2010

June 14-17 | New York City

GLOBAL ROUNDTABLE

GLOBAL ROUNDTABLE

Summary of Insights, Strategies & Action Items

Proceedings of the International Public-Private Preparedness Summit

Summary of Insights, Strategies & Action Items

Proceedings of the International Public-Private Preparedness Summit

June 14-17, 2010 – New York City

International Center for Enterprise Preparedness
New York University

William G. Raisch, MBA– Director
Karen Coyne
Margaret Della
Carol Shields
Emily Raisch

NYU's International Center for Enterprise Preparedness (InterCEP) maintains a global outreach as the first academic center dedicated to private sector emergency preparedness and risk management. InterCEP is a program of the university-wide Center for Catastrophe Preparedness & Response (CCPR). Founded in 1831, New York University is one of the world's largest private universities. The University, which includes 14 schools and colleges, occupies six major centers in New York and has additional facilities worldwide.

285 Mercer Street, 4th Floor, New York, NY 10003, USA | 01.212.998.2000 | www.nyu.edu/intercep

Contents

EXECUTIVE SUMMARY

The International Public-Private Preparedness Summit was held June 14-17, 2010 at New York University in New York City. This document summarizes the proceedings, highlighting important themes and developments. Summit participants included sixty-six public and private sector leaders representing fifty-five different organizations from the United States, the United Kingdom, the Netherlands, Italy, Belgium and Japan. These participants engaged in a series of facilitated roundtable discussions, focusing on the following themes:

Recent Events – Lessons Learned, Strategies Going Forward

Times Square Bomb, Iceland Volcano, Border Security and Violent Operating Climates

This roundtable investigated how the Times Square Bomb illustrates the changing face of terrorism, and how firms located in high-value target areas assess and mitigate their risk. Security risk in a global trading and manufacturing market was also discussed and the related need for flexible planning for unforeseen emergencies. The Iceland volcano eruption as well as the U.S./Mexican border were examined as illustrations of the diverse range of disruptions that can impact an organization.

Challenges in Risk and Resilience and the Asian Operating Environment

This roundtable discussed strategic and tactical approaches to resilience and security. Challenges inherent in operating enterprises in India and China were discussed.

Cyber-Security Threats: Challenges & Strategies

This roundtable focused on the economics of cyber risk, the misalignment of incentives and the causal factors and risk to intellectual property as well as the emerging threats posed by cloud computing. Participants emphasized the need to document and share best practices while standards are being developed.

Key Strategies to Realize Value in Risk & Resilience

The Argument for Investment in Risk Management & Resilience, Enterprise Risk Management, Certifying Private Sector Preparedness

This roundtable discussed the benefits of risk management for an enterprise including one firm's experience with standard adoption and certification.

Supply Chain Risk Management (SCRM) & Related Issues

This roundtable discussed the risks in supply chains in an increasingly global economy where seemingly localized events such as the Icelandic Volcano eruption have worldwide impacts on all aspects of supply chains. Also discussed were the impacts and challenges of counterfeiting and gray market products.

Identifying What Works & Doesn't Work in Public-Private Collaboration

Structures and Strategies for Partnering on Information, Resources and Joint Action – Parts I & II

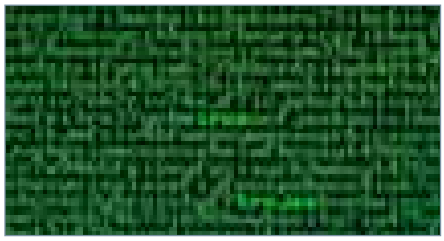
These roundtables focused on public/private collaboration, existing structures and outreach efforts, with a look at different platforms, strategies and approaches to collaboration.

Prioritizing Common Issues & Organizing to Develop Targeted Solutions

This roundtable focused on reflecting on the Summit discourse and identifying common problems that could be addressed collaboratively with the goal of developing concrete solutions to them. The Global Roundtable has a history of organizing core groups of its members (Task Forces) who serve as catalysts with other stakeholders in identifying and advancing

actionable strategies to impact targeted issues. Areas for potential common action included:

1. A global solution for supply chain integrity/counterfeiting.
2. Actionable strategies for cyber security and a compelling business case in support of them.
3. A global knowledge base on public-private collaboration in risk management and a platform to advance collaboration between the public and private sectors internationally.



BACKGROUND

The International Public-Private Preparedness Summit

The International Public-Private Preparedness Summit was organized by the International Center for Enterprise Preparedness (InterCEP) at New York University (NYU), the world's first major academic center dedicated to private sector preparedness. In recognition of the fact that societal security and preparedness for major disruptive events depends on the interface between the public and private sectors, InterCEP created the Summit to promote public-private cooperation in emergencies and to enable international sharing of preparedness strategies and best practices. InterCEP chose a roundtable discussion format to encourage dialogue as well as foster critical relationships among leaders with significant global responsibilities. Summit participants included key executives from Global 1000 companies, national, regional and major metropolitan governments, as well as key international non-governmental organizations.

The Global Roundtable

The Global Roundtable is a body of professionals dedicated to improving overall societal security, resilience and emergency preparedness. It serves as the advisory body for InterCEP at New York University. The Roundtable is comprised of members from both the public and private sectors. Members come from a diversity of resilience and risk management arenas including operational risk management, security, emergency management, business continuity, crisis management, disaster recovery, corporate resilience, civil defense, military, intelligence and law enforcement. InterCEP convened the Global Roundtable to identify and analyze key issues, develop potential solution strategies and, where appropriate, participate in the implementation of these strategies.

Method

This document presents a summary of the proceedings of the International Public-Private Preparedness Summit, held June 14-17, 2010 at New York University in New York City. In the interest of promoting frank discussion, all comments made during Summit roundtables were not-for-attribution with the exception of the remarks of keynote speakers which are reproduced in abridged, summary form. The proceedings presented here derive from transcribed, anonymized recordings of the roundtables and participant-observation notes taken by InterCEP staff. We have taken care to exclude any information that may potentially be confidential to those individuals and organizations that were present. At the same time, we have tried to capture insights and strategies offered in the discussion that will serve as a ready reference for those who attended the summit as well as benefit those individuals and organizations that did not attend. No effort has been made by InterCEP to validate statements made by participants.

KEYNOTE ADDRESS

Joe Petro
Managing Director, Security and Investigative Services, Citigroup

Joe Petro, Managing Director, Security and Investigative Services for Citigroup, gave a breakfast keynote address at this year's Summit.

SUMMARY

In his keynote address, Petro spoke of experiences and lessons learned from Citigroup's rescue of employees and recovery of operations after January 2010's devastating earthquake in Haiti.

The Earthquake in Haiti was Citigroup's first opportunity to implement crisis management plans developed after 9/11.

The Earthquake in Haiti was Citigroup's first opportunity to implement crisis management plans developed after 9/11. Citigroup has detailed, very explicit and practiced crisis plans. We learned in Haiti that [the crisis plan] didn't matter all that much in the final analysis. What really made a difference in Haiti were the people who executed that plan, their ingenuity, resilience, resourcefulness and courage. Our operation in Haiti was small: forty-three employees operating in one three-story building. I did not have any security staff in Haiti– our staff in Puerto Rico had oversight for security and investigations, so we had no one on the ground.

Lack of communications and reliable information was a critical issue.

One of our employees jumped out of a third story building and was able to make a ten second call to our command center to inform them that our building had just collapsed. After that we had really no information about the conditions on the ground except what we saw on CNN. We had to make some very quick decisions based on very partial information. First we selected a team –not only was the Puerto Rico team closest, but fortunately its three members were all Army National Guard. These staff members were prepared and well trained to go into an environment like Haiti.

Cash was our highest-priority item to take into Haiti.

The Puerto Rican team took a supply of U.S. currency (in cash) with them. The team landed in Port-au-Prince airport 14 hours after the earthquake occurred and it was bedlam. Immediately the team found someone who spoke English and paid him to act as an interpreter. The team rented five rooms in a hotel, which they used as a base of operations.

The physical site had to be secured.

When the team arrived at the site the next day, there were hundreds of people crawling all over the ruins because there were valuables and money inside. The team hired a couple of Haitian policemen armed with shotguns to clear the site. Through incredible resourcefulness and use of cash they were able to obtain machinery and fuel and hire local workers. Having obtained these assets, we were able to dig through the rubble and rescue three of our staff. Afterwards, with the help of special equipment it was determined that although five people were still missing, there was no one left alive in the building.

Command center was set up and communications protocol established.

The center of all relief efforts was set up in Santo Domingo, Dominican Republic, where Citigroup has a business office. Our security team used the local business offices as the base of operations. All supplies, equipment, manpower were funneled through there, as Haiti's airport was a mess. We sent trucks filled with supplies at the back of UN convoys. To each of our families we distributed a tent, generator, food, emergency equipment and other necessary supplies. Two doctors from a Mexican rescue team provided medical care to our employees. As communications began to normalize, our relief workers began to get numerous calls from senior management. This became problematic as our team was very busy with recovery operations and could not afford to be on the phone all the time briefing management. We told senior management there would be no phone calls to Haiti- all phone calls must go to the command center. We set up calls between the command post and senior management for daily briefings. The command post prepared replacement rescue teams, coordinated purchase and procurement of supplies and largely managed day-to-day operations.

Information Security Nightmare.

Bank documents were strewn all over the site. People were going through the documents looking for anything that could be worth money. We were able to remove hard drives from the servers and our e-crimes labs were able to recover most of our databases containing our customer information. We hired local Haitians to collect all the documents and put them in trash bags. They collected over 1,000 bags. Looters were another problem, constantly in the building looking for things of value.

Within ten days we were able to resume our operations.

Scotia Bank gave us a teller position, which allowed us to resume banking operations in Haiti. The original COB (continuity of business) site was unusable because it was on the third floor and our people refused to go to the third floor, even though engineers had certified it as structurally sound. We implemented a new site and transferred all support responsibilities back to the business managers after about fourteen days.

We had five employees that were killed, several employees injured and nine evacuated to the Dominican Republic. Eleven of our employees lost their homes and thirty-two employees needed medical attention. We took in thirteen tons of equipment and supplies over the approximately two-week period and rotated about fifteen of our security staff in and out of the Dominican Republic.

Lessons Learned from Haiti Disaster.

- Communications problems were a huge issue. We have since purchased more satellite phones and distributed them around the world.
- Ensure that a COB site is chosen that is actually usable and functional for its intended purposes under the direst circumstances.
- Establish a call tree arrangement ahead of time to keep employees and upper management informed without impeding the people on the ground conducting the operation.
- Conduct routine risk assessments and follow up. We had an emergency exit stairwell installed after such an assessment (despite initial concerns as to the cost). During the earthquake a dozen of our people escaped via this stairway.

GLOBAL ROUNDTABLE ONE

Recent Events – Lessons Learned, Strategies Going Forward

Times Square Car Bomb, Iceland Volcano, Border Security and Violent Working Climates

Overview

This roundtable discussed how the Times Square Bomb illustrates the changing face of terrorism, and how firms located in high-value target areas assess and mitigate their risk. Security risk in a global trading and manufacturing market was also discussed and the related need for flexible planning for unforeseen emergencies. The Iceland volcano eruption as well as the U.S./Mexican border were examined as illustrations of the diverse range of disruptions that can impact an organization.

