Proceedings of the Global Risk Summit
New York, June 13-15, 2011
Draft – July 29, 2011

Executive Summary

This document presents a summary of the proceedings of the Global Risk Network Summit, held June 13 – 15, 2011 in New York City. Summit participants included seventy public and private sector leaders representing more than 50 different organizations from nine nations. These participants engaged in a series of facilitated roundtable discussions, focusing on the following themes:

Developing the First Global Risk Network: The framework was vetted for this initiative to develop a trusted community of international corporations and other key public and private stakeholders collaborating to address shared risks. Input was solicited on core activities, targeted risks, geography and initial results-oriented special projects.
Action Items:

- Recommendations for initial special projects to include production of a playbook for building public-private partnerships around large public events; a matrix of public-private partnerships; addressing the topic of organized crime
- Interested corporations should contact InterCEP now to participate in the Network to assure that effective January 1 your priorities are reflected in targeted risks, geographic focus and special projects focused on delivering key solutions to company operations.

The Japanese Crises – Earthquake, Tsunami, Nuclear Incident and its Wider Repercussions: The damage wrought by the earthquake and tsunami that struck northeast Japan in March of 2011 revealed previously overlooked single points of failure, not only at the Fukushima nuclear power station, but in private sector supply chains across the country. Rigid business continuity plans and fragile lines of communication led to confusion and missed opportunities as the disaster unfolded.

Middle East & North Africa Turmoil: Instability in the Arab world poses ongoing challenges as high oil prices give dictatorships in oil-producing countries room to maneuver against widening domestic discontent. The turmoil in the region shows how political risk can catch organizations by surprise, and underlines the importance of thorough pre-planning for security and evacuation, as well as the utility of maintaining trusted relationships across organizational lines for mutual assistance during a crisis.

Technology and Risk Management: The Spectrum of IT Threats to Continuity Risks: The growing threat from "hacktivists" and cybercriminals strikes at the heart of the balance between convenience and security inherent in internet commerce. Potential mitigation strategies discussed include robust information sharing between law enforcement and the private sector, reducing technological risks by keeping critical files quarantined from the internet, and creating a culture of security among employees, contractors and everyone else in the personnel ecosystem.

Supply Chain Risk / Management Challenges and Strategies: Supply chain executives from major

companies described for the roundtable the unique challenges facing their firms' continuity operations around supply chain risk, and room for collaboration among roundtable members were explored.

Considering the Spectrum of Risks & Geographies: Prioritizing Key Risks & Geographic Focuses for the Global Risk Network: The urgent need for the creation of a global, public-private information sharing network was discussed, stressing the need for communication through enduring and trusted inter-organizational relationships.

What is Critical for Successful Collaboration?: ***Defining Principles & Policies to Promote Public – Private Partnership:*** The benefits of public-private partnerships, especially in crime prevention, were discussed, along with rationales for engaging with stakeholders outside the traditional risk prevention environment.

Who are the Critical Players in Operational Risk & Crisis?: ***Targeting Organizations & Engagement for a Robust Network:*** Best practices for effective information sharing and crisis management were discussed. The importance of having effective intelligence before an event and the importance of preparing for disruptions of systems and processes rather than specific events were also discussed.

Core Activities to Achieve Business Value: ***Determining Central functions of the Network to Achieve Real Impacts:*** The real-world impacts of public private partnerships were discussed, in terms of information and technology sharing, and especially in the realm of establishing trusted relationships that deliver results in crisis situations. The opportunity for growth in the Global Risk Network was specifically identified as desirable in this regard.

Introduction

The Global Risk Network acts as a scaffolding that supports durable and trusted inter-organizational relationships that help private enterprises weather crises by identifying and addressing shared risks in advance, as well as by building capacity for information sharing and mutual assistance. The Global Risk Network forums focus on gathering in one room the right people from the right organizations in the private and public sectors, to facilitate conversations that generate insights, spread best practices, highlight opportunities for improvement, and add to a shared knowledge base. This is tried and true approach that has already proven itself useful in navigating an uncertain world.

Much of the framework for the Global Risk Network has been developed with input from corporate organizations that are challenged by their global footprints. A core strength of the Network is that it establishes liaison relationships that connect private sector operational risk managers with their public sector counterparts in national governments and international organizations, as well as from existing public-private partnerships and non-governmental organizations. Finally, capitalizing on its foundation at New York University, the Network establishes robust relationships with relevant subject-matter experts, providing an on-call resource for assistance with operational challenges.

Special Note: These summary proceedings seek to convey the information shared during the forum from participants. No independent validation of information shared has been undertaken by the Center.

