



Security Analysis and Risk Management Association

JOIN SARMA  
CONTACT SARMA

[Printer Friendly](#)

## The Risk Communicator: December 2008 Edition

Welcome to The Risk Communicator, SARMA's newsletter for information, trends and issues of interest to security analysis and risk management professionals.

This complimentary news service is distributed monthly. Please feel free to share this e-mail with your colleagues and encourage them to sign up to get their own copy [here](#).



If your server is blocking HTML e-mails, you can view the current Risk Communicator by pasting the following address into your browser:  
<http://sarma.org/news/theriskcommunicato2/>

## Officers' Corner

### Change and Opportunity in the New Year

For many people, the New Year is a time to take stock, reflect on the past 12 months and take the first tentative steps towards making the next year even better than the one just passed.

Here at SARMA, we're making resolutions, too, and among them is a renewed commitment to improving communications with our membership. We hope that you'll not only be pleased with some of the changes that are in store, but that you will also take the opportunity to become part of the effort. Whether it's joining a discussion on our LinkedIn page, contributing articles to The Risk Communicator, or adding to the SARMApedia, we want 2009 to be a year of collaboration and professional growth for SARMA and all of its members.



Kerry Thomas,  
President

The most obvious change you'll soon notice is a new platform for our membership outreach and communication initiatives. Constant Contact is a well-regarded Internet publishing tool flexible enough to support a broad range of outreach activities. We're very excited about the opportunities this change offers for enhanced communication and interaction, and I encourage all

### Contents

- [Officers' Corner](#)
- [News](#)
- [Research and Analysis](#)
- [Commentary](#)
- [Members' Corner](#)
- [Key Reports](#)
- [Job Board](#)
- [Miscellaneous](#)

### Subscriptions

[Subscribe](#)  
[Unsubscribe](#)

to the Risk Communicator

### Contact SARMA

**SARMA**  
P.O. Box 710172  
Herndon, VA 20171  
Phone: (703) 635-7906  
Fax: (703) 635-7935  
E-mail: [info@sarma.org](mailto:info@sarma.org)

### Get Involved in SARMA

Get involved with SARMA today.

SARMA members to share feedback on this new software when it is fully implemented with the next issue of The Risk Communicator in January.

The move to Constant Contact also comes as we are making some changes to the newsletter itself. First and foremost, we have retained a professional journalist to oversee its production. Avi Klein, a Washington-based reporter and editor specializing in defense issues, came on board starting with the November issue, and he has already taken the bull by the horns, both in expanding our roster of contributors and by ensuring that we publish on a reliable monthly schedule. Members interested in contributing news, calendar items, research reports or other material should contact Avi via his SARMA email at [avi.klein@sarma.org](mailto:avi.klein@sarma.org).

We are also making great strides with our Common Knowledge Base project. In October, DHS released its Risk Lexicon, and we have now incorporated much of that work into our own SARMApedia. This now gives us a total of 200 terms, but there is still much work to be done. If you have glossaries, lexicons or just common understandings that arise from your assessments, methodology development or papers, please visit the [SARMApedia website](#) to add them, or contact [projects@sarma.org](mailto:projects@sarma.org) for assistance.

Finally, I hope that the New Year will also see the further growth of our LinkedIn page. We created the page earlier this year to provide a networking tool for the security analysis and risk management community, and its success to date already tells us that our members find this to be a valuable resource. We will continue to build the page throughout 2009 by adding new content and opportunities for collaboration. Don't miss out -- take the plunge and [sign up now](#).

All in all, 2009 promises to be a great year for SARMA, and I hope that you will take full advantage of the many exciting opportunities that are in store. Until then, here's wishing you a joyous holiday season and a safe and happy New Year.

Kerry Thomas  
President

## SARMA Salutes Stromgren for Service on Board of Directors

With great regret and sincere thanks for his service, SARMA's Board of Directors announces that Chel Stromgren has resigned his position on the Board in order to focus on other commitments. Stromgren, Chief Scientist for Strategic Analysis and Decision Support for SAIC, currently serves as the Principal Investigator on the DHS Port/Mass Transit Technical Assistance Program and has provided direct support to DHS in the development of terrorism risk assessment standards and methodologies.



