AV 251-1309

Michael Sterlacci
Asst General Counsel (Legal Counsel)
Room 3E988, The Pentagon
Washington DC 20301-6000
(703) 697-2714 AV 227-2714

Larry Stitt
Chief, Security Division
Office of the Deputy Chief of Staff
for Intelligence
USAISC, Attn: ASIS-S
Ft. Huachuca AZ 85613-5000
(602) 538-6622 AV 879-6622
FX 538-8787

Gary L. Stoops
Deputy Assistant Director
(Security Programs Manager)
Federal Bureau of Investigation
9th & Pennsylvania Ave., N.W.
Washington DC 20535
(202) 324-4507

Edward W. Teets, Jr.
Chief, Physical Security Support Svcs
U.S. Department of Justice
Security and Emergency Planning Staff
10th and Constitution Ave NW RM 6539
Washington DC 20530
(202) 514-4667 FX 514-4699

Carol A. Thomas
Division Security Manager
LOGICON, Inc.
222 W. 6th St.
P.O. Box 471
San Pedro CA 90733-0471
(213) 831-0611 x2835 FX 548-4870

Terry D. Tibbs
Director, Security Division
Naval Supply Systems Command
Washington DC 20376-5000
(703) 695-3655 AV 286-3655
FX 746-5697

Howard W. Timm
Program Manager
Defense Personnel Security Research
Education Center
99 Pacific St., Bldg. 455-E
Monterey CA 93940-2481

D. J. Tollstrup
Manager, Information Security
LTV MEG Missiles Division
P.O. Box 650003 MS: MSF-80
Dallas TX 75265-0003
(214) 266-9745 FX 266-1508

Neal W. Tuggle
Security Manager
Sverdrup Technology, Inc./TEAS Group
P.O. Box 1935
Eglin AFB FL 32542
(904) 678-2001 FX 729-6377

Alfred J. Veiel
Dir, Interagency OPSEC Support Staff
IOSS
6411 Ivy Lane
Greenbelt MD 20770-1405
(301) 982-2313 FX 982-2913

Frank J. Waldburger
Manager, Corporate &
International Security
Hercules Incorporated
Hercules Plaza
Wilmington DE 19894-0001
(302) 594-7122 FX 594-5471

James L. Watson
Facilities Security Regulations &
Training Manager
AT&T Bell Laboratories
1 Whippany Road, Room 4A-332
Whippany NJ 07981
(201) 386-3780 FAX 386-7368

Ronald S. Weaver
President, National Classification
Management Society
3 Creek Court
White Plains MD 20695
(703) 602-3204 AV 332-3204
FX 602-2001

Richard M. Welby, Asst Div Mgr
Security and Plant Protection
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena CA 91109-8099
(818) 354-1380 FX 354-7297

Kurt Wesley
Manager, Security Operations
General Electric Company
Military & Data Systems Operations
P.O. Box 8048
Philadelphia PA 10101
(215) 531-7340 FX 531-3509

John J. West
Security Administrator
The Boeing Company
1355 N. Atlantic Ave.
Cocoa Beach FL 32931
(407) 783-0220 x386 FX 784-2014

Martin F. Wiskoff
Senior Scientist
BDM Corporation
2600 Garden Rd., North Bldg
Monterey CA 93940
(408) 373-3073 AV 878-2448
FX 646-2041

Suzanne Wood
Researcher
Defense Personnel Security Research
Education Center
99 Pacific St., Bldg. 455-E
Monterey CA 93940-2481

William J. Yankee
Director, DoD Polygraph Institute
Building 3165
Fort McClellan AL 32605-5114
AV 865-3803

E. M. Zrodlo
Manager, Security Support Services
Lockheed Missiles and Space Company
1111 Lockheed Way
Sunnyvale CA 94089-3504
(408) 742-5791