> "Terrorism as a whole, whether organizations like Al Qaida or inspired by Al Qaida, has shifted to smaller and more independent operations, much like you saw on Times Square, [compared with] the larger, more well coordinated and orchestrated events [such as 9/11]."

"We've seen a change in the way terrorists do business."

Participants agreed that this year's Times Square bombing incident illustrated the dynamic nature of terrorism, both in local and global terms. While terrorism is a centuries-old concept, the attacks on September 11th were many people's first exposure to terrorism. The 9-11 attacks were very well coordinated, consisting of several orchestrated attacks launched from multiple cities that took years to plan. This is not, however, representative of the majority of present day terrorist threats.

Attendees noted that terrorism as a whole, whether actually executed by organizations like Al Qaida or inspired by them, has shifted to small and more independent operations, much like what was seen at Times Square. This was contrasted to the larger, more well coordinated and orchestrated events such as 9/11. Often, there is no communication or coordination with senior leadership and once the training

> "Talk to Scotland Yard and ask them if they would have anticipated a bunch of doctors were going to try and burn down Glasgow Airport."

cycle has been completed the individual travels to the site of a planned attack.

As one participant explained, "the attacks are often very low tech, not elaborate schemes or devices, and involve very minimal planning for the attack. Materials used, whether explosives or weapons, are normally locally obtained and for the most part legally obtained. "In the event these small operations fail, the terrorists' back-up plan may be simply to obtain a weapon and attempt to kill as many people as possible in a crowded area.

Participants pointed out that once individuals are in what is often called a "threat country" (Afghanistan, Pakistan, Yemen, Saudi Arabia, etc.) it is hard to track their movements, particularly because tens of thousands of people travel back and forth between these countries. Some terrorists targeting the U.S. may have family ties in Pakistan or Afghanistan, making travel between those countries and the U.S. unremarkable. It's particularly difficult to establish a profile that fits any potential threat because of the evolving nature of terrorists and terrorism. "Talk to Scotland Yard," explained one participant, "and ask them if they would have anticipated a bunch of doctors were going to try and burn down Glasgow Airport."

> Technology is not necessarily our friend.

Media leaks and communications-"Feeding the Beast" in emergencies.

Participants agreed that "Technology is not necessarily our friend" in that it facilitates access to and by the media during emergencies. In one recent highly publicized investigation, media leaks hampered the apprehension of the perpetrator, as he was well aware of actions to locate him because these actions were publicized on TV, the radio and the Internet.

Furthermore, today we are accustomed to getting information almost immediately and thus senior management often demands constant updating. Participants described this "insatiable search for information" as "feeding the beast". During one particular event, a participant related that the demand for information by outside sources reached "a point where in our joint operations center I detailed individuals whose sole job was to feed the beast. This is a common problem and a concern for all of us." Compounding the problem is the fact that in emergencies, the first information released is often largely incorrect.

> The Times Square bombing has a positive impact in that "it has given us the impetus to make sure that our plans are fresh and remain ready and actionable when the time occurs and that the people who have to execute those plans are prepared to do so.

One participant pointed out, "It's difficult when you're getting leaks, as happened in Times Square, because then there is absolute frustration at the top of an organization because they see on the news more than they are being told by their own staff because the information hasn't yet been confirmed properly. And that disparity causes an enormous amount of tension".

Even "failed" terrorist attacks succeed in some ways.

While many perceive the Times Square and the Christmas Day attempted bombing on a Northwest flight as failed attacks, participants noted that at the end of the day, the events can be looked upon as at least partial successes by terrorists and clear failures of intelligence. While in both instances there was no loss of life and terrorists were apprehended afterwards, neither event was prevented by intelligence efforts or formal security precautions.

"The attack on Christmas Day was a success in many ways in that it bypassed and was able to penetrate what we like to consider our most secure means of transportation (air flight) despite the fact that anybody who's flown lately can attest how difficult it is to fly because of all the security. Additionally, "during the Times Square incident, the attacker bypassed our trip wires, our security and initiated a device and it's only the failure of that device that saved a lot of lives. Quick action by those on the scene, the police, bystanders and the fire department prevented any further damage."

Another participant noted that while, "the bomb didn't go off, the success occurred when the notoriety occurred. The success occurred because the terrorist was among us, he lived among us, he thrived among us, and he was able to secrete himself in a way that was necessary for him to plot this and execute it."

> "...Even if the bomb doesn't go off, we're forced to close another freedom and they perceive that as being a success."

Despite this, there are preparedness successes that counterbalance that failure. "We've been hearing since 9/11, 'if you see something, say something.' Well, there's no better example than the street vendors who reacted to that truck sitting there. It was a matter of seconds after the truck was parked and the terrorist walked away before somebody came and said 'Hey, we got to take care of this. This isn't right."

Participants stressed the difficulty of creating security measures to combat constantly changing threats. Participants agreed that attacks across the globe over the last few years show an incredible variety of tactics and approaches. "The face of terrorism, the enemy that we fight changes. Their tactics evolve to counteract our successes, and this is, literally, the long war, a never ending battle." Furthermore, as new security measures are created, "terrorists are constantly trying to find the areas where we haven't closed loopholes, and attack them. They are looking for our susceptibilities, and even if the bomb doesn't go off, we're forced to close off another freedom and they perceive that as being a success."

Times Square was an attractive target for several reasons.

One participant noted that while the iconic World Trade Center was destroyed, "that doesn't mean that there aren't other iconic targets" in New York City. Further, he noted that Wall Street has become a very hardened area, the midtown area may be perceived as "not quite as hard... except on New Year's Eve." Furthermore, he noted "You've also got major media there – probably can't have an event occur with more cameras focused on it anywhere in the world than in Times Square. Times Square also represents commercialism, consumerism, and to some extent, more historically than currently, hedonism. These are all things that radical fundamentalists would point to as the reasons why the west must fall."

> "You don't have to be the target, you just have to be in the neighborhood."

The firm itself need not be the target to be at risk.

One participant discussed the challenges of having business headquarters located in areas such as Times Square. An organization may have thousands of employees and the predominance of its executive leadership in a single location. While the firm may not view its particular business or brand name as having iconic value for terrorists, he emphasized that "you don't have to be the target; you just have to be in the neighborhood."

One firm recognized the target value of Times Square several years earlier after a 'parcel bombing' involving a cyclist tossing a bomb in front of the military recruiting station very early in the morning. While there was no loss of life, this event was a "wake-up call" according to one participant.

After recognizing vulnerability, what steps should be taken by a firm?

After recognizing vulnerability, it was suggested that the first step a firm should take is to ensure that its building offers protection in case of an attack. One participant noted that its building controls airflow so that in the event of an attack with radiological or chemical weapons "we can shut the air intake down almost immediately". Additionally, there is no exchange of air with the subway or train stations underneath the building and "the infrastructure of our building is in no way attached to the train stations that run underneath us. Those were conscious design goals when the building was built." Furthermore, he noted that the building is wrapped in a Mylar film, which, in the event of a blast, will keep the blast from creating flying shards of glass, which "are the projectiles that cause the most injury. In Oklahoma City for instance, most of the people who died there died from flying glass, not from falling concrete or other things like that."

Even after making a building more structurally secure, an organization has to consider the mentality of staff members as a possible vulnerability. One participant offered that many of the people working in his building were in the city when 9/11 occurred and a certain percentage of them "simply don't want to talk about it. They don't want to have anything to remind them that it occurred down the street." This mindset can be counter-productive when trying to prepare people to be ready for an emergency. For some firms, especially those in New York City, the Times Square bombing attempt had a positive impact in that it clarified a real and present threat and thereby provided "the impetus to make sure that our plans are fresh and remain ready and actionable when the time occurs and that the people who have to execute those plans are prepared to do so."

> Eighty percent of Mexico's exports come to the U.S. and 50% of Mexico's imports come from the U.S. Mexico is our second largest source of foreign petroleum. The U.S. is the biggest foreign investor in Mexico.

U.S. border security and the high risk operating environment in Mexico.

The U.S.-Mexico border was described by one participant as the busiest, most economically important border in the world with roughly one million legitimate travelers and a billion dollars of goods transiting the border each day. According to the participant, "Eighty percent of Mexico's exports come to the U.S. and 50% of Mexico's imports come from the U.S. Mexico is our second largest source of foreign petroleum. The U.S. is the biggest foreign investor in Mexico." It is estimated that over the next five years, U.S. corporations will invest 115 billion dollars in Mexico and for many businesses "there is a business imperative to operate in Mexico. If you do not operate in Mexico then your competitor will."

However, the operating environment can be extremely problematic. In addition to legitimate trade between the U.S. and Mexico, the narcotics trade between the two countries is estimated to range from forty to sixty billion dollars a year. Efforts to stem the drug trade have included the "war on drugs," an offensive against the illegal drug community declared by Mexico's President Calderon in 2006. While over 50,000 Mexican troops deployed in this effort, cartel bosses have fought hard to maintain power. As one participant noted, "If you were the head of a forty to sixty billion dollar a year industry, you would fight pretty hard to maintain that" and to date, there have been 24,000 drug-related deaths, extreme brutality and violence in Mexico.

Violence includes not only clashes between the government and drug cartels but also among competing cartels as well. Participants agreed that there is a businesslike manner in which these organizations, be they termed drug cartels, organized crime or terrorists, operate. They should not be underestimated, as many are not crude undertakings, but rather very organized entities and sophisticated, dangerous adversaries.

Gray ash and global impact – The Icelandic Volcano.

A participant from a firm that was extensively impacted from the recent Icelandic volcano eruption described this event as his firm's black swan in that it was an unforeseeable, game-changing event. "Imagine," he proposed, "the preposterousness of telling supply chain, customer operations or finance executives that the presence of a sheet of ice on a remote mountain at the 64th parallel would impact seven million travelers, cripple the airline industry, impact European and other economies, cost the firm tens of millions of dollars and cause cruise ships in Bermuda and Mexico to lose revenue."

In Iceland on March 20th, the initial volcano erupted with no real significant impact. Later on April 14th, the main Icelandic volcano erupted. This time the ice covering the mountain increased pressure on the water vapor and shot ash several miles into the air. This eruption had global consequences.

During the following days northern European airspace was closed and by April 17th, twenty countries had full or partial airspace closures. By April 18th, 80% of European airspace was impacted in some way and 6.8 million travelers had been affected. The impact reached far beyond holiday and business travelers. According to one participant, "U.K. troop movements out of Afghanistan were affected because how do you get troops out of a war zone, you typically fly them home." However, restricted air space proved problematic.

Participants agreed that a key problem in planning for risks like this is that "we base our planning and operational management on empirical and predictive strategies and events like this often originate outside our systemic perspective, outside our thinking."

Value of planning for impacts not necessarily scenarios.

The consensus was that the best preparation is introducing new systems, controls and measures that allow for the contemplation of these kind of game-changing, unforeseeable events. At the very least, it was agreed that it is possible to prepare for potential impacts of a

> A plan must be "…a balance between writing a cookbook and writing a football playbook. You may not be able to plan every step like you would in a cookbook, but if in general you know where you want to go like in a playbook then you'll get there.

wide range of scenarios if not for the scenario itself.