Chel Stromgren

Stromgren first filled a mid-term SARMA Board vacancy in July 2007, and was then re-elected to a full term in May of this year. As a Board member, he

[SARMA website](#)  
[SARMApedia](#)  
[Volunteer To Serve](#)  
[Feedback / Input Form](#)  
[Join SARMA](#)

### Sponsor Notices

SARMA thanks the following organizations for their support:



### Links of Interest

[SARMA on LinkedIn](#)

[Red Team Journal](#)

[Steel City Re](#)

### The Risk Communicator

*The Risk Communicator, newsletter of SARMA, the Security Analysis and Risk Management Association*

Send questions and comments to  
Editor-in-Chief  
[newsletter@sarma.org](mailto:newsletter@sarma.org)

Copyright 2008.  
SARMA All rights reserved.

played an important role in SARMA's mission to expand and professionalize the risk management and security analysis disciplines, and his inputs and energy will be missed.

SARMA's Nominating Committee is currently considering potential candidates to fill the vacancy created by Chel's departure, and hopes to make an announcement in the near future.

[Return to the top](#)

## News

### SARMA Annual Conference Slated for June '09

SARMA is pleased to announce that the 3rd National Conference on Security Analysis and Risk Management will take place from 16-18 June 2009 at George Mason University's Arlington VA campus. The conference is the only national event organized by security risk analysts and managers for their peers in government, industry and academia.



SARMA's 2nd Annual Conference

Individuals interested in speaking at the conference and organizations interested in sponsoring the event can email the SARMA Conference Committee at [conference@sarma.org](mailto:conference@sarma.org) for additional information and submission requirements.

### Join SARMA on LinkedIn

Have you ever wished you could network more effectively with other SRM professionals? Ever wanted to ask a question, discuss an issue of interest or share a good article with your colleagues?



Now, thanks to the marvel of social networking, you can! SARMA has created an Internet discussion group that is accessible to anyone with a LinkedIn account and approval from the group manager. Join a group that is informative, professionally beneficial and fun!

To create an account, go [here](#). If you already have an account, you can go directly to the SARMA group [here](#).

See you online!

[Return to the top](#)

#### [PRIVACY POLICY](#)

The views expressed in the Risk Communicator reflect the views of their authors, and do not necessarily reflect the views of SARMA, the US Government, or the employers or clients of the contributors.

# *Research and Analysis*

## The Reputation Value of Security: Managing a Critical But Intangible Asset

*By Robert P. Liscouski and Nir Kossovsky*

During the 1992 presidential election, Democratic advisor James Carville realized he had to focus both the electorate and his candidate, Bill Clinton, on what really mattered: "Its the Economy, Stupid." Within 10 years, terrorists seeking to discredit and immobilize the United States had adopted the same strategy by attacking the World Trade Center. It was, to their minds, a perfect example of what Carl von Clausewitz called the enemy's vulnerable center of gravity. Their aims were beyond the physical collapse of the building: they wanted the entire economy to collapse along with it.

What is true about an entire economy is true about individual companies as well, and the challenges are just as significant. In an economy where reputation comprises upwards of 60 percent of the market capitalization of traded companies, the center of gravity resides somewhere within the value of the intangible assets that give rise to reputation value. These intangible assets include business processes that govern ethics and integrity, quality, safety, sustainability, innovation and, of course, security.

Of these, security is among the most volatile and unpredictable, but the rewards for successfully managing the risk are substantial. In our own experience monitoring the financial effects of reputation using an index we maintain at Steel City Re, we have observed that superior intangible asset stewards experience greater sales, net income, earnings multiples and stock price stability, and they reward shareholders with above-average equity returns.

Operationally, the primary challenge for those tasked with maximizing resilience is setting targets for management. There are no standards for what is "secure enough," no meaningful actuarial measure of threat and no framework for reasonableness of capital investment. In fact, the only certain thing is that security events, or threats of security events, can be catastrophic in terms of reputation and enterprise value.

