Global Movement Management: Strengthening Commerce, Security and Resiliency in Today’s Networked World

W. Scott Gould, Daniel B. Prieto, and Jonah J. Czerwinski
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgments</td>
<td>5</td>
</tr>
<tr>
<td>Foreword</td>
<td>7</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>9</td>
</tr>
<tr>
<td>I.  The Unique Character of Risk in the 21st Century</td>
<td>19</td>
</tr>
<tr>
<td>II. Intelligent Immunity: A New Approach to Address Global Risk</td>
<td>27</td>
</tr>
<tr>
<td>III. Applying a Global Movement Management Framework</td>
<td>31</td>
</tr>
<tr>
<td>IV.  Strategic Human Capital: Baseline for Success</td>
<td>43</td>
</tr>
<tr>
<td>V.  Technology to Enable Information Sharing</td>
<td>55</td>
</tr>
<tr>
<td>VI.  Governance: A Coordinated Approach</td>
<td>75</td>
</tr>
<tr>
<td>VII. Moving Forward</td>
<td>93</td>
</tr>
<tr>
<td>About the Authors</td>
<td>97</td>
</tr>
<tr>
<td>Acronyms and Glossary of Key Terms</td>
<td>100</td>
</tr>
<tr>
<td>Appendix A. Global Movement Management Analysis of the Maritime Cargo Sector</td>
<td>105</td>
</tr>
<tr>
<td>Appendix B. Additional Detail on Maritime Security Programs</td>
<td>113</td>
</tr>
<tr>
<td>Appendix C. Direct and Indirect Benefits of Security Investments</td>
<td>115</td>
</tr>
</tbody>
</table>

To request additional copies of this paper, please visit: [ibm.com/gbs/government](http://ibm.com/gbs/government)
Acknowledgments

The authors would like to thank their colleagues at IBM for contributing valuable insights and providing support during the process of writing this paper, especially David Amoriell, David Abel, Julie Anderson, Milinda Balthrop, Bryan Barton, Joni Bettge, Robert Biciocchi, Courtney Bromley, Lia P. Davis, Leigh Coen, Igor Frolow, Thomas Glenn, Arnold Greenland, Joi Grieg, Alan Heath, Paul Hempstead, Christer Johnson, Jeff Jonas, Shannon Karl, David Lipstein, Jim Loving, Robert Luby, David McQueeney, HarrietPearson, Mark Purcell, Vic Romita, Richard Rybacki, Laurie Skantze, Leanne Viera and Michael Wilson. In addition, Christian Beckner’s contributions in the preliminary stages of developing this paper, and as the co-author of the first Global Movement Management paper, were critical to this project.

Several outside experts collaborated with the authors in developing the core ideas in this paper. They include Scott Borgerson, Stephen E. Flynn, William K. Hagan, Admiral James Hull, Rob Knake, John Scott and John Raidt. The authors are also grateful for the excellent research support provided by Steven Bogden and Meghann King. Administrative support from Charlyn Isaac and Thealisha Muse also was indispensable. Our editor, Karen Porterfield, provided the highest level of dedication to this work, and we are thankful for her professional commitment. The authors also acknowledge the numerous contributions from colleagues in the federal government at the Department of Homeland Security, Department of State, Department of Defense, and members of Congress and their staff with whom the authors met. Consultations with these individuals helped to inform this paper’s presentation of risk, existing public sector efforts and the critical challenges faced by the nation’s homeland security leadership and its many dedicated practitioners.
Global Movement Management: Strengthening commerce, security and resiliency in today’s networked world

Foreword

IBM introduced its Global Movement Management strategy in 2005 in its paper, “Global Movement Management: Securing the Global Economy.” That paper asserted that, despite the daunting complexity of the myriad global movement systems, virtually all are more alike than different. We believe that policymakers, business leaders and security professionals should focus on these similarities as the key to developing sound strategies for improving the performance, security and resilience of global movement systems while also seeking to preserve core societal values.

Reactions to the central ideas proposed in that first paper were overwhelmingly positive. Many of the stakeholders we engaged – homeland security, military and intelligence officials in the United States; customs, ports and border organizations around the world; Congressional members and staff; think-tank experts; and members of the business community – acknowledged the validity of the central ideas, especially the need for a common vision and framework. Many called for additional depth and detail as they delved into their specific areas of interest. IBM itself realized a deep connection between risks in the global movement system and IBM’s own ability to deliver products and services around the world as a globally integrated firm.

The more we understood the common needs of all stakeholders in the global movement system, the more we came to understand that there is an urgent need for virtually all companies and governments to maintain the health and welfare of global movement systems and strengthen them wherever possible. Furthermore, there is enormous potential to create new markets for products and services that strengthen the global movement system. Finally, a strategic approach to global movement systems can help strengthen public policy, promote greater cooperation between stakeholders and guide investment decisions.
In response to stakeholder requests for more analysis on the subject, we developed this paper, “Global Movement Management: Strengthening commerce, security and resiliency in today’s networked world.” This paper builds on the previous paper in four ways:  
- We analyze risk in the 21st century using a new approach for managing the unique risks facing the global community today.  
- We provide an updated and more comprehensive analytical framework for analyzing strengths, weaknesses, opportunities and threats in specific individual movement systems.  
- We provide examples of how to apply the revised and extended Global Movement Management analytical framework to help guide policymakers, business leaders and the public concerned with strengthening global movement systems.  
- We present a strategy and specific recommendations to build what we call “intelligent immunity” into global movement systems through employing strategic human capital, technology and governance.

Most importantly, this paper presents a strategic vision to guide the efforts of a vast network of stakeholders, a vision that is largely absent from today’s efforts. It is a call to action for individuals, companies and governments to work together to help make the global economy more secure and resilient while improving commerce and protecting privacy. This paper also provides the means for corporations to drive greater harmonization in the global movement system, resulting in lower total costs and higher overall performance. Finally, it provides government and other regulatory organizations with a means to improve security and resilience without harming commercial interests.

There is no doubt that achieving these goals is a challenge with profound economic, human, technological and governmental implications. We invite our readers to engage in this effort to strengthen commerce, security and resiliency in today’s networked world.
Executive summary

The health and well-being of modern society depend on highly integrated, complex economic systems that serve to move people, cargo, conveyances, money and information around the world every day. These systems include, for example, immigration, aviation and transit systems for the movement of people; maritime, trucking and air cargo for the movement of goods; pipelines and electric grids to transport fuels and energy; and the Internet and other communications networks to move information and to enable financial flows. Collectively, these systems comprise a circulatory system for the global economy: what we refer to in this paper as the “global movement system.”

Global movement systems embody a unique intersection of public and private interests. They are largely owned by the private sector, and users are mostly companies and the general public. At the same time, the functioning, availability, security and stability of these systems are essential economic “public goods,” in which governments have significant economic, national security and public welfare interests. Society expects global movement systems to be like water, electricity and other utilities: People simply expect them to work and to be available on demand. When they fail, consequences are rapid, widespread and significant.

Twenty-four hours a day, seven days a week, the global movement system shuttles goods and services, capital and labor, and bits and bytes around the globe to provide the substance of daily life: jobs, wages, food, electricity, education, news and information, and leisure and entertainment. As a result, nations and economies are becoming increasingly integrated and interdependent. The United States relies on the rest of the world to supply two-thirds of its oil and to finance 44 percent of its public debt. China relies on exports for 36 percent of its gross domestic product (GDP). The primary engine of India’s recent economic growth has been information technology outsourcing, even though it accounts for only 5 percent of India’s GDP. Tourism accounts for almost 20 percent of GDP in many Latin American countries. Emerging markets’ share of global exports doubled from 20 percent in 1970 to 43 percent today and emerging markets hold 70 percent of foreign exchange reserves. Africa has recently emerged as a major petroleum exporter and is developing strategic economic relationships with China and India, providing commodities for their rapid industrialization.
Global movement systems as exploitation targets

At the same time, however, the same systems can threaten societies and economies if they are exploited by malicious actors to inflict harm or if naturally occurring disruptions are managed poorly. The tight integration of global systems means that disruptions that may seem small or localized at first can rapidly magnify, spill over into other systems and cause serious harm that is difficult to envision or predict.

These challenges are the natural result of the networked nature and sheer complexity of today’s modern global economy. The effects are well described by chaos theory, which asserts that even relatively simple systems that obey known rules and behaviors can display unpredictable outcomes depending on the slightest variations in the nature of an event or disruption. As individual movement systems become increasingly networked, interconnected and interdependent, small disruptions and events can create an even higher level of unpredictably. Making matters worse, the transmission of disruptions around the world is occurring at an ever faster pace.