A well thought out continuity of operations plan can be utilized effectively for unanticipated scenarios, such as the volcanic eruption in Iceland. Such a plan must be, "…a balance between writing a cookbook and writing a football playbook. You may not be able to plan every step like you would in a cookbook, but if in general you know where you want to go like in a playbook then you'll get there."

An executive from a firm with thousands of suppliers (including several hundred single-source suppliers) indicated that sound business continuity plans could be adapted to respond to the unexpected. "When the Icelandic volcano erupted we had about 2,000 employees that were affected via travel plans, but that was not what put the red flag up for us. What did was that with a quarter of the world's shipping completely shut down we had several hundreds of millions of dollars in parts and equipment sitting on runways, sitting in factories, sitting at Fed-Ex locations that were not moving. Of course, we did not have a written volcano eruption business continuity plan. We did, however have a plan for a pandemic. In that plan there was a scenario in case of global travel shut down to contain the spread of the pandemic. So we dusted off that plan and actually used it to run through the situation for the volcano. In there was a playbook on what we do to re-route flights, to charter flights and that's really what we used. We survived that event with minimal disruptions. The consumer never really saw anything and luckily Wall Street didn't see anything to be concerned about either."

> "The problem is that we haven't come up with a good mechanism to analyze the economics of cyber security."

GLOBAL ROUNDTABLE TWO

Challenges in Risk and Resilience and the Asian Operating Environment

Overview

This roundtable discussed strategic and tactical approaches to resilience and security. Challenges inherent in operating enterprises in India and China were discussed.

Four key security challenges in operating in India and China

Businesses operating in India and China have noted four significant security challenges while operating there:

1. Physical Security,
2. Safeguarding Intellectual Property,
3. Corruption and
4. Cyber-Security.

According to participants, each situation had to be evaluated differently with consideration given to local customs and operating environment. In India typical measures to ensure physical security (including the presence of security guards) were felt to be largely inadequate because neither the host country nor many multi-nationals operating there perceive physical security as a problem worth addressing. They are unwilling to pay for good security and, as one participant noted, "You have to do it yourself." In China, "locking up" in the physical sense is second nature, and businesses have fewer reasons to be concerned about physical security.

In terms of safeguarding intellectual property, India is a safer environment for businesses, as its economy is focused on services and not manufacturing (thus removing much of the incentive for this kind of crime). If, however, your business carries intellectual property into China, participants advanced that they

> "In identifying potentially corrupt employees, "…One can build a fairly accurate financial picture of somebody's financial state. For example, seeing how many vehicles are registered in a person's name, how many houses they or their family own, and if that person is earning a thousand dollars a month how is it that he's driving a Lamborghini."

> We are seeing changes as a result of partnerships in the public/private sector with Indian authorities across the whole of India and it's building momentum. So those historical resistances and obstacles are beginning to be broken down.

will, "…penetrate your organization. They'll hack your systems, and they're very, very good at it."

Corruption is another concern for businesses operating in China. While corruption is also a problem in India and most emerging markets, many consider it the single largest problem facing China today. Participants noted that as China's size and economic growth have accelerated," so have all the risks that go with them." Additionally, China's size and ties to the global economy mean that local problems quickly go worldwide. Recent examples cited included counterfeiting, intellectual property theft, defective toys sold in the US and Europe and food scandals. Recently, a contaminated batch of melamine, a chemical added to dairy products within China, spread to New Zealand dairies as well, creating an international scandal.

Finally, cyber security presents a global risk that is both growing and difficult to quantify. As one participant noted, "we haven't come up with a good mechanism to analyze the economics of cyber security. If you have something that they perceive of value, which could be anything at anytime, then there is a fairly substantial risk. We have to come up with a protocol on how to manage that problem."

Combating corruption and industrial espionage through due diligence

In both India and China, it is important to understand the government as well as the workforce. In China, the governing party is present in every successful operation, whether or not their presence is visible. For companies operating there, it is important to find staff members with a government and or party background who can provide insight on how to effectively deal with both the party and government. An important step in identifying members who may be on more than one payroll is through due diligence research.

Participants noted that information is available, if hard to access, in China. While there are very few national databases, by accessing them it is possible to find out about the shareholdings of companies, their legal representatives, the registered capital and date of formation. There is usually information on accounts (albeit unaudited), the shareholders and legal representatives of the organizations. If one is diligent, by looking at bank accounts and firm records, "one can build a fairly accurate picture of somebody's financial state." This information can hint at sources of corruption or at undisclosed party/government membership. Research can include, "for example, seeing how many vehicles are registered in a person's name, how many houses they or their family own, and if that person is earning a thousand dollars a month how is it that he's driving a Lamborghini."

Regional differences affect the availability of information. On China's eastern seaboard business operations are more transparent, and governments are more aware of how business works and appreciate the need to operate on a more level playing field in terms providing accurate information. Inland, however, multi-national companies investigating their local partners there have found that local governments blocked efforts to try and obtain information. Corrupt local governments create these obstacles because they are working hand-in-hand with the local businesses.

> By making it a game, these security officers are much more diligent in doing their inspections.

In India, the hierarchical culture can present a challenge. As everyone knows his or her place in this very hierarchical society, workers "have grown up in competitive silos fighting with one another for every single opportunity, communicating only to the layer above them. The result is a workforce that is very bright, focused and very inflexible." It was suggested that this workforce mentality doesn't support initiative, making it difficult to train people well and rely on them to be resourceful and inventive on the job. However, participants noted "seeing changes as a result of partnerships in the public/private sector with Indian authorities occurring across the whole country and it's building momentum." These are signs that those historical resistances and obstacles are beginning to be broken down.

A game with real consequences in counter-terrorism.

In recent years with the shifting of terrorist targets, it has been especially important in the hospitality industry for hotel security forces to share best practices. Leading firms are seeking to engage their officers and motivate them to be constantly diligent in their efforts.

> …The guard who runs the mirror under the car and he's been doing it for the last six months and he's never found anything so he just stops looking. He's not looking at the mirror. He's thinking about his girlfriend on Friday night and what they're going to do.

While security officers may be well trained, the repetition of day-to-day operations often leads to decreased alertness and slips in vigilance. One participant spoke of a training measure aimed to address "the guard who runs the mirror under the car and he's been doing it for the last six months and he's never found anything so he just stops looking. He's not looking at the mirror. He's thinking about his girlfriend on Friday night and what they're going to do." To change this behavior and motivate guards to consistently perform their duties with vigilance, they have made vigilance in procedures a game – one with both positive and negative consequences. Once a week their hotels are mandated to test their checkpoints. Hotels have some type of a device positioned under a car, in a suitcase or with someone as they walk through a metal detector. If the security guard finds it, he is rewarded with the equivalent to three days pay. If he doesn't find it, the first time he goes back for more training, the second time he loses his job. By making security a game with tangible gains and losses, hotels motivate these security officers to be much more diligent in their inspections.

Applying the STAR Process to security operations.

STAR (Screen, Train, Audit and Repeat) is a methodology which when consistently applied enhances continuity of security operations.

Screening refers to due diligence and the need to know whom you are hiring. With regard to training, participants held that it is no longer adequate to run a one-time workshop telling employees what they should be doing. Training must be ongoing and remind staff that there are codes of conduct by which the employer, employee, vendor and affiliate must comply and that these are absolutely essential.

Audits, when applied randomly on an internal and external basis, are excellent deterrents for both "sloppiness and corruption." Random audits, it was suggested, should include suppliers and vendors. The audits should be undertaken to ensure that targets do not know when the audit is taking place. The audits should include an opportunity to check the records of those being audited. Finally, it is important to repeat the process to ensure ongoing compliance and to account for staff turnover and other changes.

> The STAR approach (Screen, Train, Audit and Repeat) is a methodology that when consistently applied, enhances continuity of security operations.

Knowing the staff and organizational structure in each operation is essential. One participant described a corporate operation in which a different expatriate manager was generally assigned every three years. Yet, it was the local manager who was the one who truly controlled the business operation. That local manager had fluency in a number of languages and knew how to manipulate the system. He had the capacity to cover up fraud schemes for several years until a new expat manager was rotated in. The application of the STAR methodology (here with an emphasis on Screening and Audits) can combat this kind of corruption and ensure a secure operation.

Resilience is about the ability to withstand and thrive during turbulent times.

"Traditional risk management is often taken to imply more of the down side of risk, to include the up-side and related opportunities we focus on resilience in our plans," offered one participant. He continued, "One caution I'll offer about all of this is it's all about the journey; the destination of full implementation and a perfect system is not achievable. The five program processes for which I have coordination responsibility are business continuity planning, incident management, crisis resolution, emergency planning and disaster recovery. These are all networked together because they are related. The continuum for risk and resilience spans anticipating and preventing what risk events you can on the one hand, and managing and resolving those risks you can't prevent and ultimately do occur."

Empowering the lowest levels to manage incidents.

According to one participant, they address incident management by providing "some tools to our business units." He posited that "the rubber meets the road …in the business units. That's very important because that's where we want incidents managed and resolved – at the lowest level where capability exists. So it is our job to train these folks in this common-sense methodology." He added, "One tool we have developed is problem identification. So many incidents get off to the wrong start because they've identified the wrong

> One tool we have developed is problem identification. So many incidents get off to the wrong start because they've identified the wrong problem…

problem. Often it's consumer confidence. You need to know what emotion you're trying to manage from the external perspective – not the technical solutions. When you have a consumer confidence problem and you're arguing [that scientific analysis suggests that something that happened] won't hurt you, that's decisively resolving the wrong problem. Another tool is stakeholder analysis (market sensitivities). If something similar to what you're facing has already happened in that market place, be careful because that can compound your problem. We also focus on communication strategy and media management."

In going global, we don't try to prevent all risks.

One executive relayed how his firm is committed to global market penetration saying, "We do not want to be told that it's too risky a market- we're going to go there. We're going to fix it later and that's what we specialize in is fixing it rather than preventing it."

We don't try to "predict" risks but we do "forecast" and look at trends – up, down and stable.

One participant remarked, "I have responsibility for global threat analysis. That effort consistently monitors over two hundred countries. We've designed a quantitative system for looking at political risk. It uses variables that we think are important to political stability and risk and gives us an option for trending. We don't call it predicting, however. As Yogi Berra said, 'it's very difficult to predict, particularly the future,' and I agree. So we take forecasts out about two years in terms of a trend- up, stable, down."

> We do not want to be told that it's too risky a market- we're going to go there. We're going to fix it later and that's what we specialize in is fixing it rather than preventing it.

Coconut Risk and Subway Risk – you've got to prepare for both.

"Recently, an article came out of MIT discussing two types of risk- coconut risk and subway risk," cited one executive. "Subway risks are those with a predictable aspect. You know, for example, that the subway often arrives five minutes late, five minutes early; you know that kind of stuff. You can see the bell curve and you can predict and model risks like those- that's quantifiable risk. What no one has figured out to any satisfactory degree is how to deal with the coconut risk. The coconut risk occurs when you sit under a coconut tree and a coconut drops out and hits you on the head. Those risks are unpredictable- akin to a black swan. There are some risks (subway risks) that are quantifiable, and we are trying to mature our system into a more quantitative system. We want to be careful that we try to measure those subway risks and deal with those coconuts through good preparation."

KEYNOTE ADDRESS

Janet Williams
Deputy Assistant Commissioner – London Metropolitan Police Service

Janet Williams, Deputy Assistant Commissioner, London Metropolitan Police Service, gave a luncheon keynote address at this year's Summit.