We suggest a process comprising five steps that, as with good manufacturing practices, can't guarantee a good outcome but can improve the balance of probabilities.

### *1. Identifying the Priorities*

In every industry, companies work hard to assure customers that the goods and services delivered will meet fundamental quality standards. In the food industry, the baseline is freedom from contaminants, toxins and poisons. In the travel industry, it is a combination of customer service and personal safety. Identifying the areas where, for example, a terrorist attack will cause maximum damage to enterprise value (i.e., the center of gravity), is the first

step in effective management of risk to intangible assets.

### *2. Managing Risk in a Dynamic and Ambiguous Threat Environment*

Recognizing that risk is relative, good risk management practice calls for a rich understanding of the baseline geopolitical and criminal threat environment as those threats relate to the company's vulnerabilities. This requires senior decision-makers to stay informed about evolving threat conditions and maintain updated assessments of the company's baseline security measures and vulnerabilities. In our analysis of the business processes underlying reputation, we group them into three broad categories: people processes, physical processes and cyber processes.

### *3. Ensuring Organizational Commitment*

As with other matters that speak to enterprise value, an organization must engage its leadership at the board and "C" levels. Within this leadership, two cultural values must flow through the organization. The first is a culture of communication. Those at the tactical level closest to threat data must understand that they are empowered to question security assumptions.

The second is a culture of action. One never possesses sufficient information, and those empowered to act need to be willing and able to act on the basis of information available. As Clausewitz noted, "It is even better to act quickly and err than to hesitate until the time of action is past."

### *4. Making the Case for Initial and Ongoing Investments*

The business case for risk mitigation and insurance to protect enterprise value against catastrophic security risk may not conform to a conventional return-on-investment analysis. But it will create measurable changes in operating profit, net income, earnings multiples and stock price stability. Moreover, in the absence of reasonable efforts, liability falls squarely on those charged with corporate governance -- affirming the principle that catastrophic risk management is a core strategic concern.

In these challenging economic times, companies will be tempted to reduce spending in areas where they perceive that no immediate value is likely to be realized. Security costs are typically viewed as an expense, not an investment to maintaining value. This is often not as much a fault of the company as it may be the failure of those responsible for security to make the business case to senior management that security is an enterprise-wide intangible asset that creates measurable value. Tying security investment to shareholder value is clearly a way to make that business case.

### *5. Battling Complacency*

The continued absence of a catastrophic event may lead to a lack of focus and appreciation of the magnitude of the ongoing risk. The single most effective means of combating complacency is to conform to good practices and ensure the periodic board-level examination of risk management processes.

To conclude, in most traded companies, the buck stops with the CEO and the board of directors. In companies where intangible assets comprise a material fraction of the market capitalization, shareholders reasonably expect that the

company will have in place systems to assure the optimal management of those assets, and resilience should those assets be impaired. Controls and related processes can be an important part of good practice standards and reduce the variance associated with asset management and the related risks. As James Carville might say today, "It's the reputation, stupid."

*Robert P. Liscouski and Nir Kossovsky are, respectively, Senior Vice President and Chief Executive of Steel City Re, a firm focused on corporate reputation protection. This article is adapted from an updated version of "The Intangible Value of Security in a Volatile Global Economy," Intellectual Asset Management 24 (2007): 49-52, reproduced in Critical Infrastructure Protection: Elements of Risk, George Mason University School of Law Critical Infrastructure Security Program monograph (December 2007): 93.*

[Return to the top](#)

## Commentary

### Anticipating the Future: The Use and Utility of Red Teaming

By Mark Mateski

Can red teaming and alternative analysis help decision-makers anticipate events? As you might expect, the answer is not a simple "yes" or "no."

First, anticipating events is extremely difficult, and most analysts -- futurists included -- will tend to caveat their work heavily. This is partly due to the limitations inherent in every analytical technique, and partly due to the analyst's natural reluctance to leap at long shots. While this can lead to muffled insights and recommendations, it also helps avoid spectacular mistakes.

