



**May 22 and 23, 2007  
Georgetown University  
Conference Center**



# **Risk-Based Decision Making for Security Applications**

**The Future of Security Analysis**

## **Goals of the Conference:**

- ◆ Provide security analysts and risk management professionals a forum to discuss issues and best practices with peers
- ◆ Facilitate efforts to mature the profession of security analysis and risk management through consistent leadership, self-governance, collaboration, and inclusiveness
- ◆ Begin the development and execution of a comprehensive strategy to ensure the future of the profession, through the development of the next generation of security analysts and risk managers

All these goals are meant ultimately to enable better protection of the nation through more effective security investment against all man-made threats to the US national, economic and homeland security.



## DAY I

### WELCOME, STATE OF THE PROFESSION, AND VISION FOR THE FUTURE

**ED JOPECK**, FOUNDING PRESIDENT AND CHAIRMAN OF THE BOARD, SARMA

### SARMA ANTITRUST POLICY BRIEFING

**FERNANDO LAGUARDA**, MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C.

### STRATEGIC PLANNING TO IMPLEMENT SECURITY RISK ANALYSIS IN DHS

**STEVE TAYLOR** AND **STACY MARCOTT**, US DEPARTMENT OF HOMELAND SECURITY

Much of the existing body of knowledge on risk assessment and risk management was developed for issues that do not possess the same degree of complexity, uncertainty, and ambiguity as those associated with homeland security decision-making. This fact presents a significant challenge for developing a common framework to assess and consider risk as a factor when making homeland security and related public policy decisions. The discussion by representatives from Policy and Management will include an overview of the current approach within the Department for risk assessment and risk management and how the department is maturing its efforts to ensure improvement in the risk arena.

### USAF SECURITY FORCES APPLICATIONS OF SECURITY RISK ANALYSIS

**LT. COL. JIM MARRY**, US AIR FORCE SECURITY FORCES

The USAF employs an industrial security model developed during the Cold War. Efforts are underway to transform to a risk management based security model. The transformation requires shifting from resource focus to threat focus and from compliance oriented operations to effects oriented operations. Central to USAF security risk management is identifying risk tolerance and systematic planning processes to reduce risk exposure. The presentation discusses the USAF risk management model and planning processes as well as organizational consequences and challenges encountered implementing the new methods.

### RETURN-ON-SECURITY-INVESTMENT (ROSI) FOR IT SOLUTIONS

**BROOKE DAVIS LANGHORNE** AND **TODD PARKER**, SYMANTEC

Being that IT is in everything and everywhere, organizations have gained an appreciation for and accepted the fact that proper Risk Management and IT solutions can greatly increase performance, improve processes, and secure critical assets. Now the challenge is translating the operational efficiencies and process improvements into a common language that is understood by all... dollars and cents. Risk & Return-on-Security-Investment (ROSI) have become a priority for business enterprises that leads to answering questions like: How

does a business become secure? How much security is enough? How does a business know when its security level is reasonable? What is the right investment and time to invest in security? Which system components or other aspects should be targeted first? This presentation will explain ROSI for IT professionals, and help them understand the relationship between risk assessments and conducting ROSI. Together, both provide critical data in determining an organization's ROSI values for justifying IT budgets, IT Security projects, and security solutions.

### INTELLIGENCE THREAT ASSESSMENT TO SUPPORT RISK ANALYSIS

**MELISSA SMISLOVA**, DEPUTY DIRECTOR, HOMELAND INFRASTRUCTURE THREAT AND RISK ANALYSIS CENTER (HITRAC), US DEPARTMENT OF HOMELAND SECURITY

Although threat analysis is by its nature the most subjective component of the risk equation, it is an essential aspect to truly understanding risk and prioritizing protective efforts. The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) was established within DHS to bridge the gap between intelligence analysis and security analysis and to provide threat information for use in risk assessments. Ms. Smislova will review HITRAC and its role in DHS and provide insight into the challenges of threat analysis in the risk-based programs that DHS oversees.

### U.S. INTELLIGENCE COMMUNITY APPLICATIONS OF SECURITY RISK MANAGEMENT

**ROBERT GLEESON**, TECHNICAL DIRECTOR, OFFICE OF PHYSICAL SECURITY AND ASSOCIATE DIRECTOR FOR SECURITY AND COUNTERINTELLIGENCE, NATIONAL SECURITY AGENCY

While the concept of security analytical risk management (ARM) is not new and most government organizations recognize the value of applying ARM to their security programs, security managers continue to find it difficult to institute this process at the program level. Through a series of practical examples, "war stores", Mr. Gleeson will discuss how the Intelligence Community applies risk management in the security arena. These examples cover a wide range of security programs including physical security, technical security, information technology (IT) security, antiterrorism, and critical infrastructure protection. The intent of the presentation is to be both informational and motivational in that Mr. Gleeson recognizes the need to persuade security practitioners that analysis and risk management are critical skills for security professionals if the Nation is to properly balance security needs with available resources to address the dynamic threat environment of the 21<sup>st</sup> Century.