SUMMARY

Williams' keynote address focused on the changing nature of cyber security risks and possible private / public collaboration strategies to address them. Williams also related these risks to recent terrorist incidents.

The Investigation into HMRC.

In 2007 I was called by the British Government to lead the investigation into the HMRC (Her Majesty's Revenue and Customs) child benefit data loss. This situation involved the loss of two computer discs with several million sets of data on all persons receiving child benefit in the U.K. Almost all families' financial data was potentially compromised. There was huge media interest in this case and it was of grave concern to the government. In the end, lessons learned were more about systems and process and teams than "cyber security".

The systems and process in HMRC were good and quite sophisticated but problematic in that the people implementing them didn't understand how or why their part of the jigsaw was important. Systems rely on people, and if we don't invest in explaining the significance of their role they are likely to take short cuts or neglect things with dire consequences. I have since found this to be a profound vulnerability in several other organizations. To believe in a system without properly testing and examining it for gaps or conducting resilience contingency testing is unwise. How would your organization function if your systems went down for two hours?

While I was fairly sure the computer discs in question were simply lost through human error, I became interested in the potential impact if they were in criminal hands. What would be the extent of the identity theft, and the use of the information in cyber space for criminal purposes?

Specifically, I wanted to know:

- Who is buying and selling identities in bulk?
- What crimes are they used to facilitate?
- What harm is cyber activity causing?
- How can law enforcement fight this threat, which acts with speed and agility and crosses jurisdictional boundaries at will when we have insufficiently skilled law enforcement?
- How are we to get a real understanding of the depth of the problem when there is still no obligation to report data breaches in the U.K.?

Limited funding and a view that cyber security is very specialized work that does not impact upon "public confidence" makes getting answers to these questions even more difficult. The importance of cyber security is valued at a poor second against the very real concerns of homicide, rape, child abuse, and street robbery that "feel" more serious, immediate and all too real.

It is important to work as a team.

It is only by coming together as a team, agreeing on working principles, having fewer but more vigorously enforced rules that will we minimize drift. We have to test how "joined up" we really are by engaging in open honest de-briefs, testing our communications, challenging our command procedures, and gaining an understanding of the legislation that constrains or enables us.

The Enigma Room.

Let's look at the team we put together to take on this fight. Bill Gates says "leaders need to have the confidence to surround themselves with people who are better than they are". That includes a variety of disciplines, experience and skill. This isn't new thinking.

During the Second World War there was a room next to the enigma room. It contained an eclectic mix of experts including historians, statisticians, physicists, clergy and doctors of medicine. A problem was thrown in and the experts bounced off each other to provide a solution. Back in 1855 when faced with the cholera epidemic, Dr. John Snow of St. Georges Hospital, an anesthetist, Rev. Henry Whitehead, a Soho clergyman and social entrepreneur, and William Farr the Registrar General, came together as leaders of what became a wide group that solved a complex problem with a simple answer - clean water.

It's important to anticipate cyber risk, rather than just respond.

The cyber adversary is agile and intelligent. He is enjoying a good deal of initiative in the struggle and he doesn't have to work too hard either. We, his adversaries are docile and complacent. Our response to the threat is reactive rather than anticipatory. We are using redundant threat assessment methodology which means we're only recognizing and beginning to address the cyber threat at the point it is fully formed and potent.

So, as part of our policing response to e-crime we have a small multi-skilled police unit ranging from highly trained high tech investigators to forensic accountants, surveillance officers and covert operatives working with and within a Virtual Task Force made up of financial institutions, telecommunications experts, academia and "a red team" provided by Chatham House. We share intelligence and lever resources to the benefit of the whole. We collaborate quickly across jurisdictions to identify, locate and neutralise the e-crime threat. The Virtual Task Force is dynamic, creative, highly skilled and competitive.

Our opponents work on the "OODA" loop, they Observe Orient Decide and Act. We believe we can only defeat the threat by:

- Making their illegal activity dangerous or costly.
- Forcing them into the physical world (where they are vulnerable to observation and detection)
- By disruption, lengthening their decision-making / action cycle, making them more susceptible to intelligence oversight and thereby allowing security and law enforcement to steal the pace on them.

There has been success in fighting cyber crime.

We have had some dramatic success to date. We have developed, with PricewaterhouseCoopers, a "harm matrix" and we are now able to quantify the harm caused at the various stages of criminal activity, how much criminals invest, and the return received. We are able to quantify the work and effort of law enforcement and our partners in the Virtual Task Force.

The first case we conducted was Operation Poplin, which involved an OCN using a new type of Trojan against online banking and a network of mules to extract monies. In two months the criminals gained £949,600. Victims lost £1,507,000 and the wider impact was £243,400. By disruption and arrest a conservative savings to victims was £9,042,000, all of which would have had to be passed to the consumer, "the man in the street," one way or another.

I know this is a drop in the ocean but it's important for three reasons:

1. The Virtual Task Force shares intelligence, works dynamically, learns and provides cross jurisdictional reach and expertise to complement that of law enforcement; thereby reducing a job from three years to three weeks.
2. We are showing that the public and businesses are harmed by e-crime and we can prove the cost. This will impact upon public opinion in the medium term.
3. The VTF (Virtual Task Force) and Operation Poplin have provided proof of concept that private / public collaboration works against e-crime. As our work progressed we realized that we don't have the balance right, prevention is always better than cure.

Public-Private Partnership is Key in the Fight Against Cyber Risk and Crime.

Later this month we are launching a new partnership with industry. Together we will pool our resources to raise mainstream awareness of cyber crime by identifying the issues and delivering crime prevention advice in collaboration. We believe that partnership working through synergy between industry and law enforcement will engender trust and increase public confidence. It will also ensure that any crime prevention material that is produced will meet the needs of the consumer, save industry money and reduce the number of victims of cyber crime. It will also ensure that businesses effectively shape and put to practical use the lessons we are learning and deliver the messages at the most effective distribution points. Despite this, it is but a drop in the ocean.

Detectives shouldn't call themselves such if, in two years, they don't understand how to be effective in cyber space. All probationary constables and all levels of detective training now include cyber modules appropriate to role. Let's think about this. Isn't it crazy that our police officers can give crime prevention advice about physical security of our homes but not how to be safe online?

I think industry must adopt international standards, share intelligence on threat, and effectively police their own systems. This isn't only important to protect customers, but indeed their own interests. To this effect and as part solution we are working with law enforcement, the private sector and academia to produce an ACPO (Assoc. of Chief Police Officers) good practice guide for digital evidence and e-crime

standards for industry supported by the British Standards Institute.

Terrorists can pose a cyber threat.

So where does cyber link with counter terrorism? From a law enforcement perspective, I can see the impact of extremist material, fed directly into homes, unchallenged on the minds of vulnerable or impressionable people (which act as an echo chamber). We know that terrorist organizations "educate" people on the net and the availability of bomb making literature has been exposed in court. Debriefs of convicted terrorists indicate their interest in developing cyber threats.

All of us, if we are wise, now police our systems for both external and internal threats. We, as nations, are investing billions of pounds in physical security to meet the terrorism threat. Terrorists aren't stupid, however- why bother planning to physically defeat concrete walls and security checks when you can float over on a cloud and infiltrate an organizations' infrastructure, plant part of a jigsaw virus and sit safely in another jurisdiction confident that you probably won't be caught but the impact of your action will be profound, memorable and awesome. A terrorist needs intent, capacity and capability to carry out an atrocity. I think we need to be proactive now and not be complacent simply because the "threat" is not being identified by traditional means.

I think the U.S. Secret Service has lessons to offer here. It is interesting to me that their detectives there are both protection and cyber trained. Scotland Yard protection officers, under my command, are about to receive similar cyber training. How many of our children's Facebook accounts hold details and pictures that can compromise us?

If you think laterally, the risk is obvious.

GLOBAL ROUNDTABLE THREE

Cyber-Security Threats: Challenges & Strategies

Overview

This roundtable focused on the economics of cyber risk, the misalignment of incentives and the causal factors and risk to intellectual property as well as the emerging threats posed by cloud computing. Participants emphasized the need to document and share best practices while standards are being developed.

Cyber risk as a "sleeping giant".

Participants agreed that while cyber security lacks the visibility of terrorism and physical security, it is "very much a real threat and one that has dramatic potential impact to both individual organizations and society at large." Technology is only one aspect of cyber security. Addressing public policy and economics are critical to ensure a secure and sustainable system. One participant noted that to date efforts to combat cyber threats have focused largely on how cyber attacks are made (the tactic used) rather than investigating why they are undertaken. This myopic focus ignores the fact that many "people are making a lot of money from cyber attacks."

> "So far, at least in the United States, and I think primarily world-wide, we have been focused on how cyber attacks occur, not why cyber attacks occur…"

Incentives on cyber security are misaligned; individuals often have no significant motivation to follow security practices.

In cyber security terms, losses resulting from lapses by individuals are often borne by others. In the case of personal banking, losses to the individual's account are often borne by banks. One participant noted that when a private citizen's personally identifiable information is stolen (identity theft) and that person loses large sums of money, the bank generally pays for the loss, even if the individual's carelessness was the cause.

Further, it was suggested that Individual carelessness is why cyber terrorists who "attack the Pentagon attack through a subcontractor of a major defense contractor, because that

subcontractor, which may be a small two person operation, doesn't have adequate cyber security. From there you get to the Pentagon's major weapon contractor, from there you get to the Pentagon itself."

Some contended that there is no incentive for most individuals (often the initial weak point) to improve his or her cyber security because they don't stand to lose anything. It was argued that core investment is being undermined because of vulnerabilities at the edges of the network. "A tremendous problem exists in that we have large gaps within our organizational structure and we're not monitoring the people closely enough."

Participants suggested that this was an instance of "the Tragedy of the Commons" in which no one feels responsibility for an asset and as a result, the asset becomes misused, degraded and devalued. Many do not feel liable or responsible in cyber security situations.

Simple, basic security practices can address 80-90% of all cyber losses.

A participant noted the President reported in his Cyber Space Policy Review that American industry lost roughly a trillion dollars in intellectual property alone last year. "Everybody agrees, independent research, the CIA, NSA… that if we simply follow the standards and practices that we already have in the books, we can solve 80-90% of this." The participant referenced a study undertaken by Verizon in which 400 cases were studied using forensic analysis which found that 87% of cyber attacks could have been mitigated simply by using standards and practice that are comparatively easy to apply.

Intellectual property, identity protection, and transparency.

> Our lack of attention to cyber security reflects, "The Tragedy of the Commons; if nobody feels responsible, it gets neglected.

In some respects, protecting individual privacy from identity theft is very similar to protecting the intellectual privacy rights of an organization. There are many groups looking at this. Microsoft for example is involved in a number of alliances and is creating various white papers. The federal government is also making progress- the president signed a memorandum appointing a board to look at the protection of intellectual property.

> It's defending yourself against any potential weaknesses in the way you do things.