Countries today are not alone in facing and influencing the challenges and opportunities of complex internetworked global systems. Fifty-one of the top 100 global economies are companies, 300 multinational corporations account for 25 percent of total global assets, and more than 40 percent of total world trade occurs within corporations.

Individuals have also gained new prominence on the global landscape. As a result of globalization and technology, individual actors can intentionally cause disruptions and inflict damage on a massive scale that was previously the sole domain of nation-states. The September 11, 2001 terrorist attacks undertaken on U.S. soil by 19 individuals at a cost of approximately US$500,000 caused an estimated US$80 billion in damages. The attacks shut down the entire U.S. aviation system. Cascading effects rippled around the world, affecting many countries and industries. As then U.S. Secretary of Defense Donald Rumsfeld lamented, “The cost-benefit ratio is against us! Our cost is billions against the terrorists’ cost of millions.”
The 9/11 hijackers exploited U.S. immigration systems, benefited from poor information sharing within the U.S. government and used our own airplanes as weapons against our centers of finance and government. The 9/11 terrorist attacks drew the world’s attention to the following:

• The efficiency, security and resilience of the global movement system are integrally linked in today’s highly networked and interconnected global economy.

• The drive to improve efficiency has made global movement systems more vulnerable.

• Much of the physical infrastructure in global movement systems is in poor condition due to age, everyday wear and tear, deferred maintenance and underinvestment in new capital projects.

The 9/11 attacks heightened awareness of the fact that while global movement systems are the lifeblood of the global economy, they also present important vulnerabilities and serve as a potential pathway for pathogens and disruptions.

**Security improvements and performance can work together**

Because greater efficiency can make global systems more vulnerable and brittle, many observers assume that the converse is true: that investments in greater security and resilience inevitably must come at the expense of business performance. However, this need not be the case. This paper explains that improvements in security and resilience can help improve overall economic performance. Security and commerce are not in opposition.

Economic performance, security and resilience are mutually reinforcing goals and can be achieved in tandem. In addition, this paper suggests that in a networked economy, business leaders must expand the frame of their investment decisions to give greater weight to considerations beyond their short-term bottom lines and beyond the four walls of their organizations. Company executives need to give greater consideration to their roles in supporting public goods like resilience, stability and the benefits that come with economic interdependence. The same is true for public sector policy makers, who now must consider a broader range of commercial factors in recognition of the private sector’s ownership of and influence over global movement infrastructure. In short, we must learn to realign our thinking to address the networked nature of the global economy.
This paper, therefore, offers a new analysis of the challenges facing countries, corporations and individuals in today’s highly interconnected world. It also proposes a comprehensive framework to improve the performance, security and resilience of global movement systems.

**Key ideas**

The key ideas presented in this paper focus on 21st century risk, intelligent immunity, the Global Movement Management analytical framework, strategic human capital, leveraging unique data assets and skills through technology, and addressing a critical governance gap. These topics are summarized below.

*21st century risk* – Risk in the 21st century is unique because, for the first time, individual actors or individual events pose viable strategic threats to international systems. Threats are asymmetric. Small groups of malicious actors can create global harm many orders of magnitude greater than their cost of operations. Seemingly small local disruptions can potentially cascade and be magnified through tightly interconnected systems to create far-reaching and more extensive damage than often can be predicted. And this trend is forecast to continue.

*Intelligent immunity* – We developed a new approach to guide the formation of policies, plans and implementation efforts to address terrorism and other threats to global economic systems. We call this approach “intelligent immunity.” This approach is designed to address the economic and security risks in global movement systems. It seeks to make critical economic systems more resistant to disruption by improving their overall health. Commerce, security and resilience constitute the essential elements of a healthy system. Achieving this requires an integrated and evolving mix of preemptive, preventive, preparatory and responsive measures that leverage human capital, technology and governance in new ways.

The intelligent immunity approach focuses not only on making systems more secure against intentional threats like terrorism, but also on making them more resilient in the face of virtually all manner of disruptions as well as seeking to improve their overall performance. Intelligent immunity sets the stage for a holistic approach to improve the overall health and well-being of global movement systems while avoiding actions that impede commerce and impair daily functioning.
Global Movement Management framework – A consistent analytical framework is valuable to better understand and assess the complicated systems and subsystems that comprise the global movement system. The analytical framework through which we can understand how to achieve intelligent immunity identifies five key flows – people, goods, conveyances, money and information – as the lifeblood of the global economy.

We broaden and deepen our original Global Movement Management framework to include both the physical and logical aspects of each flow. We provide a robust framework for analyzing the complex global movement systems that make these flows possible, including the global aviation system, maritime cargo shipping, immigration systems and the Internet. The simple yet powerful foundation of the framework is that even the most complex global systems can be reduced to their components, and the systems are more alike than they are dissimilar. Focusing on similarities can provide the means to harmonize decisions, investments and activities to improve performance, security and resilience across the board. The analytical framework can be a valuable aid to guide thinking and action by global leaders to manage risk in global movement systems and achieve common goals.

A strategy to overcome the asymmetric risk posed by terrorism and natural disasters in the highly networked global movement system should link the full range of available tools to achieve these goals. Our analysis suggests three main opportunities to achieve intelligent immunity that involve new strategies for people, technology and governance.

Strategic human capital – We believe that individuals within companies and governments face increasingly complex choices about how to improve performance and address risk. Individual managers and employees face unprecedented volumes of information, new technologies and competitive pressures that complicate their work. At the same time, in a networked economy, decisions made at the individual level can have increasingly global ramifications.

Unfortunately, the critical role of people in managing risk and complexity in a networked environment is often overlooked. From the front office to the front line, people make global movement systems work. We call for a new strategic approach to human capital that transforms the relationship between individuals and their organizations by improving trust and access at virtually all levels. This
results in a greater shared ownership of mission and objectives and empowers individuals to make “the right decisions at the right time.” This approach, adopted by individual organizations in the global community, will help promote intelligent immunity across the entire system.

Strategic human capital requires leaders to employ emerging techniques for managing in a networked environment. These techniques include improved collaboration, latitude to reach across and outside organizational boundaries, investment in organizational transformation, new and more flexible structures, enhanced technology and, above all, greatly improved training for managerial and supervisory skills across the workforce. To address these challenges, we recommend:

• Taking a strategic approach to front-line employees in global movement systems
• Leading, organizing, training and equipping front-line employees for the new tasks at hand
• Engaging society on a more comprehensive basis in recognition of the new level of personal responsibility that each user has for the system in a more connected and interdependent world.

The goal of this effort is to enhance the individual employee’s understanding of his or her important role in improving enterprise performance and reducing risk. We argue that a significant initiative for investing in human capital and establishing standards for human capital development in the areas of security and preparedness will make companies and governments better able to prevent, withstand and respond to disruption. Increased investments in this approach will allow people to assume higher-order responsibilities and automate tasks that do not require human intervention, further leveraging the time that front-line personnel have to focus on their unique contribution to the safe and reliable operation of the global movement system.

Leveraging unique data assets and skills through technology – Those who have managed and operated portions of the global movement system — on the front lines in government or in the private sector — almost universally agree that we need to change how we use technology to simplify work processes and make human activity more effective. Despite widespread recognition of the importance of sharing information, companies and governments are failing to fully
leverage natural advantages that they possess in information and technology to strategically address asymmetric risk in global movement systems. Global Movement Management sets forth a vision for data collaboration on a significant scale to make it easier for individuals to do their jobs, for companies to improve their performance and for societies to maintain the global economy.

This paper sets forth a technology strategy for global movement systems that includes three major components:

• Adoption of a “micro-macro” approach that unlocks currently trapped data to achieve greater information granularity and that promotes greater information federation/aggregation

• Building the “connective tissue” needed to enable greater collaboration both vertically between individuals and organizations, and horizontally among organizations

• Peer production that results from unlocking information and sharing it more widely, helping to drive innovation to dramatically improve the performance, security and resilience of global movement systems.

In sum: Unlock trapped information, share it broadly and create new knowledge and innovation.

We can improve the use of technology to enable individuals to be more effective in their jobs, especially when they have been given the training and authority to make good use of it. More importantly, we can use technology as a strategic advantage by leveraging our ability to manage information to which dangerous elements do not have access – and to do so on a broad scale in order to prevent, detect and interdict malicious activities.

