Wharton
University of Pennsylvania

RANE
Risk Assistance
Network + Exchange

KNOWLEDGE@WHARTON

DECEMBER 2014

SHARED RISKS, SHARED SOLUTIONS

Finding the Leading Risk Expertise in an Interconnected World

www.ranenetwork.com • http://knowledge.wharton.upenn.edu

Shared Risks, Shared Solutions

Finding the Leading Risk Expertise in an Interconnected World

THE NATURE, FREQUENCY, AND SEVERITY OF RISK have changed in today's interconnected world, and solutions, whether for prevention, mitigation, or recovery, are often elusive. The issue is not due to a lack of knowledge but the absence of a collaborative network that can offer multidisciplinary insights and assistance in developing strategies at the three inflection points of risk — prevention, mitigation and recovery — according to David Lawrence, founder and chief collaborative officer of RANE (Risk Assistance Network and Exchange), an information services start-up that helps companies and individuals manage risk through collaboration with experts from around the world.

"Risk management should not be a competitive sport or a Darwinian experience for those with fewer resources," Lawrence said at "Shared Risks, Shared Solutions," a RANE event held November 14 in Washington, D.C. "There should be no public vs. private sector, no them vs. us, no you vs. me," added Lawrence, formerly associate general counsel and managing director at Goldman Sachs.

It was in this context that RANE, in partnership with the George Washington University's Homeland Security Policy Institute and Knowledge@Wharton, presented its first in a series of knowledge-sharing events. Experts from the public and private sectors explored not only shared risks and solutions, but also shared responsibilities and opportunities.

While the various panels addressed specific risk-related topics, from climate change and cyber security to terrorism, several key themes resonated throughout the day. These included the need for greater cooperation between the public and private sectors as well as among various private sector players; and the need to truly understand risk, whether imminent or longer term, highly probable or less likely, and the potential outcomes and the consequences of delaying action.

RESPONSIBILITY AND ROLES

With the notion of shared responsibility as a premise, much discussion centered on the roles stakeholders should play in risk management. Deputy secretary of Homeland Security Alejandro Mayorkas raised it in the context of how the government must balance its roles of enforcement and those centered around diagnosis, mitigation and remediation.

Michael Chertoff, executive chairman, Chertoff Group and former secretary of Homeland Security, pointed out the danger in relying only on the government. "If the federal government thinks it has to manage every risk, it's going to overwhelm the federal government," he said. "There are some risks that the federal government ought to be involved in directly and operationally, but for others the federal government can enable the private sector."

With regard to cybersecurity, Stephen Chabinsky, former deputy assistant director, cyber division, FBI, envisioned a "robust system of collaborative task forces or groups that are international and have [representatives from both] the government and the private sector." Such a framework would enable immediate responses under an agreed-upon set of rules. "The discussion in the future is how can the

private sector stabilize situations? How can they restrain with restraint? Similar to how the private sector works in the physical world, how can that be done so that the [U.S.] government and international governments view that as a help?"

The private sector can better cooperate with the government around risk if the government issues "clear and understandable guidelines around the rules of engagement," according to Frances Townsend, former Homeland Security advisor and executive vice president of MacAndrews & Forbes, a holding company with diversified interests in public and private companies. If such guidelines existed, companies, particularly those publicly owned, could better fulfill their fiduciary and legal responsibilities to their shareholders. "But … the government is going to have to provide clear guidance about when the private sector can do more than simply defend itself and when it can take affirmative action."

Several participants cited the lack of guidance as a hindrance to effective risk mitigation and management. Robert Dannenberg, former chief security officer of Goldman Sachs and former senior officer, CIA, said: "From our perspective … you couldn't hack back … where's the help coming from in Washington?" He spoke of the CEO of a competitor calling the White House and saying, "You have to do something about this." The message was clear that the private sector is unwilling to rely solely on the government for both offensive and defensive measures.

Clear rules of engagement will benefit everyone, agreed Robert Hormats, vice chairman, Kissinger Associates, and former undersecretary, Department of State. "The business community can be quite knowledgeable itself. But I think the government at the national level can go in and argue for laws and implementation of regulations that can actually help the business community."

Juan Zarate, former deputy national security advisor, called for a more active role on the part of the private sector in dealing with risks that threaten national security. "The thing that is missing in our national security strategy, whether it's with respect to counterterrorism or more broadly transnational threats and other threats that we face, is thinking about the private sector not as ancillary actors and not as regulated sectors but as protagonists in actually solving problems."