Roundtable One

Summary

The damage wrought by the earthquake and tsunami that struck northeast Japan in March of 2011 revealed previously overlooked single points of failure, not only at the Fukushima nuclear power station, but in private sector supply chains across the country. Rigid business continuity plans and fragile lines of communication led to confusion and missed opportunities as the disaster unfolded.

An Unprecedented "Domino" Crisis

On March 11, 2011, a magnitude 9.0 earthquake and accompanying tsunami disrupted a vast area of Japan's northeast coast, setting off a multi-staged crisis. The quake and continuous aftershocks produced damage to buildings and power and transportation infrastructure. The primary quake sent tsunami waters rushing as far as six miles inland. Tsunami waters knocked out the cooling systems of several reactors at the Fukushima nuclear plant, triggering partial meltdowns in three reactors, resulting in the release of radiation and severe power shortages across the region.

Casualties are still being tallied, but at present more than 14,000 are dead, with 10,000 missing and 5,000 injured. Of the dead, more than 55 percent were 60 and older, primarily because the tsunami struck in the afternoon while most workers were inland. 78,000 houses were completely destroyed. Building reinforcement technologies reduced damage from the quake, as did internal earthquake-proofing measures such as securing bookshelves. But the combination of the shaking and the tsunami overwhelmed the region's defenses. Following the quake, the architects of the Fukushima plant noted that the plant itself had withstood one of the largest earthquakes in Japan's history, only to be undone by tsunami damage to its external support systems. The failure of unexpectedly vulnerable support systems, leading to much larger problems, proved to be a common experience for many organizations in Japan in the aftermath of the disaster.

The Effectiveness of Warnings

Immediately following the quake, a tsunami warning was issued by the country's national meteorological service, distributed by NHK TV and over public address speakers. Some local government agencies used social networking, primarily Twitter, to communicate the risk, but this was not part of any official response plan. While the majority of people in the affected area reacted correctly and without panic to the warnings, the effectiveness of the warnings was hindered by two factors: First, widespread suspicion about the accuracy of the tsunami forecast, especially among young people, who had not previously experienced a tsunami before and were disinclined to take the warnings seriously. Second,

the tsunami waters were in fact much higher than the warnings suggested.

Management Processes in the Disaster

A majority of firms saw their Business Continuity Plans function properly in the disaster. Failures came when the plans were inflexible, or too specific. There was usage of plans related to other threats but with similar impacts. For example, several firms are reported to have activated their pandemic continuity plans, because their employees could not get to work due to power outages or transportation disruptions. Physical damage to buildings and systems further hampered continuity operations, as lost data led to communications failures, for example an inability to locate or track critical personnel.

Other companies saw their operations hobbled because their planning did not cover supply chain partners. The disaster uncovered an unmanaged concentration of risk at the fourth tier and under supplier level in the supply chain. Most of these suppliers are small to medium enterprises without business continuity planning, who were knocked offline at some stage of the disaster, leading to supply chain failures.

A related cause for concern was that the public sector was unaware of the interdependencies through the supply chain, and so had a limited understanding of the private sector's capabilities.

Lessons Learned

Business continuity plans targeted primarily for addressing formal requirements were most likely to fail in the disaster, while flexible plans (especially those attuned to unique firm vulnerabilities) were most likely to succeed. Still, there were flaws in the risk expectations in the public and private sector. Government risk maps were inadequate to the scale of the disaster, leading to damage in unexpected areas. Participants cited some concern about striking the balance between flexibility and chaos in continuity planning. Said one participant: "When there are multiple plans within an organization or for a particular incident… how do you develop flexibility without disorder?"

Underscored was a focus on the risks posed by supply chain partners with faulty business continuity planning. One participant said that "you have to make sure second, third and fourth tier suppliers have crisis plans in place—the same plans you do." The failure of one link in the supply chain due to lax continuity planning can sink a firm even if it is confident in its own crisis management. As one participant noted: "Our products are temperature controlled. If the power goes out and our backup power suppliers aren't prepared, our product is spoiled."

The main area of concern for participants was deficiencies in crisis communication. Getting access to information in Japan, for the American-based companies especially, was extremely frustrating. Participants perceived that the Japanese government had stonewalled their requests for information. Even getting access to US Embassy officials was difficult, according to participants. The information that

was distributed was seen as ineffectual. "There was a lack of *confidence* in the messages coming out of the government officials," said one participant. There was concern around the room about maintaining clear communication lines between governments and private sector entities that control critical infrastructure affected by a crisis.

Another participant noted that even intra-organizational communications were frayed: "Our challenge was not only information sharing with governments, but communications with our own people on the ground, and having them have to mobilize on their own with the lack of guidance we could provide from the states. We didn't have a robust process to communicate with our people on the ground in Japan, and that thin process broke down."