The sharing of currently trapped data will not occur until tools and services become affordable and widely available for data harmonization and interoperability; permissioning, anonymization and encryption; and data aggregation, analysis and visualization. If such tools become widely available and a significant amount of currently trapped data becomes shared, the resulting greater awareness of global systems will help enable companies to improve economic performance by identifying opportunities for improvements in critical economic flows. In addition, this same action will help improve security by making it easier to identify vulnerabilities and to spot anomalies. It also will
help improve resilience by enabling companies and governments to isolate disturbances, avoid overreacting to disruptions, and restart operations more quickly after an event.

Finally, we assert that greater enterprise visibility can help partners and competitors identify mutually beneficial best practices. Upstream companies can be better equipped to provide warnings of supply shortages or other disruptions before they affect downstream partners. Downstream companies can provide early warnings about demand or delivery disruptions to those upstream. Companies can benefit from greater communication with government and law enforcement officials about intentional threats. Governments can augment counterterrorism efforts with more accessible commercial data while also providing a higher degree of protection for privacy and civil liberties than is currently the case. By freeing up trapped data and sharing greater volumes of information, companies and governments can take advantage of open-source techniques or “peer production” to drive innovation and help make global systems more efficient, resilient and secure.

Addressing the governance gap – Governance is the collection of institutions, rules, standards, norms, decision rights, practices and processes that administer, coordinate and/or direct activity within a system or enterprise. Governance for global movement systems is the means by which a diverse and interdependent community of global stakeholders pursues improvements to the performance of global movement systems. Governance of those systems today is characterized by the lack of a coordinated approach that is necessary to address networked risk. We call this the “governance gap.”

To bridge this gap, participants in the global movement systems need to embrace a more comprehensive set of factors to understand the actual risks, costs and benefits that accrue to an organization in a networked environment. Moreover, participants need a means by which to organize their efforts to address these risks, costs and benefits. Our research shows that organizations have successfully met the challenges of organizing efforts across national boundaries in the global movement system before – for example, for international maritime cargo and for the Internet. These success stories provide a model for establishing a new global movement system governance framework.
Therefore, we call for the creation of a Global Movement Management Organization (GMMO) based on key attributes of these models for success. We envision a new international entity to fill the governance gap that presently limits the effectiveness of international efforts. The GMMO can serve to bring together key stakeholders with a shared interest in strengthening global movement systems and provide an effective forum and process to enable cooperation among regional, national and sector-specific stakeholders.

The GMMO can leverage existing international organizations through dedicated and visionary leadership to facilitate three important activities. First, it can align security and resilience with commercial imperatives in global movement systems. Second, it can improve international cooperation and harmonization among public and private stakeholders to strengthen global movement systems. Third, it can integrate security and resilience in a deliberate effort to harmonize risk management activities globally and to enfranchise less developed economic actors through a number of incentivizing mechanisms, including grants, loans, services and training.

Furthermore, as we studied the role of people, technology and governance in the global movement system, several principles that support this GMMO approach emerged: aligning with market incentives, layering horizontal and vertical approaches to improve security, and placing useful information in the hands of front-line employees while helping to ensure that they have the training and authority to act. Improved information sharing will require greater standardization of technologies, tools and protocols. Privacy and other data protections must be addressed at the architecture and design layer. Finally, mechanisms and metrics to measure, assess and optimize policies and programs are required to help make efficiency, security and resilience initiatives work.

In summary, the performance, security and resilience of global movement systems have always been deeply intertwined. September 11 provided a catalyst to invest in security, but, too often, security initiatives have been viewed as being at odds with commerce. This paper supports the idea that commerce, security and resilience are mutually reinforcing objectives. Importantly, we propose a strategy that employs assets that we have, and the terrorists do not. These include large numbers of dedicated people, the better use of technology to unlock trapped commercial data and dramatically improve information sharing and
the formation of international organizations to leverage the combined weight of governments, non-governmental organizations and corporations around the world. This strategy will help to counter the asymmetric risk posed by terrorists and manage the unpredictable consequences of unintentional disruptions. The ideas and recommendations in this paper – promoting intelligent immunity as a means to manage 21st-century risk, applying a global movement management framework, strengthening human capital, making better use of technology and creating a new international governance organization – provide a starting point for stakeholders across virtually all sectors to help build more efficient, secure and resilient global movement systems.
I. The unique character of risk in the 21st century

Risk today is characterized by the rise of the individual as well as the rise of small groups as strategic threats and the speed and unpredictability with which the harmful effects of disruptions in one part of the world can spread to other companies, sectors and countries. Harm generated by small factions at low cost can transmit quickly through highly networked global economic systems and magnify into unexpected and exponentially larger damage. Never before have the risks facing the global economy and international community been more complex and intertwined.

Historically, states have been viewed as the key players in the international economic and political system. States controlled territories and armies. They acted as agents representing their societies on the world stage. Other than disease and natural disasters, states were uniquely capable of inflicting damage to other countries and disrupting the international system. Until the early 20th century, regional wars, natural disasters and disease posed the largest-scale risks to the international system. The two World Wars were, in reality, less “world” wars than extensions of conflicts between regional powers. The threat of nuclear war between the United States and the Soviet Union for most of the latter half of the 20th century made risk truly global for the first time.

Starting in the 1950s and 1960s, scholars and academics began acknowledging the increasing importance of non-state actors such as international organizations and multinational corporations to the international system. By the 1990s, with the end of the Cold War, concerns over global risk shifted to cross-cutting issues – the environment, poverty, HIV/AIDS, drug trafficking, weapons proliferation – that transcended country-to-country or even region-to-region solutions.

Asymmetric risk
The terrorist attacks of 9/11 focused attention on a new form of risk in the 21st century: asymmetric risk. The 9/11 attacks demonstrated that individuals or small groups of actors with malicious intent could intentionally exploit or attack global movement systems and create much more extensive and widespread damage to the broader global economy. To be sure, the risk posed by individual malicious actors or localized events causing much wider systemic harm had been on the rise for
some time due to globalization. (See the sidebar, “Examples of asymmetric risk.”) But 9/11 sharpened attention on asymmetric risk because of the boldness of the attack, the low cost and small number of actors involved, the intentional nature of the disruption and the global repercussions of the event.

The rise of individual (or small groups of) actors and individual events as viable strategic threats to international systems is the unique challenge of the 21st century. (See Figure 1.) This is the dark side of Metcalfe’s law, which states that the power of a network increases by the square of the number of users.\(^\text{11}\) If greater connectivity makes networks more powerful, it is also the Achilles’ heel of networked global systems. In many cases, this challenge has outstripped the ability of traditional hierarchical organizations to respond effectively. This implies the need for a new comprehensive and coordinated approach and global guidance for change.

**Figure 1. Asymmetric risk compared to traditional risk.**

A recent study of supply chain disruptions covering ten years and 861 firms provides a quick measure of the massive impact of even small disruptions like production or shipping delays. After announcement of disruptions, companies, on average, suffered losses in stock valuation of nine percent, or roughly US$130 million per incident, with a cumulative cost of US$112 billion.\(^\text{14}\)
Examples of asymmetric risk

**Internet** – In 1999 a lonely computer programmer in New Jersey named an e-mail virus after an exotic dancer and posted it more as an “act of graffiti” than an intentional act of destruction. The Melissa virus was the first incident of its kind on the commercial Internet and inflicted an estimated US$300-600 million in damages, shutting down approximately 10-25 of the Fortune 500 companies, with an additional 250 disconnecting from the Internet as a precaution. In 2000, a college student in the Philippines authored the I Love You computer worm, which propagated via people’s email contacts in Microsoft® Outlook® Contacts list. Resulting damages were estimated at US$5 billion.

**Finance** – In 1992 Singaporean trader Nick Leeson made a series of successful speculative trades that accounted for 10 percent of the annual profits for his employer, Barings Bank – then the oldest merchant banking company in London. After his initial successes, Leeson began making riskier and riskier trades, incurring heavier and heavier losses, which he hid from his employer. By 1995, he had incurred US$1.4 billion in losses, resulting in Barings Bank’s collapse.

In 1998 the Federal Reserve Bank had to orchestrate a US$3.6 billion bail-out for the Long Term Capital Management (LTCM) hedge fund in order to prevent a wider collapse in financial markets. LTCM was founded by a former vice chairman of Salomon Brothers, and its board members included the Nobel-laureate economists who had invented the techniques for valuing financial derivatives. At the beginning of 1998, LTCM had US$5 billion in equity assets, US$124 billion in debt and US$1.25 trillion of off-balance sheet derivative positions, most of which were in interest rate derivatives. In mid-1998 Russia defaulted on its debt, which threw global financial markets into turmoil and jeopardized most of LTCM’s positions. The firm was losing hundreds of millions of dollars in value per day and within months lost nearly all of its equity value. Fearing that the failure of LTCM could trigger a wider collapse in global financial markets, the Federal Reserve Bank of New York organized a US$3.6 billion bail-out by LTCM’s major creditors.