Qualitative analysis is often best suited to address human-driven complexity, but qualitative approaches generally sacrifice analytical precision for flexibility and descriptive power. Scenarios in particular are susceptible to problems related to the [conjunction fallacy](#), and a persuasive narrative can actually lead a decision-maker to misperceive risk. Quantitative analysis, on the other hand, gains in precision but often obscures its workings behind a curtain of formulas and algorithms, in many cases reducing a decision-maker's willingness to trust the results.

Second, analysis is not an all-or-nothing proposition. An analyst, for example, might predict one element of an event but fail to anticipate others, and the value of the anticipated element is certain to vary by context. Further, getting a foundational element wrong will often preclude getting a dependent element right.

The following model defines the various elements of anticipation and their relationships. It's a rough, back-of-the-envelope sketch, but it helps clarify the challenge.

1. Strategic elements form the foundation. I loosely characterize these elements as the 'who' and the 'why'. Examples of specific elements at this level include an opponent's goals, preferences and perhaps even depth and breadth of resources.

2. Operational elements come next and build on the foundation of strategic elements. I characterize the operational elements as the 'how' and the 'what'. Examples of elements at this level include the method of attack, the class of target and the opponent's technological capability.

3. Tactical elements come last and build on the foundation of strategic and operational elements. I roughly characterize the tactical elements as the 'when' and the 'where'. They also include the specific 'who' -- the individuals who execute the event. Examples of elements at this level include the time and place of the event.

What does this simple model imply? Foremost, it suggests that a red team will probably not anticipate elements of a higher level correctly if it misreads elements of a lower level. Conversely, a red team that correctly identifies elements of a lower level is more likely to anticipate elements of a higher level. For example, a team that correctly interprets an opponent's goals and preferences is more likely to anticipate the target and method of an attack. It is also worth noting that successful anticipation becomes more difficult at higher levels; in fact, it is arguable whether a red team or analyst can anticipate the tactical elements based on analysis alone.

A spin-off benefit of the model is that it provides a shorthand heuristic for describing levels of surprise. Using this model, a strategic surprise occurs when an analyst or decision-maker fails to anticipate all levels before an event; an operational surprise occurs when an analyst or decision-maker anticipates the who and the why but fails to anticipate the what, how, when and where; and a tactical surprise occurs when the analyst or decision-maker anticipates the who, why, what and how but fails to anticipate the when and the where. As always, the analyst should never overlook the possibility of deception. Successful deception at the strategic and operational levels is almost certain to enable a strong surprise.

Finally, the value of anticipatory analysis must be measured in concert with the function of intelligence collection. Even though standalone analysis is not likely to anticipate the tactical elements of the model above, good analysis at the strategic level can point intelligence collection toward the operational and tactical elements of the model. In other words, an analyst may never be able to anticipate the when and where of an unlikely event, but he or she might be able to identify the what and how with enough confidence to tip collectors to the domain of the where and the when.

*Mark Mateski is the Founder and Managing Editor of Red Team Journal ([www.redteamjournal.com](http://www.redteamjournal.com)), where this article was first published. He currently consults and teaches systems analysis and system engineering part-time.*

[Return to the top](#)

## *Members' Corner*

### SARMA Members Needed for RM Survey

Want to contribute your thoughts to an ongoing risk management study? Dr. Robin Dillon-Merrill, an Associate Professor in the McDonough School of Business at Georgetown University and a founding director of SARMA, is looking for volunteers to complete a short survey for her research on crisis decision-making.

Dr. Dillon-Merrill has studied risk analysis for over 15 years, with much of her research sponsored by NASA and the National Science Foundation. The focus of her current work is the study of the factors that affect decision-making during natural and man-made disasters.

Those interested in participating can follow the link below to the five-minute survey. Dr. Dillon-Merrill will provide a report on her findings (including data) in the January issue of *The Risk Communicator*.

[http://www.surveymonkey.com/s.aspx?  
sm=dzPldXGnTX\\_2bcWJ8Dz36g1g\\_3d\\_3d](http://www.surveymonkey.com/s.aspx?sm=dzPldXGnTX_2bcWJ8Dz36g1g_3d_3d)

Participants who share their e-mail address will be entered into a drawing to win a Georgetown University sweatshirt. E-mails will be discarded after the drawing and are not connected to survey responses.