In the absence of clear information from official sources, organizations turned to the news media for a clearer picture, but found the information there even more confusing. One participant noted the ability to cut through the clutter by accessing a network of trusted contacts on the ground in the affected region: "While the media were going into a feeding frenzy about everything that was going wrong in Tokyo, I had feedback from people I knew and trusted telling me that no, Tokyo wasn't falling apart, business is continuing there. I was getting information from a peer network that confirmed what I was hearing from my people on the ground."

Participants proposed the creation of a secure conference hotline onto which crisis managers can call in to share information during crises. Along with this, a solid framework was proposed to structure calls during a crisis to maximize time efficiency. "We have this concept of Maslow's hierarchy of needs for people. We need one of those for business, and we need to use that as a framework for any inter-organizational conference call," said one participant.

The chief benefit of this trusted peer network conference call would be to share actionable safety information, and to coordinate action across industries during a disaster. Several participants echoed concerns that the decisions of other companies, often in other industry sectors, negatively affected their crisis decisions. Said one participant: "When Delta cancelled its flights, we started to wonder if they knew something we didn't know. If the airlines don't fly, how are we going to get out of here? I understand companies have different appetites for risk, but we need to have some kind of unity of action, or there will be unintended negative consequences."

+ Risk Assessment – Identified Risks:

- Cascading failures from compound disaster events (e.g. Earthquake-Tsunami)
- Failure of unexpectedly vulnerable support systems.
- Inability to get workers to their posts because of transportation infrastructure damage.
- Supply chain failures concentrated on 4th tier suppliers, smaller firms without business continuity planning (BCP).
- Too-rigid business continuity plans left some firms unable to adapt to the shifting challenges produced by the tsunami.
- Communications failures between public and private sectors, and across national boundaries within large organizations.

- Lack of coordination in response action across sectors.

+ Risk Treatment

- Clearly identify all key support systems, work to reduce their vulnerability to likely hazards.
- Make provisions in BCP for post-disaster transportation disruptions.
- Push BCP practices to 4th tier suppliers.
- Ensure that Business Continuity Planning is flexible and is keyed to address common impacts and protect key processes, rather than responding to specific hazards.
- Increase communications between private-sector entities across industries to improve collective action after a disaster.

Roundtable Two

Summary

Instability in the Arab world poses ongoing challenges as high oil prices give dictatorships in oil-producing countries room to maneuver against widening domestic discontent. The turmoil in the region shows how political risk can catch organizations by surprise, and underlines the importance of thorough pre-planning for security and evacuation, as well as the utility of maintaining trusted relationships across organizational lines for mutual assistance during a crisis.

An Update on the Arab Spring

A fundamental shift has occurred in political risk calculations in the Arab world. It was argued that in the 1970s, political risk drove oil prices. But today, very high or very low oil prices are affecting political risk. Low oil prices can drive domestic discontent as economic hardship encourages protest movements among the public, while cash-strapped governments lack the resources to maintain order. High oil prices, on the other hand, give autocratic governments free hand in the international community to brutally repress their citizens. Less violence-prone regimes have used increased oil revenues to increase public spending as a way of tamping down discontent. As the Arab Spring spreads across the region, transitions to democracy are making progress, even in places like Egypt, where the military has taken a strong hand in the post-revolutionary environment. Said one Middle-East expert regarding the future of the region: “I’m cautiously optimistic, which for the Middle East is actually pretty optimistic.”

Lessons Learned

Two of the chief lessons learned in the revolutions in Egypt and Libya were the importance of pre-

planning for security, and of maintaining relationships across organizational lines for mutual assistance in times of crisis.

Pre-arranging security operations long before a crisis was seen as critical by participants, who had experienced trouble engaging security companies once the security situation in a given area started to unravel. One participant, speaking of the unrest in the Libyan capital of Tripoli, noted that their company had tried to "hire a security company to give us assistance" evacuating their employees, but that "even the security teams couldn't get into the country." The sentiment was echoed by security professionals in the roundtable, with one adding: "We have crisis management plans in place with our clients — when security firms get a call from someone at the last minute, almost in a panic, often they generally turn them down, because it's too much heavy lifting."

Participants also stressed the importance of staying up to date on potential security problems even in times of stability, to avoid becoming engulfed in an unexpected crisis. "You can be ignored a long time as a security guy when things are hunky-dory," said one participant, "but once crises occur, everyone looks to you. You can't be holding a wet thumb in the air when they're looking at you. You have to have long-established intelligence about events on the ground to get into a position of authority on situational awareness." The ability to be proactive in the midst of a crisis was also seen as crucial. Said one participant, regarding security around the Egyptian revolution: "What really helped was a state of mind: did the crisis control you, or did you control the crisis? I can't emphasize that enough, the psychological aspect of crisis management."