**Oil and gas** – In the summer of 2004 an insurgent group attacked a southern section of the Iraqi oil pipeline infrastructure. While the attack cost the group an estimated US$2,000 to organize and carry out (and none of the attackers were killed or captured during the attack), Iraqi officials estimated lost revenue to exceed US$500 million, a rate of return for the attackers of approximately 250,000 percent.

In February 2006 the rebel group Movement for the Emancipation of the Niger Delta attacked the loading dock of major oil export platforms in the Nigerian delta region. The attack cost no more than a few thousand dollars, and again there were no casualties. Companies affected estimated their lost revenue to be around US$50 million, a rate of return for the attackers of approximately 25,000 percent.

**Maritime trade** – In September 2002, U.S. West Coast seaports experienced a 10-day lockout resulting from a labor dispute between the longshoremen and port owners. The lockout halted the flow of containers at 29 ports, which normally processed 30 containers a minute, 24 hours a day, worth US$320 billion per year. Within days, a number of auto manufacturing plants had to close for lack of parts, toy and clothing retailers experienced disruptions that affected their holiday sales, produce manufacturers and farmers lost millions of dollars as food items spoiled, U.S. railroads backed up, and Shanghai stopped all shipments to the United States until backlogged ships and containers could start
coming back. As the lockout progressed, the impact on the U.S. economy rose from US$1 billion per day to US$2 billion per day. If the disruption had continued, damage was estimated at US$3 billion per day, or nearly 10 percent of the U.S. Gross Domestic Product (GDP). In the end, the total cost of the disruption was US$10-20 billion. A labor dispute involving 10,500 workers had threatened the jobs of 4 million U.S. workers. It took months to fully recover from the effects of the lockout.22

Manufacturing – Philips NV, a Dutch provider of silicon chips, suffered a small but damaging fire at a U.S. plant in 2000. Philips reestablished production relatively quickly, but the disruption still led to a US$40 million loss that year. A large European mobile phone manufacturer relied on Philips chips as an essential component for their mobile handsets. Because the company was slow to recognize the implications of the Philips fire, its response was delayed, and no source for replacement chips could be found in a timely manner. A seemingly small event at another company and on another continent contributed to the handset manufacturer reporting a financial loss of US$2.34 billion that year.23

Electric grid – In September 2003, storms damaged a power line that supplied electricity to Italy from Switzerland. The sudden increase in demand to other power lines caused a series of cascading failures that cut off electrical power to Italy from France and Switzerland. The resulting blackout affected 56 million people in Italy and Switzerland for up to nine hours. Throughout Italy, all flights and 110 trains were cancelled, with 30,000 people stranded on board.24

In addition to the ability of individual malicious actors or events to create significant asymmetric risk, risk has become more challenging due to other factors as well. First, the networked nature of the global economy means that disruptions are difficult to isolate. Second, disruptions move through systems with much greater speed. Third, the complexity of relationships within global networks makes it difficult to predict the nature and extent of disruption that might eventually occur. Modern complex systems, known by their efficiency, interdependence, ever-decreasing latency and declining availability of spare inventory or capacity, can create highly unpredictable effects that can transmit and magnify what started out as localized disruptions.

These challenges are the natural result of the networked nature and sheer complexity of the modern global economy. The effects are well described by chaos theory. According to chaos theory, even relatively simple systems that obey known rules and behaviors display unpredictable outcomes depending on the slightest variations in the nature of an event or disruption. As individual movement systems become increasingly networked, interconnected and interdependent, small disruptions and events create an even higher level of unpredictability.25
Types of risks facing global movement systems

Much of the damage from a disruption can occur as a result of indirect cascading effects or unintentional self-inflicted damage due to overreaction. Cascading effects comprise the indirect disruptions that occur beyond the original target or point of disruption. Cascading effects impact other sectors and economic assets because of the links between those assets and the originally affected facility or organization. Unintentional self-inflicted damage can unnecessarily exacerbate or even cause new disruptions if companies and governments overreact or react poorly to disruptions. The likelihood of unintentional self-inflicted damage is greater today than in the past. Government and private sector leaders and employees face ever greater complexity, requiring them to have greater levels of technical expertise and knowledge than ever before. In addition, the accelerated speed with which disruptions move through systems requires employees to process more information faster and to make good decisions quickly. Lack of sufficient knowledge about the nature, cause and source of a disruption can make it harder to isolate a disruption and could, for example, lead decision makers to shut down entire systems or delay the reopening of facilities. In short, point risk in networked systems can quickly threaten to become sector risk, which can quickly cascade to other sectors to become contagion risk.

Global movement systems pose other types of risk as well. (See the sidebar, “Seven types of risks to global movement systems.”) Global movement systems can serve as an enabler for malicious actors (e.g., Internet viruses and worms and the use of the Internet as an operational tool by terrorists). They can serve as a vector for weapons of mass destruction (e.g., cargo shipping containers) or a way for terrorists or other dangers to enter a country (e.g., immigration, air travel, the food supply). Some individual sectors are highly vulnerable to terrorism because they provide a mass-casualty target (e.g., mass transit, tourist hubs) or because a key component could be turned into a weapon (e.g., airplanes, rail cars carrying poisonous chemicals, gasoline tanker trucks). In virtually all sectors, disruptions will cause economic damage.

Reducing cascading effects and unintentional self-inflicted damage is an essential component to managing risk in the 21st century. It is clear that better communications, better realtime data visibility and awareness of systems, clearer protocols for isolating events and well-rehearsed playbooks for restarting systems after disruptions would go far to reduce the damage that societies
might unintentionally inflict upon themselves owing to insufficient information or insufficient planning. However, the first step to improving the overall performance, security and resilience of the global movement system is simply to think differently about risk to global movement systems.

Seven types of risks to global movement systems

We have identified seven types of risks posed by global movement systems:

*Enabling agents* – The Internet and other global communications networks have enabled terrorist groups to become significantly more effective at recruiting, organizing, training and planning around the globe. According to senior Egyptian counterterrorism officials, nearly all of the individuals involved in nine significant terrorist conspiracies in Egypt over the last two years were recruited and trained over the Internet. Saudi officials estimate that 80 percent of terrorist recruitment takes place on the Internet.

*Systems as vectors* – Certain global systems, including immigration, maritime cargo shipping, aviation and the food supply, have the potential to serve as a vector to convey terrorists, weapons or other threats into the midst of societies. To address the threat of terrorist entry, immigration policies in a number of countries, including the United States, Australia, France and the United Kingdom, among others, have been tightened, with increased credential requirements for foreign citizens seeking entry. Public officials fear that the global maritime shipping system might serve as a means for terrorists to deliver weapons of mass destruction (WMD) into the United States. In the case of infectious disease, it is feared that the aviation system could help speed the spread of new infectious diseases, causing a global pandemic. This was evident when cases of avian flu in 1997 aroused fears about an H5N1 pandemic, and in 2007 when an American with a drug-resistant strain of tuberculosis ignored orders not to travel and slipped through the global aviation system even though he had been placed on no-fly lists by homeland security officials. Finally, the risk of global economic systems acting as a vector for dangerous items was again made clear in 2007 when a chemical used in China to make plastics and fertilizer was added to wheat, rice and corn products used in the United States and South Africa to manufacture pet food, leading to the death of scores of animals and the contamination of some human food products.
Mass casualty targets – Mass transit venues have been a favorite target of terrorists for decades. Think of the IRA’s terrorist campaign in the 1970s, suicide bombers in Israel since October 2000, the 1995 sarin attacks on the Tokyo subway, and the 2004, 2005 and 2006 attacks in Spain, London and Mumbai, respectively.\textsuperscript{15} Transit targets present concentrated populations within small spaces. At the same time, the “open” ability of the public to enter and exit transit systems easily also makes them difficult to defend. Similarly, tourist venues with a large groups of people in a contained space present attractive targets, as evidenced by the Bali nightclub bombings in 2002.