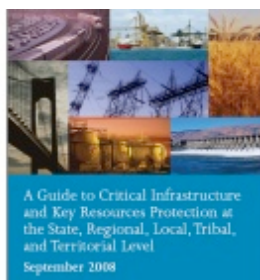
To learn more about the research project itself, or ask questions, please contact Dr. Dillon-Merrill at [RLD9@Georgetown.edu](mailto:RLD9@Georgetown.edu).

[Return to the top](#)

## *Key Reports*

### A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level

This September 2008 report from DHS contains a lengthy discussion of using the Risk Management Framework to develop a resources protection plan. Text includes a detailed look at the intent and suggested content of each section of a local, state or tribal CIKR



protection plan.

[\[Get the Report\]](#)

## Forging a New Shield

In this November 2008 report, the Project on National Security Reform calls for the creation of the position of director of national security, one of whose responsibilities would be to prioritize objectives and establish risk management criteria for executive branch decision-making.



[\[Get the Report\]](#)

## Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat

Brian Jackson of the RAND Corporation argues in this recently released 2008 report that "[i]nstead of seeing an either/or choice between traditional prevention and mitigation or resiliency measures, it is more productive to consider them together in an integrated way -- as two complementary elements of a strategy aimed at lessening the consequences of successful terrorist attacks."



[\[Get the Report\]](#)

## Terrorism Insurance: Status of Coverage Availability for Attacks Involving Nuclear, Biological, Chemical or Radiological Weapons

A broad survey of the insurance industry by the GAO finds that property/casualty insurers still generally seek to exclude such coverage from their commercial policies by relying on long-standing standard exclusions for nuclear and pollution risks. The December 2008 report also discusses two proposed remedies -- to either require coverage for terrorism losses, or for the federal government to insure all such losses itself.



[\[Get the Report\]](#)

[Return to the top](#)

## **Job Board**

### **Management and Program Analyst (Risk Analyst)**

National Protection and Programs Directorate

Vacancy Ann.#: DSHQRA08-5147

Who May Apply: Public

Pay Plan: GS-0343-13/15

Appointment Term: Permanent

Job Status: Full-Time

Opening Date: 7/18/2008

Closing Date: 12/31/2008

Salary: From 82,961.00 to 149,000.00 USD per year [[View the Announcement](#)]

### **Management and Program Analyst (Strategic Risk Specialist)**

National Protection and Programs Directorate

Vacancy Ann.#: DSHQRA08-5146

Who May Apply: Public

Pay Plan: GS-0343-11/13

Appointment Term: Permanent

Job Status: Full-Time

Opening Date: 7/18/2008

Closing Date: 12/31/2008

Salary: From 58,206.00 to 107,854.00 USD per year [[View the Announcement](#)]

### **Management and Program Analyst (Risk Analyst)**

National Protection and Programs Directorate

Vacancy Ann.#: DSHQRA08-5175

Who May Apply: Public

Pay Plan: GS-0343-9/11

Appointment Term: Permanent

Job Status: Full-Time

Opening Date: 7/28/2008

Closing Date: 12/31/2008

Salary: From 48,108.00 to 75,669.00 USD per year [[View the Announcement](#)]

### **Management and Program Analyst (Risk Analyst)**

National Protection and Programs Directorate

Vacancy Ann.#: DSHQRA09-6009

Who May Apply: Public

Pay Plan: GS-0343-11/13

Appointment Term: Permanent

Job Status: Full-Time

Opening Date: 10/16/2008

Closing Date: 12/31/2008

Salary: From 58,206.00 to 107,854.00 USD per year [[View the](#)

[Announcement](#)]

[Return to the top](#)

## *Miscellaneous*

Want to Contribute to The Risk Communicator?

Do you know of an item you would like to see included in The Risk Communicator? Do you have ideas for new and interesting features for future editions? If so, please contact the newsletter staff at [newsletter@sarma.org](mailto:newsletter@sarma.org).

[Return to the top](#)