What government used to be able to do through trade sanctions and the like, the private sector, particularly the banks as "gate keepers," can accomplish, according to Zarate. "If you can financially exclude America's enemies from access to capital, access to the elements of the 21st century, global, financial and commercial systems that they actually need to give life and breath to their agendas, then you're going to have strategic impact on their ability to harm U.S. interests."

BARRIERS TO COLLABORATION

A "trust deficit" between the public and private sectors was cited by both Mayorkas and Townsend as a barrier to collaboration and clarity around roles and rights — a function more of mixed messaging than lack of good will or effort. "At a very senior policy level, government officials are sort of lambasting the private sector for greed, corruption and malfeasance, while with a different voice [another part] of the government is either legally requiring the assistance of the private sector, or asking for information," pointed out Townsend. "You need a consistent message." Without it, the necessary partnership between the government and the private sector will be impossible.

> **"The best risk mitigation is in learning and collaboration."**
>
> —Tim Murphy, former deputy director, FBI

Citing his experience working in the public and private sectors, Dannenberg said that informal collaboration was simpler and more effective. "I think the formal structures … for cooperation between the public and private sector have a lot of work ahead of them. There were a lot of things that I wasn't able to share with the government without having to go through the legal structures in my firm to get clearance in order to share. But on the informal level, I think the interaction is really effective."

Dannenberg, Townsend and Mayorkas all pointed out that cooperation is often a function of personal relationships — people knowing whom they *can* call rather than whom they *should* call. "We haven't necessarily built the system or infrastructure to institutionalize that [communication] process," admitted Mayorkas. "That work remains ahead."

INFORMATION SHARING

Yet several panelists pointed out that compliance and security issues sometimes get in the way of the necessary collaboration. "I think the government could provide a little more clarity as to how companies should mitigate certain vulnerabilities, rather than coming out with high

level platitudes," said Tim Ryan, managing director for cybersecurity and investigations at Kroll. "The companies I respond to are usually confused as to the difference between compliance and security. And there is a whole compliance effort there that is not making them secure."

In addition, much of the information the government collects is derived from classified or sensitive law enforcement sources, which makes it difficult to share classified information with parties that don't have a contractual relationship with the federal government.

"We get around that in different ways and we use things like cooperative research and development agreements, and other sort of tortured means to get that done," said Tom Corcoran, chairman's senior policy advisor, House Permanent Selection Committee on Intelligence. He hoped that before this Congress disbands, it would pass legislation to better enable information sharing.

The legislation before Congress would allow the government to provide the private sector with key information about threats, particularly from overseas, that it has collected. The goal is to help block or stop threats. Two other critical aspects of information sharing are getting private sector companies to share best practices with one another, and encouraging private companies to provide tips and leads voluntarily to intelligence and law enforcement agencies.

"This is the most controversial part of what we are doing," Corcoran acknowledged. "I'm not suggesting there is no information sharing going on … but it's not nearly as rich as it could be," he noted, further citing legal concerns as a chief hindrance.

Farah Pandith, former U.S. State Department Special Representative to Muslim Communities, in speaking about geopolitical threats, echoed the need for not only increased public/private partnership but for private/private partnerships. "How do we begin to make that happen?" she asked. The right conversations are starting, "but it's not happening fast enough and it's not happening aggressively enough."

IMMEDIATE VS. LONG-TAIL RISKS

A challenge for virtually all parties in the public and private sectors is risk assessment, whether it is recognizing the danger of long-tail risks as disparate as the effects of climate change in the next 20 or 30 years or the consequences of ISIS's ability to influence young Muslims through social media; or truly grasping the potential of seemingly unlikely threats, and understanding where risk may come from.

"We define risk as threat, vulnerability and consequence, and the interplay between those three," said Chertoff. "So whether it's biological, whether it's cyber, I think the underappreciated risk is the thing that has not yet occurred but has a significant consequence."

FINANCIAL RISKS

Joseph Romm, former acting assistant secretary, U.S. Energy Department, pointed to several risks with unknown timeframes that he believes are not being carefully studied or dealt with appropriately by industries or markets. Those risks include: the likelihood of droughts in several breadbaskets around the world, with consequent high food prices and civil unrest; rising sea levels that will render coastal property virtually worthless; fights over the water supply; and the potential collapse of value in companies that rely on fossil fuels.