### SECURITY RISK MANAGEMENT – ONE SIZE FITS ALL?

**NANCY A. RENFROE**, PSP, DIRECTOR, SECURITY RISK MANAGEMENT, SECURITY ENGINEERING &

APPLIED SCIENCES SECTOR, APPLIED RESEARCH ASSOCIATES, INC.

Is it possible to utilize one standard security risk management assessment methodology to evaluate risk for a wide variety of facility types with diverse missions? If so, what techniques are required? What level of consistency can be achieved when the standard methodology is implemented by a large number of different assessors? This presentation will draw from lessons learned working with numerous large organizations tasked with assessing a wide variety of locations. You will gain insights into implementing a standard methodology that can still meet your specific requirements.

**LUNCH SPEAKER: THOMAS BOSSERT**, SPECIAL ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND SENIOR DIRECTOR FOR PREPAREDNESS POLICY

### THE PSYCHOLOGY OF AVOIDING DISASTER READINESS DISASTERS

**ROBIN DILLON** AND **CATHY TINSLEY**, McDONOUGH SCHOOL OF BUSINESS, GEORGETOWN UNIVERSITY

When making decisions, a rational decision maker should consider the probability of a loss, the cost of mitigating actions, the size of the loss with or without such actions, and (if relevant) the duration of the protection afforded by the mitigating actions. Then, the rational decision maker chooses actions where the expected benefits, as measured by a reduction in damage, exceed the cost of the mitigation. Costs and benefits should be discounted to consider the time value of money. How well does this framework hold for security decisions regarding terrorist events? This research examines how individuals, organizations, and communities cognitively interpret past events and currently available probability information in the context of a risk-based decision framework for disaster preparedness decisions.

### PROTECTING TOMORROW'S TECHNOLOGY TODAY

**DICK HENSON**, US ARMY G-2/ARTPC PM/ COR

This presentation will address the technology protection challenge we face today: the conundrum created by the natural tension which exists between our need to limit access to technology that could provide a competitive advantage to an adversary and our desire to cast the widest possible net in pursuit of that technology. The next topic will be finding a solution to this problem: the systematic application of a sound risk management process, the foundation of which is the identification of what *really* needs to be protected ("Crown Jewels") and the way we integrate threat and vulnerabilities to arrive at appropriate countermeasures to protect the "jewels".

### TVA / RISK VISUALIZATION METHODOLOGY

**MATTHEW ELDER**, SYMANTEC  
Symantec is involved in research with George Mason University sponsored by AFRL and HS-

ARPA to automate and improve risk identification, risk analysis, and risk visualization by integrating the GMU's artificial intelligence with Symantec's LiveState and Discovery products. GMU's artificial intelligence technology, called Topological Vulnerability Analysis (TVA), helps reason across large sets of vulnerabilities for enterprise networks. Specifically, TVA analyzes how multiple vulnerabilities spread across different machines can be combined by an attacker to reach a critical resource or high value target, to then visualize and prioritize the risks associated with such "stepping stone" attacks within large networks. Symantec's Discovery product feeds the TVA "reasoning software" with a detailed picture of the assets and configurations present on the network so that the reasoning software can best analyze real risks.

**PANEL DISCUSSION: CAREERS OUTLOOK IN SECURITY ANALYSIS AND RISK MANAGEMENT**  
MODERATOR: **ED JOECK, SARMA PRESIDENT**

**PANELISTS:**

- **Geoff French**, Senior Program Manager, CENTRA Technology Inc.
- **Lisa Bendixen**, Vice President, ICF Consulting

**THE SARMA COMMON KNOWLEDGE BASE WIKI**

**JASON ADOLPH, SRA INTERNATIONAL AND KERRY THOMAS, PWC**

A wiki is a web site anyone can edit. SARMA (with the pro bono technical assistance of SRA International) has created a wiki to collect, collaborate upon, and share information of importance to the security profession and its practitioners. The speaker will discuss how a wiki works and demonstrate the SARMA wiki site. SARMA members will also be present to discuss SARMA's planned use of the wiki for the Common Lexicon Project, and the Encyclopedia of Security Analysis Methods.