The DOD is looking into the formal government mechanisms needed to protect intellectual property in the long term, including eliminating counterfeit parts from the supply chain. Its efforts are not limited to electronics and cyber security- this is a broad counterfeit initiative. The latest presidential memorandum will harness many of these efforts and work to build a coherent, unified whole. "An aspect of intellectual property theft that is not often considered is the time delay between when something happens, and the actual time when the hardware or software was implemented." If it's a decade out, or years out, it may be difficult to attribute who is responsible for the crime or loss: management may not be the same, and the people responsible for protecting the information may not be there anymore. This creates an economic issue as well. This delay is rare in cases of theft of personal information, where the causes and results can be identified quickly after the incident.

Cloud based computing is complicating cyber security.

Cyber security is not simply transactional in the sense of a money exchange observed one expert. Rather, "Cloud based computing is problematic because it is a blend between cyber and supply chain" and makes it difficult to tell when "buying an application where it's hosted, and even who developed it."

One participant observed that "there is a big rush to supply chain, and there's a lot of activity around this move to

the cloud. This has resulted in a need for a business impact analysis for cyber security events; no one's really sure of the risk profile of the cloud because you don't know who you're dealing with." He added that the "…supply chain should be seen from a hardware, software, and services perspective."

Identifying and quantifying losses is a significant challenge. One participant provided an example of ATM software fraud in which the Russian mafia, by embedding malware in ATM programs, stole $10-$15 million from ATMs around the world over a 24 hour period. The cost of cyber attacks and cyber compromises has doubled twice in the past two years, and the total cost is estimated at $1 trillion.

These statistics brought up a number of questions. Is cyber crime, once seen as a criminal activity, now a terrorist activity? Is it economic espionage? "It's not just defending yourself against someone else's intent, it's defending yourself against any potential weaknesses in the way you do things, intentional and unintentional." It was stressed that every company should have a strong perimeter fence / firewall and equally importantly, a strategy to command and control the environment inside that firewall, to evaluate both sides of the fence. Yet it was also observed, "Even with all the firewalls in the world, however, if your developers are not following standard practices there will be a problem."

> "The trick is to make this simple, realistic, and practical…and then move forward."

It's vital to share best practices now.

Participants agreed that it is important to share processes and lessons learned now while wider efforts toward standards and similar solutions evolve.

Participants discussed the 'low hanging fruit'- problems we know how to solve now if we do these fairly simple things. It was argued that there is a lot that enterprises can be doing right now, which has been defined in simple terms, things that can significantly affect cyber security. Incentivizing security measures helps increase adherence. An example was offered of "the first level administrative assistant knows that she needs to rotate her passwords in order to get her 125 dollar bonus at the end of the quarter."

Noted one participant, "The trick is to make this simple, realistic, and practical … and then move forward."

Participants offered as a model how the hotel industry came together to share their ideas and best practices on security. As one participant pointed out, "you only get so much traction if you have one hotel worried about their security – when you have all the hotels talking together about how they secure their properties, you get a lot better product." A similar collaborative effort is needed on cyber security.

> "…Bad guys share information, why shouldn't the good guys?"

Another participant added, "We're working with the software assurance program. It's a DHS, DOD and Department of Commerce led effort that is fully public/private and has software assurance guide books and handbooks out there for free that describe the best practices for software assurance."

Participants also discussed ISACs (Information, Sharing and Analysis Centers) developed with DHS encouragement around each of the nation's critical infrastructure sectors. The purpose of the ISAC is to develop public/private collaboration by sharing information about risk management including such issues as cyber threats, cyber vulnerabilities, and related incidents. It was observed that, "bad guys share information, why shouldn't the good guys?"

New action guide, developed by ANSI and ISA, is a public-private partnership aimed at providing concrete solutions to cyber risk needs.

Financial Management of Cyber Risk, an Implementation Framework for CFOs, provides strategies to help bolster information security and ultimately mitigate cyber risk. The publication is available at no charge at www.ANSI.org. It was created to provide a practical and easy-to-understand framework for executives to assess and manage the financial risks generated by modern information systems. The guide

- Explains the true economic impact of cyber events and describes a six-step process for addressing the issue on an interdepartmental basis.
- Focuses on the single biggest organizational vulnerability of cyber systems – people. The largest category of attacks on cyber systems is not from hackers to the system, but from insiders who already have access.
- Provides a framework for analyzing the ever-changing legal and compliance regimes that organizations will have to manage as governmental attention naturally increases.

- Describes how operational and technical issues can be better understood and integrated into an enterprise-wide risk management regime.
- Lays out the comprehensive communication program that organizations need to prepare before, during, and after a cyber incident.
- Addresses the issue of risk management and transfer. Even the most prepared organizations can still be compromised.

The guide was developed by the American National Standards Institute and the Internet Security Alliance in collaboration with a diversity of other organizations including several key government stakeholders. Even with this resource, a clear challenge remains noted one participant. "We are not investing in security." He noted that there have been a number of studies in the last six months indicating that even though cyber attacks are increasing dramatically, international investment in cyber security is going down. Between half and two-thirds of companies are reducing or holding firm their investment in cyber security per the participant.

KEYNOTE ADDRESS

Mike Rackley

Senior Group Manager of Global Security Services, Target Corporation

Mike Rackley, Senior Group Manager of Global Security Services, Target Corporation gave a dinner keynote address at this year's Summit.

SUMMARY

Rackley's keynote address described Target Corporation's involvement in public-private partnerships and how they benefit both the public and the Target family.

Target Corporation, its role in national infrastructure and commitment to its communities.

Target is a U.S.-based retailer with 350,000 team members (employees) and more than 1,700 stores in 49 states with over 38 distribution centers and a large business services function in Bangalore, India. We have more than 2,500 team members in more than 30 countries with our sourcing division. Beyond bricks and mortar, Target.com is the third most visited website in the world with over 24 million unique visitors each month. Target is a general merchandise retailer, a pharmacy and a food supplier. We maintain a robust supply chain and when disaster strikes we make it a priority to ensure that Target remains open as a shopping environment for as long as we can and try to recover as quickly as possible when things are over. Really, Target itself is a component of the national infrastructure.

Strong community citizenship is part of Target's DNA and since 1946 Target has given 5% of our income back to the communities where we do business. We support education, the arts, social services and volunteerism. Today, Target gives more than $3 million every week back to the communities where we are. Our commitment to local communities doesn't waiver based on the economic climate – the 5% remains consistent.

Companies should evaluate the value public/private partnerships bring and how that fits into the value proposition for the organization.

Target defines public private partnerships as the sharing of ideas and resources in a mutually beneficial way that enhances the communities where we do business.

Target maintains more than two thousand public safety partnerships across the country and our leaders serve on more than 50 boards across the public safety sector. We know that successful partnerships fit into the value proposition for an organization by addressing the needs of both public and private sectors. One way private sector organizations can accomplish this is by ensuring that they influence policy, share information and define how they will share resources and risk. These partnerships also have the ability to impact reputation positively if they are done well.

I truly believe that the focus of the private sector organization should be serving as a thought leader and where appropriate a convener. This kind of forum [the International Public Private Preparedness Summit] assists in bringing together

the right stakeholders and the right thought leaders. The convener role has to be determined by who has the intellectual capital. This is not always the private sector. At Target we bring together experts to influence policy and apply that knowledge and those relationships in very real situations.

Why does safety and preparedness matter to Target?

Our safety and preparedness initiatives are critical to many of our business strategies. Our business can only thrive and survive in safe environments because our guests (customers) demand it. Target doesn't want to just be in a community. Target wants to be part of the community. Our innovative partnerships help create effective public safety solutions and we're able to enter communities that have historically challenged the success of other businesses. We work with community leaders to build stores that enhance the quality of life for residents in the area. Recently, Target's introduction into a neighborhood in Washington DC encouraged revitalization in the surrounding area and even increased property values. Our safety measures extend beyond our stores and parking lots and into the communities.

Listening, Engaging and Collaborating.

We listen to our government partners, who frequently share a need for expertise and guidance around emerging issues.

Public and private sector partners share a common goal of building safe communities. It's important to connect public agencies and private business. We must understand where resources may intersect to strengthen both of our efforts. When H1N1 became a global pandemic, we listened to the needs of our guests, other retailers business, and public partners who were all facing challenges in understanding the best method for vaccine distribution. Target's team quickly convened groups of retailers, state and local health associations, and government officials to address the vaccine distribution issues and came up with a good plan.

U.S. Customs sought Target supply chain expertise to assist in designing the C-TPAT program several years ago, which helped to strengthen the security of American ports and helps to insure the safety of the products that flow through the ports. Target is actually the second largest importer in the United States by volume. Target is a tier three C-TPAT importer and we've helped again to add value to our organization.

We've worked with several policy makers to advance the federal organized crime initiative and legislation that would make it tougher for criminals to sell stolen products online. This partnership affects a potential multibillion-dollar industry for moving stolen goods as a result of organized retail crime.

Finally, I'd like to stress the importance of engaging other businesses. At Target our intent is to act as a model or a catalyst so that other companies can see the role that they can play in partnerships with communities and encourage them to try to find the right place where they might fit.

Successful businesses have a lot to offer. Their expertise might include organizational development, talent development and technology. It could be a number of things, but I think the key is in identifying the common goal to improve the communities where all of us do business. If we do this in an open and genuine way we can all do well and our efforts will succeed. But both sides must step up in order to accomplish this.

KEYNOTE ADDRESS

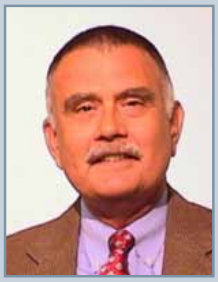
Douglas Smith
Assistant Secretary, U.S. Department of Homeland Security

Assistant Secretary Doug Smith gave a breakfast keynote at this year's Summit

SUMMARY

Smith's keynote address focused on collaboration between the private and public sectors and the Private Sector Preparedness Program (P.S. Prep). He also opened up the discussion to address issues and questions from roundtable participants.

KEYNOTE ADDRESS



Ron Reams
Senior Director – Strategy & Business Alignment, Coca-Cola

Ron Reams, Senior Director of Strategy & Business Alignment, Coca-Cola, delivered a Luncheon Keynote at this year's Summit.

SUMMARY

Ron Reams provided an informal and insightful talk in response to a last minute cancellation of another speaker. His discussion focused on the corporate culture at Coca-Cola and the system by which Coke manages risk in a business comprised of millions of people in 206 countries around the world. At his request, his insights have been integrated into the various roundtable summaries in these proceedings.

GLOBAL ROUNDTABLE FIVE

Key Strategies to Realize Value in Risk & Resilience

The Argument for Investment in Risk Management & Resilience: Identifying & Communicating Value to Leadership

Overview

This roundtable discussed the benefits of risk management for an enterprise including one firm's experience with standard adoption and certification.

> "I think in the current climate, without investment in risk management and security, we will not have customers."

Effective risk management can have many potential benefits including:

improved continuity of operations, protecting a business's reputation, meeting government requirements, fulfilling ethical obligations and others as discussed below.

Risk management safeguards human life: employees, customers and others.

Safeguarding human life is arguably the most important benefit of effective risk management. Protecting employees is ethically paramount. For participants whose businesses involved hosting the public, such as those in the hotel, sporting and entertainment venue industries, ensuring the safety and security of their patrons is equally paramount.

From a business operations perspective, it is also impossible to sustain operations without employees.

From the perspective of government entities, there is a moral and professional obligation to save lives and protect property. As one participant said, "government, at whatever level, is responsible for the public good. [Private sector] risk management has to be there and complement the work that the government does in its space. Without the two working together, you don't get very far."