"I know for certain we're not going to burn all the fossil fuels that the fossil fuel companies have based their value on … [because] the planet would be rendered uninhabitable. Science is pretty clear on that," Romm said. "Once-in-a-thousand-year events are becoming once-in-a-hundred-year events, and once-in-a-hundred-year events are becoming once-in-ten-year events. The financial system … has internalized but a tiny fraction of what scientists know with high probability is going to happen." Only after the "smart money" begins to price these risks into their transactional and assessment processes will industry and market behavior be influenced, he added.

Caitlin Durkovich, assistant secretary for infrastructure protection, Department of Homeland Security, echoed concern around events with unknown timing. "What really keeps me up at night are these slower-moving risks — aging, failing infrastructure — which are then exacerbated by a changing climate." This one-two punch has been the catalyst for a concerted government effort to develop infrastructure-resilient guidelines that incorporate the challenges of slower-moving hazards and assess the risks with science-based analysis.

In combatting long-tail climate-related threats, often the best time to raise awareness is in moments of crisis, according to Heather McGray, director for vulnerabilities and adaptation, World Resources Institute. "When you've had a significant climate event, there is an openness and an opportunity to bring people together, and start thinking longer term."

The ascendance of ISIS is another example of a continually-evolving but severe risk, based in large part on its ability to leverage social media to win the hearts and minds of young,

digital-savvy Muslims and sympathizers. Tim Murphy, former deputy director, FBI, who chaired a session on geopolitical threats, explained, "The rise of ISIS, the Islamic State, has been a case study on how terrorists have evolved in sophistication despite the multilateral efforts of governments to sanction, freeze assets, engage militarily, undertake counter-messaging campaigns, and shut down their operations. ISIS continues to gain significant support and maintain worldwide reach." Zarate mirrored these points and emphasized that the threat is very real, with multiple points of vulnerability. "It's not because of the immediate threat that ISIS presents attacking in New York, Los Angeles or San Francisco, but it's in the context of how they're innovating and motivating a broader global Jihadi movement."

The physical footprint is not nearly as dangerous as the emotional footprint, emphasized Pandith. "The threat is not today or tomorrow but over the course of a generation," she said. "One fourth of our planet is Muslim; 62% ... is under the age of 30." Muslim millennials are digital natives – and a vast resource for recruitment by jihadist armies.

In dealing with the long-term potential threat posed by ISIS, the best defense is to use the same tools the extremists have used — "the very ones developed by our country," according to Christopher Ahlberg, CEO and co-founder, Recorded Future. "I agree that this is not an imminent threat, even if you're doing business around the world. But what is really interesting is how these guys have done just a perfect Judo move on our social media platforms." He pointed out there are completely legal ways to cull data and intelligence from these platforms, to put it in context, and thus have a greater understanding of the threat and ability to combat it.

The tipping point, Pandith noted, will come from a "normalizing" of the issue through constant and ongoing conversation, and an understanding that there is no immediate solution.

"This is a 10-year, 15-year investment of money and effort, and we're going to be able to tip the balance of how many people are recruited, and then you'll be able to see a positive return on investment (ROI) and that way you'll be able to see change." She pointed out how "normalization" around AIDS and HIV changed their trajectory and impact in the U.S. Also needed, according to Pandith, are counter-message campaigns against ISIS and terrorist threats that have the consistency and staying power of marketing campaigns used by such successful multinationals as Coca-Cola or GE.

PERCEPTION VS. REALITY

Confusing perception and reality is just as dangerous as ignoring long-term threats. The nature of cybersecurity has changed from prevention to immediate detection, immediate containment, and immediate mitigation, pointed out Corcoran, a shift he labeled as "unfortunate." Risk only has three levers. "You can lower the vulnerability, lower the threat, or lower the consequence," he added. "What is really an amazing blunder in the area of cybersecurity is we have spent upwards of $100 billion globally on cybersecurity efforts that are almost entirely focused on vulnerability mitigation."

There is an urgency to switching the focus, according to Joseph M. Demarest, Jr., assistant director, cyber division, FBI, who pointed out that there is concern a threat could move from the cyber realm into something kinetic or physical. Chabinsky cited a recent statement from Europol that it believes that someone will die based on an Internet attack by the end of the year. "It could be things like autonomous vehicles being interrupted or biomedical implants being hacked."