Another key to sustaining operations in a security crisis is participation in inter-organizational groups, which help foster personal connections that can be the source of vital mutual assistance plans. Information sharing through groups like ISMA and OSAC, as well as industry working groups proved very helpful for participants in real-world crises. While information sharing and benchmarking against other firms' actions before and during a crisis can be helpful, the personal relationships are often the most valuable. Said one participant, "The relationship building is one of the most important things we can do. It's coming to organizations like InterCEP which has been very helpful." As an example of the value of these connections, one participant recalled that as NATO airstrikes began in Tripoli, "My boss got in touch with me and said 'can you get in touch with the military and tell them not to bomb our facility?'" This participant had met a military attaché at a conference previously, and this connection provided an invaluable backchannel to put the firm's property on a no-strike list.

Other lessons learned include the importance of making robust evacuation plans before a crisis, which extend from company property to final departure locations. In the words of one participant, "Often, you can get a boat or a plane, but you can't get *to* the boat or the plane. So definitely plan that." Again, the value of standing mutual assistance arrangements was repeated. Another participant noted "One of the things we saw in the Libyan crisis was people trying to go in and out of Benghazi and Tripoli. People had a lot of chartered planes with empty seats coming in and out of those cities. Organizations tried to get their empty seats given to people who needed to get out. But the message never really got out. There should be some kind of mutual assistance understanding before the crisis even starts."

Finally, participants noted the importance of maintaining detailed knowledge of the visa requirements of expatriate employees at all times, in the event that they must be evacuated to another country. Said one participant, "You might know who your expats are, but they're probably married to someone from

yet another country, so you have to worry about getting them accommodated with visas as well. That's a big lesson."

+ Risk Assessment – Identified Risks:

- Social unrest and political turmoil emerging with little warning.
- Breakdown in coordination across organizations during crisis.
- Failure of evacuation plans due to above
- Complication of evacuation plans due to poor foreknowledge of employee visa requirements.

+ Risk Treatment

- Pre-arrange security and evacuation operations during times of stability to ensure their smooth deployment when needed.
- Maintain awareness of potential security problems even in times of stability.
- Establish inter-organizational mutual assistance agreements in times of stability, and sustain them through routine contact and cooperation.
- Maintain detailed knowledge of the visa requirements of expatriate employees and their families, in the event that they must be evacuated to another country.

Roundtable Three

Summary

The growing threat from "hacktivists" and cybercriminals strikes at the heart of the balance between convenience and security inherent in internet commerce. Potential mitigation strategies discussed include robust information sharing between law enforcement and the private sector, reducing technological risks by keeping critical files quarantined from the internet, and creating a culture of security among employees, contractors and everyone else in the personnel ecosystem.

Confronting Hacktivism and Cybercrime

While cybercrimes involving fraud or data theft have been a longstanding concern to the corporate security community, the rise of "hacktivism" increasingly troubles law enforcement and private security officials alike. Hacktivism, the defacement or disabling of an organization's online presence or services, comes in many forms. Usually, the action is taken in the name of a specific cause. The threshold for carrying out hacktivism is relatively low. Said one participant "A skillset and a cause: that's all you need

to be a hacktivist."

Consequently, the damage inflicted by hacktivists generally represents more of a reputational nuisance than a serious operational risk. Occasionally, hacktivist strikes can be very costly. The US Federal Bureau of Investigation (FBI) has addressed hacktivism alongside cybercrime through its cyber-division. The division's priorities are the prevention of (1) State intrusion (state-sponsored, primarily, into federal government networks) (2) Criminal intrusion (into networks for stealing credentials, user information, primarily to get money from banks) (3) Indecent images (primarily exploitation of children), (4) Intellectual Property (counterfeit products and digital media) and (5) Fraud (malware). While hacktivism does not fall neatly into any one of these priorities, the Bureau has made concerted efforts to coordinate with private sector IT-security officers to tackle the issue.

One participant related an incident in which a company in a public-private partnership detected a spike in traffic describing efforts by the hacktivist group "Anonymous" to pick a target for a future assault. The participating government was able to alert the companies on the potential target list, and help to push back the attack before it was launched.

The rise of hacktivism and the spread of cybercrime have accelerated as more business activities move online. For example, traditional banking has been complicated by the use of remote computing. The use of security tokens, which were meant to increase security, has in some cases proved to be significant liabilities. The spread of mobile devices and the diversification of the software environment used by employees have also posed security challenges. At the same time, individuals with malicious intent have become better at the human side of compromising firm IT-security. One participant said that as many as 85 percent of emails received by their firm were illegitimate. Another participant noted that "the targeting is much better now. People even call by phone to get sensitive information from you: they know your manager, they know who you work with, and they know who your friends are."