> "In an industry that's not regulated, risk management is a market differentiator against the competition."

Managing risk effectively can enhance an organization's reputation and brand, and ultimately contribute to the bottom line.

Protecting customers and employees also protects a business's reputation, and one participant went as far as to say, "In the current climate, without investment in risk management and security, we would not have customers." With regard to consumable products, reputation for public health and safety is an asset. It was noted that especially "in an industry that's not regulated, risk management is a market differentiator against the competition."

Risk management protects assets.

Effective risk management safeguards both an organization's own assets and those entrusted to it by its customers. A participant from a financial institution added that his company has "an ethical responsibility to protect our clients and their assets. From a very practical standpoint, if we don't do that, they will go elsewhere."

Risk management impacts stock price / market valuation.

In many cases, risk management can be tied to share-price. As one participant pointed out, "What happens to a company's share-price if they mishandle or don't handle a crisis properly, versus what happens to their share price if they handle it well?" Of note was Oxford Metrica's study, which clearly illustrated this linkage between crisis management and share price in Global 1000 companies.

Enterprise Risk Management (ERM) is a growing norm among organizations.

ERM was acknowledged as an increasing focus in many organizations, especially in the current, relatively "risky" environment perceived by many. The international risk management standard (ISO 31000) was identified as a good representation of the concepts of ERM. "In essence, it's essentially identifying your risks, doing some level of analysis, and deciding how those risks should be addressed, whether by transfer, acceptance, mitigation and so forth, then implementing that plan, monitoring it and making adjustments – the plan-do-check-act cycle in your basic management systems approach. The important lesson learned at the Summit is that simplicity should be the groundwork/foundation for anything we do."

> "Risk management has to be at the highest level of the organization so that you've got the leadership buy-in to make it happen across the enterprise."

There is critical need for executive buy-in and reflection of risk management in corporate culture.

Participants also agreed that corporate culture could pose a challenge to risk management. One participant discussed the need for a change in workplace culture, because "risk management has to be firmly ensconced in performance management. It has to be at the highest level of the organization so that you've got the leadership buy-in necessary to make it happen across the enterprise."

> "…The bigger companies are going to insist that you have some level of certification or proof that you're resilient, so why wait?"

The greatest value in ERM is in its ability to help achieve objectives but the challenge of organizational silos must be overcome.

"In Enterprise Risk Management (ERM), it's the silos that will kill you," volunteered one senior executive. "You cannot get a portfolio view of risk if you're only doing risk management in silos. You absolutely have to have some way to get those silos to communicate. We have a risk taxonomy of 23 categories that we examine yearly. Last year our board of directors decided they wanted to spend one meeting a year totally dedicated to risk management. That was a real sign of motivation. The greatest value that can be added by ERM is when you can connect it to the achievement of strategic objectives. That's very, very, very important."

Risk management supports trust across multiple audiences.

Participants agreed that trust is critical for organizations – trust in one's brand, trust that the organization can deliver in difficult times, trust in one's supply chain.

Certifying to a risk management standard (as with the PS-Prep Program) can be a competitive advantage and offer real benefits in a supply chain.

A participant from an organization that was recently certified to the business continuity standard BS 25999 remarked, "…having gone through this process, I'd say I'm really glad we did it, and I really encourage everyone to take a different view of voluntary certification, rather than waiting for regulation and waiting to be pushed, be proactive and take this

on as a brand sharpener and a real competitive advantage. It will really get you there." The BS 25999 standard is one of three standards that companies can be voluntarily certified to under the newly established Private Sector Preparedness (PS-Prep) program being initiated by the U.S. Department of Homeland Security. The other two standards are NFPA 1600 and ASIS SPC.1.

The participant further remarked, "We, as everyone else in this room, I'm sure, can attest to, are constantly asked by key customers, key suppliers, 'Tell us about your resiliency, tell us about your business continuity, tell us about disaster recovery. How effective is it? Let's see your plan. Let's see your test results.' [After certification,] we don't have to get into a lot of detail because anyone who looks at the scope of our certification knows that we are further along than most organizations are."

The "Wal-Mart affect" was also stated as a justification for pre-emptive certification. As one participant observed "Big fish are going to come out and start insisting on this, just as Wal-Mart came out with EDI standards and said, 'If you want to do business with us, you're going to have to fulfill this. 'If bigger companies are going to insist that you have some level of certification or proof that you're resilient, then why wait?" It was also discussed that the PS-Prep program does look to take into account and essentially credit existing industry efforts in the certification process to build on current practice and facilitate certification.

GLOBAL ROUNDTABLE SIX

Supply Chain Risk Management (SCRM) & the Challenge of Supply Chain Integrity & Counterfeiting

Overview

This roundtable discussed the risks in supply chains in an increasingly global economy where seemingly localized events such as the Icelandic Volcano eruption have worldwide impacts on all aspects of supply chains. Also discussed were the impacts and challenges of counterfeiting and gray market products.

Global supply chains create complex vulnerabilities and effectively large geographic targets for disruptions of one form or another.

One participant reflected, "The lesson learned here is there's a lot of mitigation possible for supply chains, and while that's very, very important, you should know you won't be able to mitigate everything. We live in a very connected world, where the smallest disruption somewhere (one that you may think will not affect you) can have a large effect on you or your company."

> "...That's essentially the essence of all hazards. It should really be called all impacts, or common impacts planning."

Another added that the migration of manufacturing "has certainly jettisoned from the United States. Component manufacturing has all but disappeared in this country." This increase in globalization of the supply chain makes resilient supply chains even more critical.

Sub-contracting presents special risks and prompts the question of who is really making the product or delivering the service

Sub-contracting presents a special risk, as one participant pointed out "you may be sub-contracting to a firm in India and unbeknownst to you they sub-contract to a software development firm in China and the guy in China puts a back door into your application. The Indian subcontractors don't know it, they send it over here, and all of a sudden you have a vulnerable system." In this situation," it's hard to detect these changes, but doing so is a critical part of supply chain management /vendor management.

In addressing key dependencies, the focus should not be on the cause but the consequence.

One participant pointed out that while we tend to focus on specific emergency scenarios, we ought to be focusing more on the consequence instead of the causality. "If a chemical plant doesn't have electricity from the electric company, it doesn't matter if someone crossed two wires or if the electric company was blown up, the problem is that the chemical plant does not have electricity. The consequence, not the causality, is the real issue, which is the plant doesn't have access to its resource." Bill Raisch agreed that while different events "can have various impacts, there are a somewhat limited number of core possible impacts which may be for example the loss of access to your facility, loss of data, impact on your people, etc. That's what you prepare for. And that's essentially the essence of all hazards. It should really be called 'common impacts' planning."

To manage risk, understand an organization's mission and understand the processes that it relies upon.

In order to manage risk, it is critical to understand vulnerabilities; how might processes fail in light of certain sorts of catastrophes? A top-down analysis is key in order to evaluate dependencies.

As one participant explained, it's important to "figure out the degraded modes of operation that need to be planned for in order to allocate resources in more reasonable ways. For example, in a Katrina kind of situation there are limits to what can be expected. In extreme environments, what are the degraded modes of operation that we want to ensure we can meet? In a really extreme environment we're never going to get things back to "situation normal. It's important to have a really careful analysis about what essential services we want to have up and running." From a government point of view, "We want the governor to be able to communicate with the people, we want to be able to have fresh water available, but the fact that the corner drugstore may not be up and running may be an acceptable kind of situation."

Value and uncertainty are all integral to any risk assessment model but one number doesn't tell the whole story.

As one participant pointed out, in terms of measuring risk, we tend to use the things that we can easily measure and often these happen to be among the least useful metrics available. As the group observed, "there is an attempt to use a single number, when what you should be doing is looking at value as a probability distribution."

> We live in a very connected world, where the smallest disruption somewhere, that you may think has no effect, does have a large effect on you or your company.

The impact of counterfeiting is substantial across many sectors.

One participant warns, "One out of every ten dollars spent is now going to some kind of counterfeit. This is due to the globalization of the manufacturing base and also net centricity, or the ubiquitous architecture that's being built, both hardware and software throughout almost every organization, and the body of knowledge that exists of how to build those and the low costs that are available today for the building of those kinds of architectures. The bad guys are getting better at this- on a daily basis they are learning how to affect, not just at the system level, but at the sub-component level…So the first question is how closely do you monitor, and how far in depth do you know your supplier organization?"

Conforming to general consensus-based standards may mitigate legal liability from supply chain created crises.

A participant offered, " a year and a half ago we had a major crisis with contaminated food supplies and toys that [caused] lead poisoning, and that is a value proposition that translates into the stock price nose diving…. Standardization and [voluntary] compliance offer an organization a little bit of relief by mitigating the risk of litigation should something go wrong and people get hurt or property gets damaged. There's no fail-proof defense, but certainly a preparedness declaration by demonstration of having done everything that could have been done (that was publicly available and acceptable in the marketplace) is a very good defense."

Trust in your supply chain is critical; this is especially true for pharmaceuticals.

Toys and foodstuffs are not the only products for which supply chain integrity is critical. One participant suggested "consider pharmaceuticals; the expectation is that they are high in quality, they're going to do the job that they're supposed to do and that they won't harm us." Pharmaceutical companies face the serious issues with counterfeit drugs. Leading firms have had to invest in global security and proactively attack the counterfeiting problem.

A University of Bohn study looked at profit in counterfeiting. It found that on average €1,000 invested in fake credit cards might return €7,000; the same investment in counterfeit software might yield the counterfeiter €100,000. However, a €1,000 stake in counterfeit pharmaceuticals might return €500,000. Per one participant, "It is a significantly high reward low risk crime. It's amazing how many countries have no anti-counterfeiting laws at all."

> "Vulnerability in the United States is the internet which is a very, very significant issue here."

Pharmaceutical firms are looking for ways to attack the profit, to de-incentivize it so that the criminals realize that if they're going to counterfeit pharmaceuticals there is no easy profit to be made. Firms are pursuing civil litigation against counterfeiters and even working with a branch of the U.S. Supreme Court to look at legal issues. Experts are looking into what can be done in China to enhance their legal system. It was offered that "at the end of the day for pharmaceuticals, China and India are the center of the universe; probably 80% of counterfeit pharmaceuticals originate from those two countries." Pharmaceutical firms are especially focused on these source countries.

Raising public awareness is key because the public is often ignorant to the source and the danger of pharmaceutical counterfeiting. The source of "vulnerability in the United States is the internet, which is a very, very significant issue here." One participant described a pilot program wherein all mail coming in from China through San Francisco was x-rayed in order to detect counterfeit drugs. Of the 250 shipments of a particular drug tested, all 250 were counterfeit.

Counterfeiting is a problem not just in pharmaceuticals, but also in product lines, services, soft goods, electro-technical and aerospace components. One participant noted that U.S. customs could be a powerful ally in the fight against counterfeiting as they support importation validation. Anti-counterfeiting measures can be developed and shared with them and their inspectors can be trained to detect and turn back shipments.

One participant offered that in the ANSI and ISO world, there is an ad hoc working group called "Supply Chain Risk Management Working Group." It was suggested that their work is focusing on "security" in the supply chain. A US DoD supported Globalization Task Force is pursuing a commercially acceptable standard for global sourcing. It was also offered that the Supply Chain Risk Leadership Council is fairly new but is promising with active involvement in producing the international standard, ISO 28002.