Unfortunately, human nature tends to be such that it often doesn't recognize or accept a threat as real until it is too late, according to Howard Kunreuther, Wharton operations and information management professor and co-director of the school's Risk Management and Decision Processes Center. He noted how both consumers and companies tend not to purchase insurance until after a disaster occurs, citing the example of the Northridge earthquake of 1994, which caused enormous damage in Southern California.

"There is a sense that it is not going to happen to me until after it is too late. Hence one does not consider paying a small premium for protection against a potentially severe loss," Kunreuther said. After a disaster occurs, people focus on the consequences and often invest in protection to reduce their anxiety and gain peace of mind. Several years later they may cancel an existing insurance contract because they haven't suffered a loss.

The most difficult message to get across to people is "the best return on an insurance policy is no return at all. One should celebrate not having a loss," Kunreuther said. "Decision makers often don't focus on the likelihood and consequences of a catastrophe when deciding whether or not to protect themselves against it." He noted that despite these tendencies, firms are now beginning to place more emphasis on triaging and ranking risks. "They are asking themselves what worst-case scenarios should we pay attention to and what is the likelihood of their occurrence?"

Even if a worst-case scenario is unlikely, it still should be acknowledged as part of a crisis-management strategy, particularly in the workplace. Harold Koplewicz, founding president, Child Mind Institute, chaired a panel on the links between mental illness and mass violence in which he emphasized the importance of building systemic approaches to workplace safety and policies that clearly outline guidelines for behavior.

Gene Deisinger, deputy chief of police and director of threat management services, Virginia Tech, spoke about the four main components of workplace safety and security: planning/preparedness; prevention/mitigation; response; and recovery. "Processes" – getting people conditioned to think, act and react are more important than the "product" – preparing them for a specific event. Ensuring processes are in place and creating and shaping an internal work environment allows for the management of crises amid day-to-day operations. Generally, "the true risks are not as great as the fears," he said.

A great illustration of the importance of process came during 9/11. Tom Albright, former chief of the FBI's Crisis Management Unit, told the story of Rick Rescorla, the security chief at Morgan Stanley, who believed the Twin Towers represented a security risk and instituted frequent safety drills. The processes became so ingrained in the corporate culture — due in no small part to the support of senior management — that all 2,700 of the firm's employees survived the terror attacks. The lone exception, sadly, was Rescorla himself, who died when returning to the building to help evacuate others.

While challenges and barriers were constantly mentioned throughout the day's discussions of shared risk and responsibility, there was also shared optimism in the form of real and practical lessons, openness to new ideas, and a willingness of key decision makers to embrace new attitudes and new approaches. Murphy emphasized, "The best risk mitigation is in learning and collaboration." Frank Cilluffo, director, the Homeland Security Policy Institute at George Washington University, who also chaired a panel on cybersecurity, summed up the day by giving a call to action around the fast-changing nature of threats. "What comes across loud and clear is the environment we face … transcends what used to be pretty codified, traditional disciplines," he said. "The best way to predict the future is to shape it." ■

SHARED RISKS, SHARED SOLUTIONS

Finding the Leading Risk Expertise in an Interconnected World

ABOUT KNOWLEDGE@WHARTON

Knowledge@Wharton is the online business analysis journal of the Wharton School of the University of Pennsylvania. The site, which is free, captures relevant knowledge generated at Wharton and beyond by offering articles and videos based on research, conferences, speakers, books and interviews with faculty and other experts on global business topics.

For more information, please visit knowledge.wharton.upenn.edu

ABOUT RANE

RANE (Risk Assistance Network and Exchange) is an information services company created to help enterprises and individuals manage complex risk more effectively through collaboration. We connect the leading risk management experts and service providers with subscriber members seeking solutions to the most pressing and evolving challenges. We provide members unbiased access to:

- Experts from around the world, selected and credentialed by RANE
- Collaboration tools to work with peers and experts
- Curated and original content
- Briefings and events for sharing knowledge, resources, and best practices

RANE was founded on the premise that our collective resources afford far greater protections than any individual approach. We serve both private and public interests, with the firm belief that shared risks require shared solutions.

RANE
Risk Assistance
Network + Exchange

www.ranenetwork.com

KNOWLEDGE@WHARTON

http://knowledge.wharton.upenn.edu