Weaponization – Parts of various movement systems can themselves be exploited as weapons. The 9/11 hijackers turned airplanes into missiles. There has also been a growing fear that facilities, trucks or rail cars containing chemicals, oil and gas, and nuclear materials could be transformed into bombs, incendiaries or chemical or radiological weapons. The effects of the Bhopal disaster in India in 1984, the generally low security around chemical facilities and transport, and the use of chlorine tankers as chemical bombs by Iraqi insurgents in 2006-2007 make hazardous chemicals a particular worry.\textsuperscript{16}

Economic sabotage – Terrorists have made a concerted effort to target economic systems to inflict mass economic effects as well as casualties. In 2002, Osama bin Laden declared that the al Qaeda attacks would “fill [our] hearts with terror and target [our] economic lifeline.”\textsuperscript{17} The Bali bombings crippled Indonesian tourism for several years afterwards. Terrorists sought to attack the Abqaiq oil refinery in Saudi Arabia in 2006. Experts warn that Iraq has become a “graduate school” for terrorists to train and hone their techniques against critical infrastructure targets, and trends are worrying.\textsuperscript{18} Terrorist groups have, with increasing frequency and sophistication, targeted oil and gas, chemical, electric and water transport and facilities. When, and as, these operatives return home and disperse around the globe, their expertise will pose a significant threat to economic infrastructure targets for many years to come.

Cascading effects – Cascading effects comprise the indirect disruptions that occur beyond the original target or point of disruption. Cascading effects impact other sectors and other economic assets because of the links between those assets and the originally affected facility or organization. The electric grid provides a powerful example of cascading effects that would emanate from a sustained
and widespread disruption. As Paul Gilbert, Chairman of the Panel on Energy Facilities, Cities and Fixed Infrastructure, said in 2003 in testimony before the House Select Committee on Homeland Security:

“Because our critical infrastructure is so completely integrated, with the power out for even a day or two, both food and water supply soon fail. Transportation systems would be at a standstill. Wastewater could not be pumped away and so would become a health problem. In time natural gas pressure would decline and some would lose gas altogether. Nights would be very dark and communications would be spotty or non-existent. Storage batteries would have been long gone from the stores if any stores were open. Work, jobs, employment, business and production would be stopped. Our economy would take a major hit. All in all our cities would not be very nice places to be. Some local power grids would get back up and so there would be islands of light in the darkness. Haves and have-nots would get involved. It would not be a very safe place to be either. Martial law would likely follow along with emergency food and water supply relief. We would rally and find ways to get by while the system is being repaired. In time, the power will start to come back. Tentatively at first, with rolling blackouts and then with all its glory. Several weeks to months have passed, and the clean up would begin.”

Unintentional self-inflicted damage – Finally, one of the major risks in today’s global economy is the risk that societies, governments and economic sectors can harm themselves by overreacting or reacting poorly to certain disruptions. Lack of sufficient knowledge about the nature, cause and source of a disruption can make it harder to isolate a disruption and could lead decision makers to shut down entire systems or delay reopening of facilities. While certainly justifiable in many cases – on 9/11, for example, the decision was made to shut down the entire U.S. aviation system – it is clear that better communications, better access to realtime data and visibility into systems, clearer protocols for isolating events, and playbooks for restarting systems after disruptions, would go far to reduce the damage that societies unintentionally inflict on themselves owing to a lack of sufficient information or lack of recovery procedures in place. Reducing self-inflicted damage is an essential component to improving the resilience of global economic systems.”
II. Intelligent immunity: A new approach to address global risk

A new approach is required to guide the formation of policies, plans and implementation efforts to address terrorism and other threats to global economic systems. This approach would address terrorism within the context of globalization and with recognition of the diverse range of stakeholders in global movement systems. It would address the threat of terrorism but recognize that overreacting to threats or failing to use the full range of tools – economic, social and political, as well as military – could very well pose unacceptable costs on the critical flows of goods, services, money and information upon which the world relies. Admiral James Loy, the former U.S. Deputy Secretary for Homeland Security and Commandant of the U.S. Coast Guard, has publicly called for the need to develop just such a new and unifying approach.¹

We introduce “intelligent immunity” as the construct needed to coalesce strategic thinking about how to counter asymmetric threats. Intelligent immunity also is designed to address the networked nature of economic and security risk in global movement systems. This construct seeks to foster discussion and insight that leads to strategies that will make critical economic systems more resistant to disruption by improving their overall health. Commerce, security and resilience are mutually reinforcing, and they constitute the essential elements of a healthy system.

Achieving this requires an integrated and evolving mix of preemptive, preventive, preparatory and responsive measures that leverage human capital, technology and governance.
As an example, think of the human body with its selective and discriminating reaction to disease. In general, most people do not spend all their time worrying about falling ill. Instead, they undertake certain basic habits to maintain and improve their health and let their immune systems do the rest. Immunity in the human body serves a homeostatic purpose – generally preventing disease and, when required, returning to a steady state of health in response to attack and without harming normal systems. This immuno-response generally does not interfere with normal functioning. The immune system uses the circulatory and other systems of the human body in a coordinated fashion to address the body’s constant encounters with pathogens, employing a network of central regulators (major organs in the body) and a decentralized system of signals (neurotransmitters) that detect and then interdict pathogens with white blood cells. When a body is functioning normally, it responds to threats and problems without jeopardizing itself. It maintains its own internal stability owing to the coordinated response of its parts.

Applying the immunity analogy to the global economy, global movement systems are akin to the body’s circulatory system. Malicious actors or individual disruptions can be equated to pathogens, disease or injury. Central regulators include traditional hierarchical organizations like companies, governments and international organizations. Decentralized regulators encompass the collection of rules, norms and patterns, as well as communications that define markets and condition behavioral patterns and activity at the individual and local level. The intelligent immunity approach focuses not only on helping to make systems more secure against intentional threats like terrorism, but also on making them more resilient in the face of virtually all manner of disruptions and seeking to improve their overall performance. Intelligent immunity sets the stage for a holistic approach to improve the overall health and well-being of global movement systems while avoiding actions that impede growth and everyday commerce.

Adopting an approach of intelligent immunity to global movement systems can help society reduce risk in a way that does not jeopardize the normal functioning of critical economic flows. We maintain health and adopt patterns that adjust to 21st century risks without destroying the things we most want to preserve and that comprise the fabric of our society.
An intelligent immunity approach can also help society reduce the amount of anxiety it suffers about terrorism. Constant warning and discussion may have created an environment where perceived risk is greater than real risk. Fear itself is a desired outcome of terrorism because it drains energy and resources and erodes the social cohesion of those living in fear. Society needs to be aware, vigilant and prepared for terrorism and other disruptions, but it need not sacrifice its values, prosperity and well-being in the name of security.

Furthermore, this approach helps to describe the convergence of logical and physical security in the global movement system. The immune system comprises a number of systems simultaneously: physical systems of blood, veins and arteries; chemical systems of hormones and other neurotransmitters; and psychological and neuromuscular systems where feelings of fear transform from electrical signals to chemical reactions to physical action, with speed, coordination and precision. Analogously, virtually all activity in the global movement system involves the movement of physical and virtual objects as well as the creation and dissolution of associated information – the data and metadata that enable us to manage the global economy.

Most important, an intelligent immunity approach to managing risk for global movement systems has the benefit of treating commerce and security as complementary aspects of an integrated effort, or two halves of a whole. Many key decision makers often view commerce and security in opposition. An intelligent immunity approach allows commerce and security to complement each other in the same system; that is, to be considered as mutually reinforcing objectives within a comprehensive framework. In other words, better security and resilience can improve business performance; improvements in core business operations can improve security and resilience.
To help build intelligent immunity in global movement systems, IBM has developed a Global Movement Management analytical framework. It can be used to describe and analyze any movement system as a series of components and to reveal functional commonalities across systems so as to achieve greater enterprise visibility and provide strategic guidance for action. The Global Movement Management analytical framework can assist policymakers as well as owners and operators of global movement systems to achieve performance gains and security benefits concurrently, thus increasing the intelligent immunity of critical systems against malicious and unintentional disruptions.
III. Applying a Global Movement Management framework

To address economic and security risk in global movement systems, an intelligent immunity approach – from the multinational level through to the individual level – requires an integrated and evolving mix of preparatory, preventive, preemptive and responsive measures. Understanding how best to employ that mix depends on understanding the ways in which the global movement of people, cargo, conveyances, money and information are interrelated.

In IBM’s previous paper, “Global Movement Management:Securing the Global Economy,” published in 2005, IBM presented a framework that organized global movement systems into five key flows and a set of critical functions common to each. Building on that work, we decided to test this framework from a number of different perspectives with leaders from IBM’s supply chain, strategy and change, and human capital management practices, as well as outside experts. These consultations helped to shape a more detailed and refined framework based on a component system analysis of global movement systems (see Figure 2). While the world’s critical movement systems are highly complex, they can be broken down into their components and analyzed to provide powerful insights into how to make them more efficient, secure and resilient.
Elements of the Global Movement Management framework

The Global Movement Management framework uses a component system analysis that can be applied to any individual global movement system (e.g., immigration, aviation, mass transit, the Internet, etc) to help identify its core operational aspects as well as strengths, weaknesses, opportunities and threats. The Global Movement Management analytical framework (illustrated in Figure 3) comprises:

- Five key objects of value
- Five questions
- Five chains of movement
- Five traditional security functions
- Five emerging security functions.
Figure 3. Global Movement Management analytical framework.