## DAY 2

**RISK-BASED DECISION MAKING FOR NAVY FACILITIES & CASE STUDY: NAVY AT/FP RISK RESOURCE ALLOCATION**

**PAT JONES, US NAVY, CNIC & ROBERT LIEBE, INNOVATIVE DECISIONS, INC.**

Commander, Navy Installations Command (CNIC) has undertaken many terrorism risk management initiatives to protect CONUS Navy facilities including the development of tools that can provide a risk-based decision aid for resource allocation at CONUS Navy installations. One recent effort, AT/FP Risk-based Decision Aid for Navy Facilities (ARDA-NF), builds upon CNIC's initiatives. ARDA-NF supports a risk analysis process that examines threat scenario likelihood, facility vulnerability, and impact of a successful attack in terms of mission loss, personnel loss, and economic loss. The presentation discusses the Navy's approach to risk-based decision making as well as

organizational consequences and challenges encountered implementing the new tools.

**MULTIYEAR RISK ANALYSIS FOR THE PORT AUTHORITY OF NY & NJ**

**JOHN PACZKOWSKI** DIRECTOR, EMERGENCY MANAGEMENT AND SECURITY, PORT AUTHORITY OF NY & NJ, AND **CHEL STROMGREN, SAIC**

The notion of risk is a core pillar of our National Strategy for Homeland Security and the National Infrastructure Protection Plan. A diversity of approaches and the absence of a common theoretical framework and professional discipline hamper the development of a coordinated approach to risk assessment and management and increases the likelihood that homeland security decision-making, investment, and operations will not be harmonized where necessary across all levels of government and the private sector. John Paczkowski and Chel Stromgren will present a look at the Port Authority's adoption of risk management practices, to include an overview of the methodology, how that methodology has since matured, and its expanded use by other agencies across the country.

**RISK ANALYSIS FOR PROTECTING THE U.S. TECHNOLOGY BASE**

**ROBERT BOWMAN, SRA INTERNATIONAL**

DIA's Defense Warning Office for Technology Transfer has been doing Risk Assessments in support of the U.S. Treasury's CFIUS process and the DoD's Defense Security Service's FOCI verifications for approximately 20 years. We generate our assessments for three primary customers: the Defense Threat Security Administration, the Defense Security Service, and the National Intelligence Council. Our methodology is classified however, this presentation will focus on, and address nine separate areas that are examined to ultimately arrive at a Risk Level.

**ANTI-TERRORISM TECHNOLOGIES, RISK OF LIABILITY, AND THE SAFETY ACT**

**BRUCE B. DAVIDSON, OFFICE OF SAFETY ACT IMPLEMENTATION, DHS**

Congress enacted the SAFETY Act following the 9/11 terrorist attacks due to concerns that companies would be discouraged from developing and deploying anti-terrorism technologies and services on the significant liability exposure they would likely face if a future act of terrorism were to occur. This legislation provides critical incentives for the development and deployment of anti-terrorism technologies and services by providing risk management and litigation management protections to providers of qualified anti-terrorism solutions. This presentation will cover the basics of the Department of Homeland Security's implementation of the SAFETY Act with a focus on relevant information for security analysis and risk management professionals. The presentation also covers the steps in the application process, including the type of information required to be submitted, the different types of protections, the process timeline, and information regarding

www.safetyact.gov. A summary of approved products and services will be included.

**HOMELAND SECURITY RISK ASSESSMENT METHODOLOGY**

**SIOBHAN O'NEIL, CONGRESSIONAL RESEARCH SERVICE**

This presentation will provide an overview of the evolution of risk assessment methodologies from the Department of Justice in FY2002 to DHS in FY2007, and then discuss the discipline of risk management and risk assessment as applied to Homeland Security Grant Program (HSGP). Terrorism risk analysis and assessment do not exist in a vacuum. Risk is analyzed and assessed as a means to mitigate or "buy down" risk over time by developing certain capabilities across the country. At DHS, the State Homeland Security Grant Program is the primary tool the agency has to influence the behavior of State and local partners to take actions that reduce what both parties agree are the risks of a terrorist attack and to respond effectively to such an attack, or other catastrophe. Regardless of the complexity of the risk assessment methodology, due to the inherent uncertainties associated with assessing risk in a dynamic counterterrorism context, some level of flexibility in managing risk may be necessary.

**SECURITY RISK ASSESSMENT MODELS**  
**CHRIS KRAHE, TSA**

Our society depends strongly on free flow of people and material. Disruption of this free flow can result in significant economic and social cost. Those who wish to harm us can achieve much of what they seek by attacking this free flow. The most prestigious part of this transportation infrastructure is commercial aviation. The elements of commercial aviation constitute high value, localized targets for our adversaries, but the impact of an attack propagates throughout the system. Our difficulty is that our adversaries can choose the timing and nature of their attack, selecting what they see as a sufficiently weak place at a sufficiently weak moment. Working against this, we as defenders must ensure that the actions we take are effective and cost efficient. This presentation will discuss an analytical approach currently being undertaken by a joint TSA/Boeing working group to address this problem.