Participants expressed frustration that little headway seemed to have been made in cyber security since the problem first emerged in the 1990s. Other participants countered that the persistence of the problem could be attributed in part to the delicate balance of convenience versus security that is always weighed in the private sector when it comes to online activities. "For those of us in this room, it's easy, security always wins," said one participant. "But that's not always the case. It's a cost-benefit trade-off. One bank I know cut back on its security department. The management thought the increased loss from fraud was worth it because they could earn more money through increased business because their product is easier to use."

Lessons Learned

Despite the attention paid to technological countermeasures to the cyber threat, for example quarantining sensitive information or systems from the internet, the consensus among participants was that more effort should be directed toward a user-centered approach to cyber security. In the words of one participant, "The weakest link in your system, no matter how much security you put in, is the individual." The entire personnel ecosystem presents potential risks for leaked passwords or other sources of intrusion: employees and their families, temporary workers, neighbors, supply chain partners.

Some participants have reported success along these lines, using disciplinary tactics to create a more attentive security culture at their firms. One participant said “We send targeted phishing emails, and there are incentives for those who don’t click, and penalties for those who do. They get a letter from HR.” Another added that “We have a game at our company: if you walk away from your desk without locking your workstation, you get a red card.”

Potential Projects

Participants suggested two potential points for collaboration among members of the Global Risk Network in addressing the cyber threat. The first is the circulation of best practices on security that ideally improve security while not being too onerous on end users. Alternately, if burdensome security measures are deemed completely necessary, a cross-company group could more effectively persuade members to adopt those measures at once, minimizing the cost and loss of business. One participant added that measures that may seem burdensome when proposed are often not difficult to implement in practice. “When we looked to lock down USB drives, we thought it would be impossible,” said a participant, “but once we did it, it was a nonevent.”

Another potential project for collaboration is an anonymous, non-punitive forum for disclosure of cybersecurity breaches. “I’d love to know what the last three breaches were at company X, and how they happened, without knowing that it’s company X, and with them being comfortable that their report isn’t going to end up in the Wall Street Journal,” said one participant. Other participants cautioned that similar projects have been tried by the US Information Sharing and Analysis Centers (ISACs), with mixed results, because firms believe this kind of reporting to be a competitive disadvantage. The financial services industry, meanwhile, is seen as having had the most success with this type of reporting, seeing the collective security advantage it provides as outweighing any competitive risk.

+ Risk Assessment – Identified Risks

- Proliferation of "hacktivism," the defacement or disabling of an organization's online presence or services.
- Increasing sophistication of cybercriminals, especially in the exploitation of human assets.
- Diversification of software and hardware ecosystems complicates security efforts.

+ Risk Treatment

- Develop a user-centered approach to cyber security.
- Foster a security culture, ensuring that employees are routinely drilled in good cyber security practices.
- Maintain "air gap" security for sensitive information, storing it on devices that are never connected to the internet.
- Foster better inter-organizational information sharing on cyber security breaches.

- Maintain robust information sharing with law enforcement on cyber security issues.

Roundtable Four

Summary

Supply chain executives from major companies described during the roundtable the unique challenges facing their firms' continuity operations around supply chain risk, and room for collaboration among risk network members were explored.

The Challenge of Securing a Diverse Supply Chain

In introductory remarks, one participant illustrated supply chain complexity by pointing to the 30 major suppliers and hundreds of smaller vendors that contribute to manufacturing laptop. He noted that the complexity and interrelationships of supply chains extend far beyond the boundaries of assembly and distribution, from design, to end-users, to competitors within and across industry sectors. To put it one way: "Let's say we've got 80,000 vendors. If you use us, you have at least 80,001 vendors. My supply chain is your supply chain, if you rely on my product. Most of my competitors use the same vendors in my supply chain. "

Among the risks posed by this complexity and the close interrelationships of supply chains is a degradation of risk communications up and down the supply chain. "For example, do I want to share with my suppliers information that's sensitive? Because they might share it with my competitors." According to one participant, "Customers don't always want to tell me about problems, because it might reveal detection methodologies or reveal vulnerabilities that can be shared with competitors."

With this complexity in mind, one participant noted that his firm closely scrutinizes the Business Continuity Plans of its first-level supply chain partners, "and then we talk to *their* suppliers," out to the fourth level of the industry.

The reach of one participant's supply chain also illustrates the challenge in accurately assessing risks to suppliers far down the chain. "The issue is that when it's the supplier who's building the stamped metal that holds the hard drive — the further from HQ, the less control you have," according the participant. "When you have thousands of suppliers, how do you understand enough about them to know what you have to know?"