Source: IBM Global Business Services.
Five key objects of value – The key flows in the global economy at any given time comprise the existence and movement through time and space of any of five objects of value: people, cargo, conveyances, money and information (see Figure 4). Hence, any economic flow can be described by which one or more of the objects are involved.

Figure 4. The five key objects of value.

Five questions – Essential information is needed about any object moving through the global economy. Therefore, the following five basic questions need to be answered:

- **What is the object?** With any object in transit, it is essential to establish its identity or authenticity. Is the object what it is registered to be, or is it something else? Is the person traveling on a student visa really a student, or is it someone with a false identity document? Even if the person is a known or suspected threat, like one of the 9/11 terrorists, does the computer in front of a border or customs official provide the most complete and up-to-date information? Does the shipping container hold shoes or a nuclear weapon? Is the worker gaining access to a secure area in an airport or seaport who that person says he or she is, and has the person passed appropriate security background checks?

- **Where is the object?** This question addresses the geographic location of an object in transit at any point in time. Is the object at its origin, in transit or at its final destination? Is a shipment of fuel at the oil field, at the refinery or in the tanker truck about to enter New York’s Holland Tunnel? For a traveler, is that person in their home country applying for a visa, on an airplane from Germany to the United States, or already in the United States and, if so, where?
• **When did the object leave/When is it scheduled to arrive?** For most supply chains, a predetermined schedule answers these questions. However, it is as important to understand whether the object at a particular location arrived at the time it was expected to be there, or whether the object has been delayed. To address the “when” question, many airfreight shipping companies offer customers the ability to track shipping information and know when objects pass through key transit hubs and checkpoints. For mega-retailers moving enormous amounts of merchandise, RFID scans of shipments throughout transit allow them to determine if inventories will arrive at stores in time to meet specific regional and local demand.

• **How is the object being conveyed, exchanged, paid for?** Asking “how” in this way can provide other valuable information. Is a person booked to enter the United States by airplane, by boat or over land? How did the person send a shipment: by a trusted carrier or by a smaller company with little transactional history and unknown security practices? How did a person pay for an item: with cash, credit, a new or longstanding bank account, or informal traditional transfer systems like *hawala* financing?\(^3\)

• **Is the object secure?** Has the object been tampered with? Does it pose a risk either to itself or to other objects in the system because of what it contains or how it behaves?

*Five chains of movement* – Any object moving through time and space in the global economy can be represented in a generic “supply chain,” as depicted in Figure 5. Any object moves through time and space, from origin to destination, from the custody of one handler to another and through various control points. As any object moves, governments and companies have in place rules for how it should be handled and treated, and how its movement is recorded. While most people think of physical supply chains, in fact, global movement systems comprise five chains, some physical and some virtual. These five basic chains are described next.

*Figure 5. A generic supply chain.*

Source: IBM Global Business Services.
The supply chain represents the sequential location, custody and control points for any object as it moves from origin to destination. This can mean objects moving through the maritime cargo system, electricity moving through a power grid, a traveler moving through the immigration and air travel systems, or electronic payments moving over the Internet.

The value chain represents the monetary, economic and public-goods value of any object at any point in the supply chain.

The information chain represents the collection, exchange and storage of information about any object as it moves through time and space, from the custody of one party to another. The data chain is a subset of information that is stored and accessible in electronic form, whereas other information on goods may be recorded and stored in non-automated paper form.

The metadata chain is data about data that define uniform categories or like families of information. For example, “Passenger Name” is the metadata category for passenger data such as Jane Doe, John Smith and Mary White; or “Vendor” for a department-store retail chain might include data such as Nike, Champion, Polo and Gucci. Metadata is important because it provides a taxonomy with which to catalog and more easily understand individual data items.

The policy chain represents the rules – imposed by common practice, companies, or governments – that determine how any object is to be handled or inspected at any point in a supply chain; how information or data about any object is to be recorded, stored, exchanged or reported; and how value is to be exchanged and settled for any object at any point in time.

Five traditional security functions – The security risks associated with the five objects of value and the five chains must be managed as objects move through the global movement system. To refine the Global Movement Management framework, we took the original six security and resilience business functions identified in IBM’s previous Global Movement Management paper, adjusted them slightly and added four new functions. We then divided these ten functions into five traditional security functions and five emerging security functions.

Traditional security refers to basic security measures undertaken to reduce vulnerability to crime or an attack. These measures are aimed at hardening facilities; restricting access to facilities or sensitive areas; confirming the identity, examining the provenance, conducting inspections of people and items as they enter a facility or conveyance or while they are in transit; and stopping or seizing
items or people that are suspicious, pose a threat or are not in compliance with certain rules. The dominant response to improve security after 9/11 has, for the most part, focused on these types of activities:

- **Facility security** – These measures include the hardening of targets: building barriers; reinforcing storage units; providing electronic security measures; and adding security guards to patrol, stand watch or escort. These efforts are aimed at deterring, detecting, denying and delaying any improper attempts to access a facility.

- **Conveyance security** – Conveyance security refers to measures taken to protect objects in transit through the hardening of vessels and other steps to prevent theft or sabotage while in transit. These measures may include the use of stronger materials or reinforced construction techniques and increased use of alarms, escorts and tracking.

- **Credentialing, identity verification and provenance** – Credentialing helps ensure that people and objects are who or what they claim to be. Generally, credentials are issued at points of surety, where a credentialing authority is convinced that certain standards of proof have been met. These credentials are stored for future use to help validate claims of identity, content or other conditions. Credentialing information can be used to help manage risk and allocate inspection resources appropriately. Credentialing can also include more than an identity document. Often, officials at control points or in spot inspections will inquire about an object’s provenance, information that identifies its chain of custody, means of transport and path of travel for an object until that point of inspection.

- **Screening and inspection** – These measures help ensure that objects are properly identified and registered. Objects are physically examined, or information about objects (e.g., shipping manifests, bank records, identity documents) is screened to help determine whether objects have been tampered with or might contain dangerous or contraband items. The screening and inspection function helps validate that only lawful or low-risk people or things enter intentional openings in perimeter boundaries, such as ports of entry, and that authorities are able to track the duration of their stay within those boundaries effectively. This function is used throughout the supply chain to allocate additional inspection, enforcement and interdiction resources, and it informs compliance programs such as warnings, training, audits and facilitation programs.

- **Interdiction and enforcement** – This function includes quick actions to address a security incident before it fully materializes. Many other security functions such as perimeter security and tracking are only useful in the context of strong
interdiction and enforcement capabilities. Interdiction and enforcement can include national-level efforts for such activities as, for example, stopping illegal aliens at the border or drug runners on fast boats in the Caribbean, interior enforcement activities, and responses to breaches in physical security and checkpoint security at individual facilities.

Five emerging security functions – The five emerging security functions are, for the most part, aimed at filling gaps in the traditional security paradigm by improving knowledge, awareness, training and decision making. These emerging functions can strongly benefit security while also providing dual benefits to improve core operations and business performance:

- **Enterprise-wide security training** – Security must not be thought of as the responsibility of only dedicated security professionals like security guards and the Chief Security Officer. All personnel, from the CEO to logistics managers to truck drivers, must be taught to think about, understand and implement security in their everyday activities. Organizations need to recognize that everyday employees – not just security personnel – are the eyes, ears and sensors who are often in the best position to spot threats and vulnerabilities.

- **Tracking** – Tracking includes processes and systems to determine the location of objects and help ensure that their location is consistent with what is authorized and expected. It includes the process of attributing custody of items at any time during their movement through a system. It also includes traceability processes, such as tracking backward to find the source or origin of a system disruption (e.g., tainted food or medicine, or WMD materials intercepted in a cargo container). Tracking information can be aggregated to create a comprehensive picture of traffic within a movement system, which can be used both for security and business performance (e.g., inventory management, resource allocation). Tracking can occur in real-time, providing information at virtually all points during transit, or on a periodic but regular basis whenever objects move through control points where data can be collected and transmitted.