Cross-sector public and private groups are identifying best practices and potential models. Cisco has been active in these endeavors.

When considering a supply chain you also have to consider sole providers. As to various national efforts, a participant suggested that "everything is market driven and the market is driven globally. Today's global market is not the market of 30 years ago, or even 20 years ago when the U.S. had the ability to influence and direct markets. Other markets are growing, consuming more, and catching the attention of suppliers.

It was suggested that every responsible manufacturer or buyer recognizes that it is optimal to have multiple supply sources and in multiple locations. A business can't be over dependent in this climate. It is essential to change business strategies to adjust to the current climate.

Government's challenge in addressing dependencies on a coordinated basis

Participants noted, "One of the things that is missing in government is the 30,000 foot view." Today in Washington you could sit in 80 different supply chain risk management meetings without any of them actually talking to each other.

Dependency analysis is a much broader concept than supply chain. The government looks at dependencies by asking, what are the things that you might need from us - police protection, a particular service we have? Knowing those things in advance and building those things into Continuity of Operations plans is an area of partnership that can benefit all parties. We all have areas of dependency that are not necessarily focused on widgets or items such as human capital issues. Some in the public sector are working to build a cohesive effort around this. It was suggested that if DoD and GSA get together and change the federal acquisition regulation and make this a requirement it would make a difference.

GLOBAL ROUNDTABLE FOUR AND SEVEN

Identifying What Works & Doesn't Work in Public-Private Collaboration: Structures and Strategies for Partnering on Information, Resources and Joint Action

Overview

Roundtables four and seven focused on public/private collaboration, existing structures and outreach efforts, with a look at different platforms, strategies and approaches to collaboration.

Private sector partnership focus in government is growing.

Participants lauded the increase in focus on and cooperation with the private sector they saw in government. One participant observed, "in government we have collected information openly on private sector resources just so that we understand what the private sector capabilities are. It's naive for us to think that those resources are not there. The real work that lies ahead is determining how we collaborate and work together so that those resources are advantageously applied during a disaster."

> "So, when you move to recovery, and when you go past two weeks, and people start to walk away, that's when human beings desperately need help."

Another remarked, "I think it's good to see the growth of the private sector focus in government. This might be an opportunity for those private sector liaisons inside government to sit together at some point to figure out what it is that we can do together." He warned against developing 'tunnel vision' which would create "a situation where everyone is going after the Wal-Marts and the Targets to develop a relationship and overlooking others out there that are equally capable of providing support. By doing this, we'd underscore the image that the private sector has of government already that we're inefficient, we don't know what we're doing."

Coordination is essential for success, as evidenced by one city's method. "One of the things that we've been doing," explained one participant, is recognizing that "we have organizations that are umbrella groups through which we can reach out across a broad range of folks so that we don't just keep picking on the same individual and the same company over and over again."

One example was given of an InterCEP facilitated effort in which "post Katrina about 60 organizations, developed what was essentially a draft standard for mobilizing private sector resources to disaster, essentially streamlining the process of identifying and moving resources in the private sector to aid the public sector. This draft standard was based on best practices and lessons learned. It was ultimately identified by FEMA and the National Incident Management System Integration Center and informed new government procedures and a resource management standard that FEMA has advanced."

The U.S.'s FEMA is making nationwide changes in private sector engagement while recognizing all emergencies start local.

One participant described FEMA's recent efforts regarding public/private partnerships. FEMA's employee workforce is made up largely of reservists, not full-timers. The number of reservists dedicated to the private sector outreach has doubled in the last few months. Once trained, deployment to disasters begins immediately. During recent disasters, FEMA partnered with private sector entities including the Boston Red Sox, the Boston Bruins, the Tennessee Titans, Gaylord Entertainment, Lamar Advertising (with billboards on the I-95 corridor), Regal Cinemas and Bank of America. FEMA and these organizations were able to arrange a mutually beneficial relationship in which no money changed hands but they were able to successfully communicate information, plans and available resources to local communities.

"People may think that this takes a lot of creativity, a lot of

> With one random, cold call, to the Boston Red Sox, we asked, 'Can you help?' They said, 'Sure, we can put your message, your website, and your phone number on our jumbotron at the game, where 37,000 people are attending tonight. Would that be cool?' Yes, it would.

work and a lot of relationship building, but with one cold call to the Boston Red Sox, we simply asked, 'Can you help?' They responded, 'Sure, we can put your message, your website and your phone number on our jumbotron at the game where 37,000 people are attending tonight. Would that be cool?' Of course we answered, 'Yes, it would'."

A participant noted that within two months all of FEMA's ten regions expect to have a private sector liaison dedicated to working in the regions directly with the states and communities. There is now unified agreement within FEMA that it needs to involve the private sector in its national response coordination center." On a day to day basis, we're trying to think out of the box and do innovative things with the private sector –without being limited by bureaucracies, thoughts and ideas of the past, but channeling creativity and innovation of the future."

Participants agreed that one of the important things that FEMA is starting to do "by putting these [private sector liaison] folks in the regions, is trying to help folks at the local level understand how to leverage the relationship that FEMA is building at the national level." One participant believes "it's important for the private sector companies at the national headquarters level to understand which situations FEMA/DHS is involved in and which they aren't." Initial information and decisions are being made by organizations in the early stages of an event are being handled at the local level. FEMA can help in the "sharing of information … even to the extent of someone calling up and asking 'Can you point me in the right direction to the person at the New Hampshire EOC [emergency operations center]. Even if the contact is not FEMA, they have a point of contact for that local emergency manager and that is going to be a critical resource."

> On a day to day basis we're trying to think out of the box and do innovative things with the private sector – not being limited by bureaucracies, and thoughts, and ideas of the past, but creativity and innovation of the future.

FEMA's communications challenges.

Participants agreed that a major challenge for FEMA is to do a better job of explaining the communication channels within FEMA to the private sector, and to decide how best these can be utilized without being inundated. This is no small task, as channels of communication include infrastructure protection channels, DHS private sector channels, FEMA private sector channels, DHS public affairs channels and program channels throughout all of DHS and FEMA.

Participants also agreed that while establishing proper communication channels is important, "what you talk about" is also vital. Most people are eager to be part of response, but preparedness, recovery and mitigation can be very difficult things to sell. In a response situation, "everybody wants to know how to get stuff to the disaster area in the first 12 hours. That will always be a challenge, but you can get stuff to Haiti today. So, when you move to recovery, and when you go two weeks past the initial emergency, and people start to walk away, that's when human beings desperately need help." Raisch agreed, "I call that the 'Bruce Willis Effect.' We all want to be active in the initial response when the smoke is still in the air. However, most emergencies become old news once we reach the recovery stage and the dust has settled."

> The real work that lies ahead is how do we collaborate and work together so that those resources are advantageously being applied to the disaster.

One participant commented that the biggest challenge FEMA faces is working with states to ensure that every state EOC has an approachable and viable public/private partnership. "We can challenge our states to have a formal relationship that is identifiable, dedicated, and sustainable. I don't think those concepts are offensive to anyone, and they leave latitude to construct it however it works best… [optimally] we'd have some kind of yellow pages where we go to during the disaster and we know exactly who to talk to, so we can get good work done."

The ISAC: Information Sharing & Analysis Centers– the U.S. attempt to engage critical infrastructure sectors in the private sector.

The ISAC model has two halves: information sharing and analysis. The first is concerned with what information is being shared. The second concerns the methodological structure

and processes for the analysis. When the initial concept of ISACs was introduced in the United States in 1997, there was no large mechanism in the government for doing analysis of threat information. Since the creation of the Department of Homeland Security, a large mechanism has been created although some may question its current effectiveness in some of its analysis. One participant asserted that the ISAC model needs better definition. "Parts of it work, parts of it don't." Nonetheless it was argued that it is a worthwhile model for others in the international community to consider.

> We learn from them and they learn from us.

Part of the ISAC's role is to look for threats and vulnerabilities specific to the sector and share that information within the sector. Some participants suggested that there isn't enough sharing of meaningful information. They suggest that there is very little incident and near miss information being shared because a lot of organizations will not disclose it.

The FBI's Domestic Security Alliance Council (DSAC) goal is a two-way partnership with the private sector.

Following 9/11, industry leaders approached the FBI and suggested creating a domestic counterpart to the U.S. State Department's Overseas Security Advisory Council (OSAC). The Domestic Security Alliance Council was established in 2006 and is comprised of 135 member companies which employ 11,000,000 people in the U.S. with a GDP of about five trillion dollars or 32-35% of the country's GDP. Its mission is to enhance private sector cooperation and facilitate the timely exchange of information. "To facilitate this exchange of information, the DSAC is trying to have a more direct line with the senior leadership of these companies because if something significant happens, you may need to get information to the bureau to get some action, and hopefully the reverse is true. If the FBI needs something from the private sector, it can go to the CEO or CSO [Chief Security Officer] and it can get something done in a timely fashion."

The participant went on to describe the three legs of the stool that DSAC stands on to achieve their mission. The first is the "Domestic Security Executive Academy" where SACs (Special Agents in Charge) are paired with CEOs or CSOs of large corporations within their territory, and key relationships are built before the SAC takes up the new posting. The second leg is an "Intelligence Analyst Symposium", in which ten FBI analysts and thirty to forty private sector representatives are brought together to go over tradecraft and different tools. They are also given some scenario-based training. In this symposium, "we learn from them and they learn from us." The third leg of the stool is a web-port, a means of exchanging information. "Every day on that portal we upload products and things of interest. One of the challenges of this process is taking oftentimes classified information, filtering that back and getting it declassified and putting it up on the portal for our membership to have access to and to communicate with us about… strategic information, along with tactics, training and procedures are things that we have the capability to share through the FBI and through DHS."

Standards impact 85% of all international Trade: The American National Standards Institute (ANSI) works with all stakeholders to develop global solutions.

It was noted that 85% of all international commerce – international trade in merchandise, industrial commodities, and products- is affected by either standards or their application.

One public/private partnership which has worked to the benefit of the entire community is the partnership between the Department of Homeland Security and ANSI, which joined together three and a half years ago to run a standards panel on homeland security. One participant recounted how "as a result of 9/11 we were asked to develop systems, criteria and assessment tools to increase competency in defending ourselves against security risks. This included engagement with TSA, FBI, CIA, U.S. Customs, immigration people and we're continuing to work on it. ANSI does not develop standards. We have over 200 standard developing organizations that are assessed and accredited by ANSI. We have hundreds of certification bodies that are assessed and accredited by ANSI. ANAB is one of the ANSI activities."

ANSI is a private sector not-for-profit organization. It was established in 1918, by a partnership of federal agencies and the private sector, including several industrial organizations and trade associations. ANSI was designed to assist

manufacturing and mechanical processes, which at that time were issues of national interest. ANSI has since grown, and "today, there are many different types of standards and compliance activities that encompass just about everything you can think of, obviously, all manufacturing and technology issues, but also all the services and soft issues that have been discussed over the last couple of days" he elaborated.