Participants said that the business case for securing supply chain integrity against risk is becoming easier and easier to make. Counterfeit products are a major concern. For technology companies, it is the threat of malicious software installed somewhere along the supply chain. Physical security is a growing concern, as well. One participant from the security sector noted that their firm has a customer "who uses us for security purposes worldwide for physical security, and they have a separate agreement with us to secure their supply chain."

The Challenge of Preventing Theft, Counterfeiting and Accidents

One senior leader noted that his firm focuses on supply chain integrity in part because "when we do have a disruption, the impact tends to be magnified, because we try to run such a lean operation."

A participant noted that cargo theft incidents in their industry's supply chain are primarily carried out by organized crime with the heaviest threat in Latin America.

It also was noted by a participant that firms in the chemical industry may have special priorities in supply chain risk management related to preventing theft or counterfeiting of their products, or the accidental or deliberate release of dangerous material. Accidental releases in particular can be a significant reputational risk as one participant commented, "one accident can ruin a company." The danger of terrorist attack is also a major concern.

To counter these threats, one leading chemical company operates a global situational awareness fusion center, tracking events around the world and matching them to their potential effects on company shipments. The firm's suppliers must adhere to strict codes of conduct aimed at preventing chemical diversion or other damaging supply chain breaches. Additionally, the firm has made a concerted effort to improve the visibility of its shipments, for example using transmitting tracking devices, bar codes and tamper-evident seals.

Opportunities for Collaboration

Participants identified several points for potential collaboration on supply chain risk management. The first was the potential for future work on improving information sharing between suppliers, customers and shippers. The second was improving metrics on supply chain security, in particular improving the ability to know the true capacity of shippers in terms of resiliency in a crisis, and several participants suggested that representatives from the transportation sector, including shippers and port authorities, should be included in future network roundtable discussions. Participants also noted that there is more work to be done in addressing questions about how to ensure supply chain integrity in countries with weak or non-functioning governments. Another concern was the emerging challenges posed by regulation and the standards industry. Finally, participants stressed the importance of including employee concerns in supply chain risk planning. Said one participant: "Fundamentally you're not going to have people working for you if they don't think their family is secure, so they can go to work with a clear mind."

+ Risk Assessment – Identified Risks

- Degradation of risk communications up and down the supply chain.
- Counterfeit products entering the supply chain.
- Physical disruption of supply chain, through theft or diversion.

+ Risk Treatment

- Analyze the Business Continuity Plans of suppliers

- Promote information-sharing among supply chain partners.
- Reinforce authentication methods for products to decrease counterfeiting.
- Improve tracking methods for goods moving through supply chains to identify and respond to disruptions.

Roundtable Five

Summary

The urgent need for the creation of a global, public-private information sharing network was discussed, stressing the need for communication through enduring and trusted inter-organizational relationships.

Building Better Public-Private Partnerships

Introductory remarks discussed the structure and role of the U.S. Information Sharing & Analysis Centers (ISACs) which are public-private information sharing partnerships covering 18 critical infrastructure areas in the United States. The ISACs have had a good deal of success with anonymous information sharing among their members, particularly in the financial sector, turning this flow into actionable information on emerging risks. Participants agreed that the ISACs (as well as the UK-equivalent Information Exchanges) represent a rare example of valuable and productive public-private relationships, and can provide important models and frameworks for the Global Risk Network.

An Urgent Need to Create a Trusted Network for Information Sharing

Participants agreed that the need for building a trusted network for information sharing between major firms and public sector entities on a global scale is urgent. In the words of one participant: “The timing now is about as critical as it gets.” Emphasis was placed on the ability to reliably share basic facts on the ground, rather than analysis, during a crisis, as a tool to maintain situational awareness. Participants repeatedly expressed caution about the distorting power of the news media during crisis situations, and that there is incredible value in using the shared resources of a trusted, pre-established network to cut through the deluge of conflicting or misleading information that flows from a crisis event. One participant said: “Our CEOs are starting to realize how interconnected we are — especially because of the speed and volume of communication. The value of much of this communication however is questionable. Is media involvement valuable? Usually no. I watch the pictures without the volume.”

Emphasis was placed on the value of good communications. One participant used as an example the 2011 Chilean earthquake, in which strong preparedness practices had kept the death toll from the quake and ensuing tsunami fairly low. Still, the participant said, “about 500 people were killed by the tsunami, and they were killed by bad communications.” After the quake, one participant reported, the country’s president had taken to the airwaves to tell the public there was no tsunami risk, when in fact a tsunami had been triggered. As a result, many of those who should have headed to higher ground, did not, and

lost their lives.

On the enterprise level, a public-private Global Risk Network would have the resources to obtain clear and credible information on emerging threats, and to communicate that information to network members. This information sharing would be facilitated by the trusted inter-organizational relationships the network would foster. As one participant said, "Unless you have relationships in place beforehand, you're in trouble. Anyone who thinks they can ring up the government in the middle of the crisis is deceiving themselves— you're the last person they want to hear from."