- **Risk analysis** – Risk analysis is the analysis of data collected about an object to determine if and what kind of dangers might be posed by that object. Risk management processes information – such as an object’s contents, origin, destination, sender and receiver – in the aggregate, seeking to identify anomalies or discrepancies that warrant suspicion, investigation, clarification or additional inspection. Most important, risk management programs facilitate efficient resource management and the expedited movement of low-risk people and cargo (the vast majority of the flow) by focusing resources on those objects that pose the highest risk.
Enterprise awareness/Command, Control, Communications and Information Integration (C3I2) – Enterprise awareness is a high-level understanding of threats, vulnerabilities and potential impacts based on the aggregation and analysis of data from a variety of sources. C3I2 includes command and control activities that monitor all available information within a system and from related systems, and fuse that information to create timely intelligence about potential threats to the system. C3I2 supports efforts across all business functions to share and analyze data more effectively, improve risk analysis, and improve enforcement and interdiction response times and effectiveness.

Resilience engineering and response planning – Resilience engineering aims to create systems and processes that are robust and flexible, capable of bending rather than breaking when strained or attacked. Instead of focusing solely on physical protection and the hardening of assets, resilience engineering uses data about systems to create backup capacity and contingency plans to significantly reduce the impact of any loss. In addition to engineering, the resilience of a system depends greatly on what actions and decisions take place in response to a disruption. Are employees and executives able to calibrate and exercise response proportional to a disruption? Will they overreact, unintentionally creating additional burdens on the system, which could compound costs and magnify disruptions? The answers to these questions will depend on whether response plans are in place, known and rehearsed, enabling officials to behave in an appropriately measured manner.

See the sidebar, “Global Movement Management and the maritime cargo sector,” for a high-level overview of the maritime supply and information chains. Appendix A, “Global Movement Management Analysis of the Maritime Cargo Sector” provides a ‘real world’ application of the five analytical categories discussed above as well as a detailed depiction of maritime cargo and information flows (see Figure 13).

Global Movement Management and the maritime cargo sector

Maritime cargo comprises 90 percent of global trade. Every day 1.1 million cargo containers move around the globe, and 417 million containers are loaded and emptied every year. Over the next 20 years, the volume of cargo at major ports is expected to more than double and possibly triple. To illustrate the Global Movement Management framework using a real-world example, we applied all five parts of the component system analysis to the maritime cargo sector. Highlights of our analysis:
Technology and Information Management – Throughout the information chain, data is generally of poor quality. Automation is commonly low and paper-based, and manual entry systems dominate. Information is not aggregated or analyzed well and is most often burdened by repetitive data re-entry and re-keying.

Human Capital – Better information management can also allow employees to focus on more value-added activities and engage in training and other activities that improve their awareness, knowledge and vigilance regarding security issues. Individual people throughout the maritime cargo supply chain are critical to security. Individual managers, employees and officials package, load, handle, move, exchange, inspect and screen objects throughout the shipment process.

Governance – Improving technology, information management and human capital point to the need to harmonize best practices across a range of players and countries. This evokes the potential for companies and countries to cooperate on shared interests in improving governance relating to maritime security issues. The range of players involved throughout the maritime supply chain as well as the range of new security initiatives indicate a need to convene key stakeholders in an effort to improve governance and harmonization of efforts within individual enterprises and countries.

Our analysis showed that greater automation and data interoperability in the maritime cargo sector would increase information sharing and improve awareness of the many players involved regarding their part in the maritime supply chain as well as related activities or transactions nearby that may affect them. Reduced manual data reentry would increase the speed of processing objects and increase confidence in the security of objects that individual employees are involved in processing. Freeing up time that would otherwise be lost on managing volumes of paper forms and manual data entry and redundant re-entry could free up human capital for more profitable and productive activities. This could help improve efficiency and performance. The technology and information management capabilities to support this effort would generate both enhanced C3I2 for the private sector and more finely tuned risk analysis for the public sector authorities responsible for security.

Layered security

Traditional and emerging security functions exist at many different levels throughout the global movement system. They exist “vertically” within individual companies and sectors. They also exist “horizontally” and cross over multiple sectors as objects move from supplier to manufacturer to distributor to end user, and from company to company and country to country. Effectively layering security measures both vertically and horizontally is critical to building intelligent immunity in global movement systems.
A layered approach to security (see Figure 6) provides flexibility for owners and operators of systems while also introducing an element of unpredictability, making it harder for a malicious actor to plan and adapt. Layered security can mitigate flaws in individual security measures, help reduce false positives and provide flexibility in an environment that presents complex challenges. Most importantly, a layered approach to securing global movement systems can greatly increase overall security even if individual security measures are less than perfect. (See the sidebar, “Layering security measures increases overall security effectiveness.”)

Layering security measures increases overall security effectiveness

The effectiveness of an individual security measure is fairly weak if its failure rate is 40 percent (e.g., meaning it is effective only 60 percent of the time). However, layering a series of even flawed individual security measures can result in overall effectiveness approaching 100 percent. To illustrate, if security measures A, B, C, D and E each have a 40 percent failure rate, then layering them sequentially increases the probability of successfully stopping an attack to 98 percent. This can be expressed by the following equation:

\[ 100\% - (40\%) \times (40\%) \times (40\%) \times (40\%) \times (40\%) = 100\% - 1.024\% = 98\% \]

This simple mathematical example assumes that every security layer is independent and that measures occur sequentially. In reality, however, security measures need not be independent and sequential. Increasing the level of coordination and harmonization between layers can help increase overall effectiveness even more.
Consider a series of semi-permeable membranes, which must permit the healthy flow of commerce while also filtering out threats to the system. Each membrane possesses passageways that allow people, cargo, conveyances, money and information to pass. The passageways in these membranes can be a mix of channels (which are more regulated and demonstrate a higher degree of sensitivity and differentiation) or pores (which are more passive). The pores and channels in these membranes can be located in different positions, possess different dimensions, and establish different criteria to allow or prevent objects from passing. Together these membranes work more effectively than they would individually. They are even more effective when they are harmonized to mutually reinforce one another. In practice, the metaphorical series of membranes comprises physical control points and infrastructure, a mix of human, technological and procedural screens as well as response, escalation and redress mechanisms.

Arrayed in combination, with an effective level of coordination, a number of imperfect security layers can better prevent disruptions while also maintaining the healthy flow of commerce. Indeed, well-coordinated security layers could even help improve commerce by allowing a false alarm in one layer to be quickly resolved at subsequent and successive security layers.

Achieving good coordination between different security layers can improve enterprise awareness in global movement systems. Systemwide coordination would help ensure that at any given time, the overall security of a system is known and calibrated. However, harmonization among security layers makes it incumbent on owners and operators to be aware of the effects that their decisions in one part of a system will have in other parts of a system and on the system overall.
Outside of military activity, efforts to improve security in the past six years have focused on several notable areas. These areas include government reorganization, technology investment, increased intelligence, stepped-up law enforcement, site hardening, heightened screening and more credentialing. However, less attention has been focused on human capital – the people in industry who manage and operate our vital economic systems and those in government who oversee critical security programs. Below we describe the conditions that make the “people factor” in global movement systems so important and what can be done to improve the performance of people to achieve intelligent immunity in global movement systems.

People are a critical factor in global movement systems

People embody the point of transformation between information and action millions of times a day within critical economic sectors. They provide essential knowledge, skills and abilities as they enable or oversee the global movement of people, cargo, conveyances, money and information. Their activities require decision making and judgment based on myriad factors. These factors include people’s experience that comes from doing their jobs every day including specific, granular and detailed data from IT systems; more general knowledge about markets, systems, people and events in the system; an understanding of the rules, norms and customs that characterize the industry they work in and the organization they work for; and the ability to spot suspicious patterns or activity within systems.

Moreover, individuals within companies and governments face increasingly complex choices about how to improve performance and address risk. They face unprecedented volumes of information, new technologies and competitive pressures that complicate their work. At the same time, in a networked economy, decisions made at the individual level can have increasingly global ramifications. Several observations can be made about the dynamic role that people play in the global movement system. First, the security, resilience and efficiency of global movement systems rest primarily on the human factor. Individual human beings are both the greatest strength in global movement systems and, at the same time, a critical risk factor. People must serve as a starting point for strategies aimed at improving the strength of the system across all flows.
Second, people are essential first-order sensors because they possess both general and specific knowledge of their own environment. It is this specific knowledge that is most difficult to obtain for terrorists and is essential to their operations. Months or even years of detailed casing of a target and relentless rehearsal cannot anticipate fully every contingency, especially without arousing the suspicion of a well-prepared, well-trained and well-coordinated community. During a natural disaster, the people directly affected are in the best position to identify their specific needs and local conditions.