**SECURITY RISK ANALYSIS MODELING RESEARCH AND ISSUES**

MODERATOR: **KERRY THOMAS, PRICEWATERHOUSE COOPERS**

- **Geoffrey French**, Senior Program Manager, CENTRA Technology, Inc.
- **Detlof von Winterfeldt**, Director, USC's Homeland Security Center for Risk and Economic Analysis

Security decisions must be based on threat scenario likelihoods, facility vulnerabilities, and the impacts of a successful attack in terms of mission loss, personnel loss, and economic loss. The panel will discuss challenges encountered implementing such a risk-based decision making approach.

## MAY 22, 2007

	SALON E	SALON F	CONFERENCE ROOM 5/6
8:00	Registration, Continental Breakfast in Salon D		
8:30 - 9:00	Ed Jopeak, SARMA President, Welcome, State of the Profession, and Vision for the Future		
9:00 - 9:20	SARMA Antitrust Policy Briefing, Fernando Laguarda		
9:30 - 10:45	Technical Session 1		
	Stephen Taylor and Stacy Marcott, DHS, Strategic Planning to Implement Security Risk Analysis in DHS	Lt. Colonel Jim Marry, Air Force, USAF Security Forces Applications of Security Risk Analysis	Brooke Davis Langhorne and Todd Parker, Symantec, Return-on-Security-Investment (ROSI) for IT Solutions
10:55 - 12:10	Technical Session 2		
	Melissa Smislova, DHS/HITRAC, Intelligence Threat Analysis to Support Risk Analysis	Bob Gleeson, NSA, US Intelligence Community Applications of Security Risk Management	Nancy Remfroe, ARA Services, Security Risk Management – One Size Fits All?
12:15 - 1:30	<b>Lunch, Speaker: Thomas Bossert, Special Assistant to the President for Homeland Security and Senior Director for Preparedness Policy, Salon H</b>		
1:30 - 1:45	Break		
1:45 - 3:00	Technical Session 3		
	Robin Dillon and Cathy Tinsley, Georgetown University, The Psychology of Avoiding Disaster Readiness Disasters	Dick Henson, ARMY G-2/ARTPC PM/COR, Protecting Tomorrow's Technology Today	Matthew Elder, Symantec, TVA/Risk Visualization Methodology
3:30-4:30	Panel Session		
	Career Panel, Discussion of future of risk analysis profession and market potential, Chair: Kerry Thomas, PWC Other panelists: Ed Jopeak and Lisa Bendixen	Jason Adolph, SRA International, and Kerry Thomas, PWC, The SARMA Common Knowledge Base Wiki	
4:30-6:30	<b>Reception, South Gallery, Sponsored by Price Waterhouse Coopers</b>		

## MAY 23, 2007

	SALON E	SALON F	CONFERENCE ROOM 5/6
8:00	Registration, Continental Breakfast in Salon D		
9:00 - 10:15	Technical Session 4		
	John P. Sammon, Assistant Administrator for Transportation Sector Network Management, TSA		
10:15-10:30	Break		
10:45-12:00	Technical Session 5		
	Pat Jones, CNIC & Robert Liebe, IDI, Risk-Based Decision Making for Navy Facilities + A Case Study: Navy AT/FP Risk Resource Allocation Project	John Paczkowski, Port Authority NY & NJ, and Chel Strongren, SAIC, Multiyear Risk Analysis for the Port Authority of NY & NJ	Robert Bowman, SRA International, Risk Analysis for Protecting the U.S. Technology Base
12:15 - 1:15	<b>SARMA business meeting (Box lunches provided), , Salon E</b>		
1:15 - 1:30	Break		
1:30-2:45	Technical Session 6		
	Bruce B. Davidson, Office of SAFETY Act Implementation, DHS, Anti-Terrorism Technologies, Risk of Liability, and the SAFETY Act	Siobhan O'Neil, Congressional Research Service, Homeland Security Risk Assessment Methodology	Chris Krahe, TSA, Security Risk Assessment Models
3:00-4:15	Panel Session		
	Security Risk Analysis Modeling Research and Issues, Moderator: Kerry Thomas, PriceWaterhouse Coopers, Panelists: Geoffrey French, Senior Program Manager, CENTRA Technology, Inc.; Detlof von Winterfeldt, USC CREATE		
4:15 - 4:45	<b>Closing Thoughts, Plans Forward, Salon E</b>		