+ Risk Assessment – Identified Risks:

- Inaccurate situational awareness by over-reliance on news media coverage of a crisis in progress.
- Poor-quality communications from public and private sources.

+ Risk Treatment

- Establishment of a trusted, confidential information-sharing network that can develop clear understanding of the crisis space.
- Establishment of robust public-private information-sharing channels in times of stability that can facilitate clear communication in crisis situations.

Roundtable Six

Summary

The benefits of public-private partnerships were discussed, along with rationales for engaging with stakeholders outside the traditional risk prevention environment.

Public-Private Partnerships and Policing

Introductory remarks described the role of UNICRI as a public-private partnership working to improve policing around the world. Partnerships like these are especially important in developing countries, where in some cases private sector security is better developed, disciplined and better informed than the local police. This presents an example of when information sharing between the public and private sectors should be a truly two-way street, rather than what is often the status quo of information flowing only from the public to private sector.

Best practices for crime prevention were briefly discussed, including the importance of maintaining situational awareness around a facility and making active contributions to a safe environment for staff and customers outside the gate of any facility. This has the added effect of engaging neighboring

stakeholders in mutual protection. “The benefit is for the wider community,” said one participant.

Participants also discussed the role of employees in crime prevention. For example, staff can report suspicious activity or unsafe conditions they experience on the way to and from work, and this information can be used by management in cooperation with police to solve problems. In the words of one participant, “everybody has a role in preventing crime, inside and out.”

Doing Well by Doing Good: A Business Case for Public-Private Partnerships

While public-private partnerships are often discussed in terms of information sharing from the public to the private sector, it is important to emphasize the support that the private sector can provide to the public sector by way of resources and intelligence. For example one major retail corporation operates a forensics lab that it makes available to law enforcement as a resource. The firm also engages in philanthropy that supports law enforcement and local communities, understanding that stronger law enforcement and more stable and prosperous communities improve store safety. Such programs also have a reputational benefit. In the words of one participant, “let’s say we start up a program that decreases crime 10 percent. How does that help our business? Well, it’s a story we can tell about ourselves, it helps people feel safe enough to keep shopping in our stores, and it helps position us as a thought-leader in the public-safety space.”

In other words, finding meaningful ways to engage the public and to engage other stakeholders in mutual protection is good for business and good for government. Examples include the community building philanthropy, joint public-private security planning, and city partnerships like London First and Mumbai First. Initiatives like these allow firms and public sector organizations to do more with less by engaging across organizational boundaries whenever possible.

Roundtable Seven

Summary

Best practices for effective information sharing and crisis management were discussed. The importance of having effective intelligence before an event and the importance of preparing for disruptions of systems and processes rather than specific events were discussed.

The Benefits of Public-Private Partnership for Counter-Terrorism

Introductory remarks described the work of the United Nations Counter-Terrorism Committee Executive Directorate, a public-private partnership that facilitates technical assistance for matters of counter-terrorism. Participants described intergovernmental and public-private cooperation as crucial for counter-terrorism, for four reasons. (1) Terrorism is anti-modernist but uses the tools of globalization to carry out its attacks. (2) Every field in counter-terrorism can benefit from public-private partnerships. (3)

The private sector is a specific target of terrorism, especially as government installations become more hardened targets. Thus, the private sector benefits from partnering with the public sector in countering terrorist threats (4) The public sector can help protect the private sector from infiltration, and also assists in investments in the developing world, providing increased stability. In the words of the U.N. Director General, "The UN needs businesses. Business also needs the United Nations. The work of the United Nations can be viewed as working to create the ideal environment in which business can thrive."

Identifying and Processing Key Information Sources

Participants identified several key sources of information that must be managed and fused on a daily basis: vendors/suppliers, public sector information, social media, customers, proprietary information from contact centers, market managers, partner firms, and other information from informal sources - primarily in the form of existing personal relationships of corporate officers across organizational lines. The challenge is to collect all of this data and normalize it, but also, in the words of one participant, "to distinguish new news from old news, so we know we're not just hearing old information in a new form, or just a distorted version of something someone heard on CNN."

A steady and well-processed stream of information is key to preventing unwelcomed surprises. For example, risk managers at one participant's firm noticed a surge in Facebook posts suggesting that their industry should be targeted during the G-20 protests in Toronto. Acting on that intelligence, the firm was able to take preventative action. Still, the firm faced risks for which it had not planned. "We hadn't thought about the police using teargas on protestors," the participant said, "and that teargas affected one of our facilities. We also hadn't thought about how the police HQ was right across the street from ours, and that protestors would descend on the police HQ for days to protest. You can plan for months, but you'll never plan for everything."