Today's security problems are no longer national, but have global impact and include counterfeiting, security and cyber risk, etc. It is therefore important to work with international and regional standard setting bodies. "We connect with them in this country through ANSI" which makes it possible "to not only have a solution here [in the United States], but also to internationalize that solution so that companies don't have to do it ten different ways in ten different markets. They can create one solution, and, hopefully, have that solution accepted in multiple markets."

GLOBAL ROUNDTABLE EIGHT

Prioritizing Common Issues & Organizing to Develop Targeted Solutions

Overview

This roundtable focused on reflecting on the Summit discourse and identifying common problems which could be addressed collaboratively with the goal of developing concrete solutions to them. The Global Roundtable has a history of organizing core groups of its members (Task Forces) who serve as catalysts with other stakeholders in identifying and advancing actionable strategies to impact targeted issues. Areas for potential common action included:

1. A global solution for supply chain integrity
2. Actionable strategies for cyber security and a compelling business case in support of them.
3. A global knowledge base on public-private collaboration in risk management and a platform to advance collaboration between the public and private sectors internationally

Supply Chain Integrity: A clear need for a global solution.

The Need: There is a significant threat posed by products and services which are not what they purport to be with potential impacts on the acquiring organization due to inferior quality and/or malicious intent.

- This supply chain integrity threat includes counterfeit goods which are advanced by criminals for monetary gain (e.g., low cost knock-offs as well as high value financial transactions) and also by bad actors (e.g., nation states and terrorists) for national security and other political gain.
- This threat impacts a broad range of products (and the activities that rely on them) including computer hardware, software, services, drugs, aircraft parts, etc. It poses a particular risk to critical infrastructure operators and national security organizations.
- The human element is an important consideration in supply chain integrity and should be considered as appropriate in this effort.
- Given the global nature of commerce, a global solution is needed. Such a solution must span not only international boundaries but also span business sectors.

A Task Force Mission: There is strong interest in forming a task force of leading members of the Global Roundtable to evaluate an initiative to develop and advance the implementation of global solutions for supply chain integrity. Such a task force would reach out to and collaborate with other appropriate stakeholders.

- Actionable strategies and tactics that address supply chain integrity should be considered by the Task Force including process-based approaches.
- The ability to implement solutions on a global basis is key.

Task Force Objectives: Several objectives were identified.

- Convene key stakeholders to address the problem on an international basis
- Wide diversity of member companies spanning different industries and international markets
- Engagement of key stakeholders on a global basis
- Evaluate causes and drivers of the problem
- Identify and evaluate existing strategies and best practices
- Identify and evaluate potential global solutions including
  - Actionable short term strategies, policies, procedures (including contract stipulations)
  - The potential value of global criteria/standards for supply chain integrity and an assessment regime (e.g., certification) and other compliance solutions
- Advance the development & implementation of chosen solution(s) on an international basis.
- Undertake these objectives while considering:
  - The implications of trade relationships and law enforcement issues/concerns.

- Concerns regarding the security of the Task Force discourse on best practices and strategies with respect to proprietary concerns and the potential exposure of vulnerabilities.
- NDAs and processes that assure confidential communications should be considered as appropriate.

Cyber Security: Resources on the "what" and "why".

Both the "what to do" and the "why to do it" need to be more effectively addressed for cyber security. There was wide acknowledgement that the concept of cyber security can be perceived as overwhelming for many in the corporate realm with the default action often to relegate cyber security solely to the IT department with little or no responsibility on a wider basis in the enterprise. A distinct need was discussed for both a clear understanding of the risk posed by the cyber threat and basic and comprehensible strategies which can be widely implemented. Identified areas of focus include the concept of a risk model and the need for standard terminology around threats. Any effort should build on the good work already done by ANSI, the Internet Security Alliance and Symantec. Participants agreed that there is a "need to identify and access best practices, lessons learned and trends." A compelling argument for board members and senior management to invest in cyber security was also seen as critical.

Public-Private Collaboration: An international resource and platform is needed.

There are a diversity of programs and initiatives which have been undertaken in support of better collaboration between the public and private sectors around common security and risk management issues. Many of these efforts have moved forward haltingly as they learn lessons the hard way through trial and error. All those organizations participating in the summit acknowledged the need for further development and improvement.

Furthermore, much of the current public-private activity has been concentrated in a few geographic areas and governments. Yet wider public–private collaboration is urgently needed across the globe in a diversity of regions and countries. While it is likely many of these underserved areas will have distinct needs and considerations, much can be learned from existing efforts.

Best practices and lessons learned should be distilled from existing efforts in public-private collaboration. These could be shared among current initiatives to inform their ongoing development and evolution. Additionally, a resource of best practices and lessons learned could guide the development of new initiatives across the globe. Multi-national corporations in particular saw the need for a more collaborative public-private environment in support of global commerce and collective responsibility.

In addition, a truly international platform to forward such collaboration across sectors was seen as important. InterCEP was seen as a potential catalyst in this regard with potential collaboration with elements of the United Nations and leading multi-national corporations with a global perspective.

Participants

Thomas Anderson
Louisiana State University – Stephenson Disaster Management Institute, Director Corporate & Strategic Development

C. Warren Axelrod, Ph.D
Delta Risk, Senior Consultant; Financial Services Technology Consortium, Executive Adviser

Susan Barry
DRS Technologies,
Director Risk Management

Arnold Bell
FBI, Deputy Program Director

Brien Benson
George Mason University, Director, Enterprise Risk Management

S. Joe Bhatia
American National Standards Institute-ANSI, President and CEO

Len Biegel
Fleishman-Hillard, Senior Advisor

Darren J. Blue
U.S. General Services Administration Chief, Emergency Response & Recovery

Charles F. Burns
Indy Racing League, Director of Security

Francesco Candelari
United Nations Interregional Crime and Justice Research Institute, Liaison Representative, Security Governance / Counter-Terrorism Laboratory

Barry A. Cardoza
Union Bank, N.A., Vice President, Manager of Business Continuity

R. James Caverly
U.S. Department of Homeland Security; National Protection and Programs Directorate, Director

John P. Clark
Pfizer, Vice President &
Chief Security Officer, Global Security

Larry Clinton
Internet Security Alliance (ISA),
President & CEO

James T. (Tim) Cole
NORAD & USNORTHCOM, Chief, Private Sector & Nongovernmental Organizations Program Office, Interagency Coordination Directorate

Stephen Collins
Bank of England, Head of Business Continuity Division

Craig Corbin
Worldwide Technology Inc.,
Director, Strategic Programs

Karen Coyne
International Center for Enterprise Preparedness (InterCEP),
Project Coordinator

Ken Damstrom
Goldman Sachs, Office of Global Security,
Chief Operating Officer,
Office of Global Security

Don Davidson
Office of the U.S. Assistant Secretary of Defense, ICT Specialist (GTF)

Jos de Lange
Netherlands Defense Academy

Matthew Deane
New York Yankees, Manager,
Security Systems Administration

Margaret Della
Rutgers Institute for Ethical Leadership, Senior Program Manager

Dennis Dumont
Raytheon Company, Project Manager, Enterprise Preparedness Program

Evelyn Farkas
Supreme Allied Commander Europe (SACEUR) and Commander, U.S. European Command (EUCOM), Senior Advisor on Public-Private Partnerships

Anthony Farneti
Waste Management, Inc., Manager, Security Interests - Midwest & Canada

Gregory Ferris
Morgan Stanley, Managing Director and Global Head of Business Continuity Planning

Angelyn S. Flowers
University of the District of Columbia, Director, Homeland Security-Emergency Management National Legal Preparedness Project

Greg Fowler
Federal Bureau of Investigation (FBI), Special Agent in Charge of the Counterterrorism Division and the New York Joint Terrorism Task Force

Edward Gibson
PriceWaterhouseCoopers, Director, U.S. Forensics Technology Solutions Practice

Mark Haimowitz
Disney ABC Television Group, Director, Business Continuity Planning

Karen Hughes
American National Standards Institute – ANSI, Director - HSSP
(Homeland Security Standards)

John J. Imhoff
Ernst & Young LLP, Director,
Office of Firm Security

Hiroshi Kamezaki
Tokio Marine & Nichido Risk Consulting Co. Ltd, Manager, Business Resiliency Department

Mitchell Komaroff
Office of the U.S. Assistant Secretary of Defense for Networks and Information Integration, Director, Globalization Task Force

Richard Lyall
Anschutz Entertainment Group (AEG Europe), Facility Services Director

Richard Maddison
Financial Services Authority, Deputy Head of Business Continuity Risk, Financial Stability & Financial Services Authority

Howard Mannella
Expedia, Principal Resiliency Strategist

Tim Mathews
Educational Testing Service (ETS), Director, Enterprise Resiliency

Gerard McAtamney
London First, Director, Security and Policing

Jerry McCarty
Port Authority of New York and New Jersey, General Manager, Emergency Management

Andrew McCruden
Ziff Brothers Investments, Director of Business Continuity

Nicole McKoin
Target Corporation, Senior Business Partner, Assets Protection-Community Engagement Team

Jaime McLain
Cisco, Business Resiliency Manager

Nader Mehravari, PhD
Lockheed Martin, Director, Corporate Business Resiliency

Victor Meyer
Deutsche Bank, Global Head of Corporate Security & Business Continuity

Participants

Josh Miller
Control Risks, General Manager, Operations in Mexico, Central America & the Caribbean

Penny Neferis
JetBlue Airways, Director, Care and Emergency Response

Alan Orlob
Marriott, Vice President, Safety & Security International

Joe Petro
Citigroup, Managing Director, Security and Investigative Services

Marcus Pollock
Federal Emergency Management Agency (FEMA), Chief of Standards and Technology for the National Integration Center, Protection and National Preparedness

Ted Price
T&M Protection Resources, Senior Advisor & Consultant

Mike Rackley
Target Corporation, Sr. Group Manager of Global Security Services

William Raisch
New York University -International Center for Enterprise Preparedness (InterCEP), Director

Don Randall
Bank of England, Head of Security

Ronald A. Reams
Coca-Cola Company, Senior Director, Strategy and Business Alignment

Robert Sama
Federal Reserve Bank of New York, Assistant Vice President, Deputy Chief, Federal Law Enforcement Unit

Annie Searle
ASA Institute for Risk & Innovation, Principal, Former Senior Vice President, Enterprise Risk Services, Washington Mutual

Hagai M. Segal
New York University in London, Lecturer

Douglas A. Smith
U.S. Department of Homeland Security, Assistant Secretary

Rachel Stein Dickinson
New York City Office Of Emergency Management, Deputy Commissioner, Administration, Finance & Policy

Dan Stoneking
U.S. Federal Emergency Management Agency (FEMA), Director, Private Sector

Ira Tannenbaum
New York City Office of Emergency Management, Director of Public/Private Initiatives

Chris Torrens
Control Risks, Deputy Director, Global Client Services EMEA

Iris Valdes
Former Pitney Bowes, Vice President, Preparedness, Continuity & Crisis Management

Janet Williams
London Metropolitan Police, Deputy Assistant Commissioner

Sponsors

The Global Roundtable proudly thanks the following sponsors for making the 2010 New York City Forum possible.

Target Corpoation

World Wide Technology, Inc.

Deutsche Bank

The International Center for Enterprise Preparedness

New York University
285 Mercer Street, 4th Floor
New York, NY 10003
212-998-2000

www.nyu.edu/intercep
intercep@nyu.edu