Crisis Management

The usefulness of planning for disruptions, not specific external threats was underscored by one participant: "It's not the specific event that we need to watch for; it's identifying and protecting the critical processes and material that we need to focus on. It's preparing for the impact, not the threat."

The role of training was cited as crucial from the real-world experience of several participants. One participant noted that their firm is well known for its incident management framework, which is routinely rehearsed "so nobody is scared when they get the phone call to activate it." Another participant noted that in the days leading up to the Toronto protests "what we found invaluable was doing two dress rehearsals on the logistics of getting our contingency site online--things like getting the mail rerouted, moving critical equipment and even having office supplies like copiers and fax machines." Proactive rehearsal of continuity plans led to the discovery of unexpected strengths as well. "We were proactive and realized that in practice our recovery sites weren't fully equipped, so we equipped them and realized we could run the entire company for a week without HQ," said a participant.

The value of keeping clear lines of command in a crisis situation was stressed by several participants. These lines of command should be clear parts of the incident management framework. It is vital for a firm to know who is in charge in a crisis. In the words of one participant, "it's important for the business

people to run the business side of the enterprise. Let the crisis managers manage the crises." Put another way, a participant said that crisis managers should work to "keep your CEO away from crises like civil disruptions. Help them maintain business as usual for as long as possible."

+ Risk Assessment – Identified Risks:

- Organizations caught off-guard by crisis situations due to a failure to properly fuse and analyze incoming threat data on a daily basis.
- Failure of contingency planning in a crisis due to lack of practice in times of stability.

+ Risk Treatment

- Development of a fusion capacity dedicated to analyzing incoming threat information.
- Full rehearsal of contingency plans to ensure their integrity and to train staff in their roles to improve performance in crisis situations.

Roundtable Eight

Summary

The real-world impacts of public-private partnerships were discussed, in terms of information and technology sharing, and especially in the realm of establishing trusted relationships that deliver results in crisis situations. The opportunity for growth of the Global Risk Network was specifically identified as desirable in this regard.

Real Impacts of Public-Private Partnerships

Introductory remarks explained the role of the Overseas Security Advisory Council (OSAC), a longstanding public-private partnership between the U.S. Department of State and 4,000 private-sector organizations, managed by a rotating 30-member council. Private sector partners are able to receive information from the Department of State to answer questions such as "There's an increase in troops outside my gate in Ryadh. Do you know why?" or "We're considering opening an office in a small country in Africa. Do you know who else is there? What's the security situation like?"

The public sector benefits from incident reporting from private sector partners, as well as technological solutions developed by the private sector that can be useful for public sector agencies. OSAC works by synthesizing information from public and private sources and sending that synthesis back out to its members. One benefit expressed by participants was the central role OSAC plays in rumor control. OSAC members learn from each other and have their information vetted and reinforced by government sources. This information is filtered, in many cases, by industry affinity groups. For example, the hotel community has its own internal information sharing network which is connected to OSAC.

However, it was suggested that gaps exist in even in OSAC's reach. A public-private global risk network hosted by InterCEP, at a private university which is nongovernmental and international can foster conversations and undertake projects that OSAC as a governmental entity cannot.

The work of London First was discussed, a non-profit coordinating organization representing 300 of London's biggest employers, describing its mission as "to make London the world's best city in which to do business."

London First will coordinate private sector activities around 100 days of heightened activity between July and September in 2012 around the Olympics as well as The Diamond Jubilee, Notting Hill Carnival, Wimbledon, and the 50th anniversaries of independence of several countries with major immigrant communities in London. Resiliency and security are central to London First's activities, and the organization is using the Olympic event to establish relationships and plans that will be useful in the years beyond 2012.

Finally, participants cited the relationships they built at InterCEP's roundtables as having real effects in business operations. One participant described it this way: "This isn't organizations meeting here, it's individual people. Once you stop thinking about individual people, the value goes out of it. To come on to a call with people I know, that's valuable. But to come into a call with a bunch of strangers — Listen, I have better things to do."

Other participants described the value of reaching across industry silos to discuss common problems. One participant said "I'm getting increasing calls wondering what other companies are doing. It's not even especially about emergency situations. To go outside of my industry is extremely valuable."

As an example of the real world impacts that InterCEP community has already made, one private sector participant discussed meeting a public sector counterpart at a roundtable meeting in Florence, Italy. He went on to describe how that relationship proved invaluable in the evacuation of the firm's staff during the early days of the recent war in Lebanon. "We worked together and got 72 of our people out of the country -- not just our employees, but their families, and some of our clients. I can't emphasize enough how valuable this network is. We got people out before it was too late to get people out. That's how important this network is."