The specific knowledge of time and place, written about extensively by Michael Jensen at Harvard Business School, is by definition the most expensive and difficult knowledge to obtain. It is prized knowledge in a terrorist operation and a strategic and tactical advantage for those who own, operate and seek to protect the system. It is extremely valuable information for a disaster relief coordinator striving to get an accurate picture of conditions on the ground. In both cases, people are essential to improving the security and resilience of a system because they have specific and local knowledge.

For example, a train driver on a subway, a janitor in a building, a postman on a mail delivery route, a sailor in a home port, a customs official at his or her post or a police officer on the beat all share a deep and nuanced understanding of the normal conditions that prevail in their area of responsibility. They have a sense of the people, things and activities that belong in their world. When combined with vigilance and the knowledge and willingness to take a risk and report their observations, front-line personnel can create an invaluable advantage in dealing with terrorists and provide essential information prior to or during an unfolding disaster.

Third, people are the best integrative sensors, able to fuse multiple sources of information and arrive quickly at judgments with insight. While many of the security solutions pursued after 9/11 have focused heavily on technology, technology will provide only a partial solution to improving security and resilience. New security technologies function only as well as the humans that use them. Front-line employees are the eyes and ears of any organization. They are often the best source for up-to-date local information and will often be the first to spot trouble. Well-trained employees provide robust “micro” level information, while at the same time they have the experience required to aggregate and
analyze information at a “macro” level. Strategic use of human capital development is essential to improve risk management because human collection and synthesis of information, decision making and judgment, when combined with well-designed technology, exceed the capability of technology alone.

Fourth, in addition to their role as sensors and collectors, people are the key analysts and synthesizers of intelligence and the critical “deciders” in virtually all operational contexts. People decide between actions that enable commerce or slow it. People decide how to respond to man-made and natural disruptions in a moment of crisis to protect life and property, and to restore systems to normal operation.

**Strategic human capital approach for strengthening global movement systems**

The critical role of people in managing risk and complexity in a networked environment is too often overlooked. From the front office to the front line, people make global movement systems work. We call for a new strategic approach to human capital that transforms the relationship between individuals and their organizations by improving trust and access at virtually all levels. This results in a greater shared ownership of mission and objectives, and empowers individuals to make the right decisions at the right time. This approach, adopted by individual organizations in the global community, will help promote intelligent immunity across the entire system.

This strategic human capital approach requires leaders to employ emerging techniques for managing in a networked environment. Needed techniques include improved collaboration, latitude to reach across and outside organizational boundaries, investment in organizational transformation, new structures, better technology that serves the needs of employees to sift through large amounts of information more effectively, and most importantly, greatly improved training to improve managerial and supervisory skills as well as domain knowledge.

Investments in this approach will help enable people to be able to assume higher order responsibilities by automating those chores best suited for a machine. This also will help improve their ability to manage complex data inputs and support better analysis and judgment as well as help empower them so their decisions are more influential.
We have established that people make global economic systems work. For people to succeed, investments need to be made in a system where people are empowered to:

- Act as innovators within global systems to improve the efficiency of commerce
- Act as the first line of defense to sense anomalies in and prevent disruptions to global systems
- Lessen the chance that terrorists can use the system successfully for ill purposes
- Influence or make the right decisions on how to respond to disruptions to global systems that might occur.

The approach we are talking about is flexible enough to encompass and support the broad range of roles that people play in the system under both normal and abnormal conditions; that is, during day-to-day operations as well as in a crisis. (See the sidebar, “Strategic human capital approaches.”) It is consistent with the current approach to human capital which, at its best, is based largely on a risk management strategy applied to a range of different systems. It is different from the current approach to human capital in that it is our belief that the entire system requires a blended approach to people and technology where the people factor has a primary role in the larger, layered strategy of intelligent immunity that has, until this point, been undervalued – if recognized at all.

Strategic human capital approaches

Here are two practical examples that demonstrate the different but essential roles that people play in their respective systems. In maritime cargo, taking a strategic approach to human capital would involve automating the routine transactions, significantly reducing human intervention, employing risk management techniques to identify abnormal and high-risk transactions, and focusing resources to resolve them. In this system, people would then develop, implement and operate the mitigation programs, perform exception management, make critical decisions and execute through training, warnings, inspections and enforcement. In this case, people follow the evolution of technology. By contrast, in immigration and travel, where people play an important role as primary sensors by meeting and assessing every person who enters their country, a strategic approach to human capital would begin with training and supervision that empowered them to be the first line of defense in this critical flow of the global movement system.
To enhance the positive role of beneficial actors in the system, owners, managers, operators and regulators should adopt three important recommendations:

- Take a strategic approach to front-line employees in global movement systems.
- Lead, organize, train and equip front-line employees for the new tasks at hand.
- Engage society on a more comprehensive basis in recognition of the new level of personal responsibility that each user has for the system in a more connected and interdependent world.

The motivation to participate in these efforts will, of course, differ between commercial and governmental players. But both sectors must realize that neither sector can accomplish its goals without the involvement and positive assistance of the other.

**Take a strategic approach to front-line employees**

A strategy to improve the security, resilience and efficient commercial exchange of global movement systems must encompass people and the different roles that they play on the front lines. It must allow people to easily report anomalies, take action based on their conclusions and provide incentives to bear the risk of doing so. To successfully harness the knowledge of front-line workers, it is essential to co-locate specific and general knowledge together and empower employees to play a significant role in decision making regarding the efficiency, security and resilience of critical systems. Co-location means placing information in the hands of people with the right general and specific knowledge who are also empowered to make decisions wherever they are in an organization.

Front-line workers in global movement systems employ human judgment that can be a source of strength through specific knowledge and training as well as a potential source of weakness through poor decision making, inattention or corruption. A strategic approach to front-line workers requires a different kind of thinking and a higher level of investment in leadership, training and professional development to achieve better quality and innovation in global movement systems. This will require an organizational culture shift in which trust becomes more important, thereby enhancing exchange of information and encouraging front-line employees to act more like owners of the entire mission, not just a narrow portion of it.
A strategic approach aimed at improving front-line performance has a number of important attributes. For example:

• People need to be empowered and incentivized to assume risk and take the initiative by trying new approaches. This means rewarding an employee who suggests a new model that improves the ability to identify and manage risk in the system. It means avoiding penalty if a new suggestion does not yield improved efficiency or effectiveness. There should be trust that an employee’s actions are honorable – for example, if a government employee reaches out to another government agency or the private sector, it should be assumed that he or she is doing so in good faith. It also means providing an environment where employees can freely establish links with other government agencies as well as with the private and non-profit sectors so that front-line employees can learn about innovative homeland security efforts and pilot programs.

• In government especially, managers and supervisors may need some amount of dedicated funding to pay for regularly scheduled training, travel and skills development necessary for informed risk-taking, innovation and collaboration. Professional development is critical to keeping pace with the rate of change in the threat environment.

• Improved incentives and better training will create a more supportive environment where employees can experiment with new techniques and develop innovative strategies. The innovation that results will help to more quickly and accurately prevent or identify and interdict problem actors in the system. The strategic use of employees advocated here goes far beyond simply paying them more or offering additional benefits. It means leveraging their knowledge, performance and commitment as employees and human beings to create a more intelligent, innovative and rapid response to risk – putting more intelligence in intelligent immunity.

• The same investments in people within corporations that have been shown to measurably improve total shareholder return now must be made in the government and non-governmental organizations that exercise extensive influence on global movement systems. Moreover, we argue that increased globalization, liberalization of trade and increased standardization of IT and telecommunications have already given rise to new ways of structuring collective enterprises and organizing people, driving the evolution of the globally integrated firm.
The “circle of influence” for public, private and non-governmental workers on the front line must be broadened to match a new “circle of concern.” Investments in strategic human capital should focus on creating a new organizational culture to perform at higher levels by improving the quality of leadership, the flexibility of organizational structure, availability and effectiveness of training, and better equipment in order to increase security harmonization and coordination across global movement systems.

Lead, organize, train and equip
Greater emphasis must be placed on a variety of actions designed to empower front-line employees. These actions include developing better and more network-proficient leadership; more streamlined organizational structures; enhanced training for domain-specific challenges as well as sound supervisory and management skills; and finally, technology tools to help front-line workers deal with the enormous volume of information that they confront without feeling overwhelmed, and without having the sea of information supplant human judgment.

Leadership – Strengthening global movement systems will require managing change on a massive scale – from a system where security was of secondary concern to commercial imperatives to one where security and resilience become co-equal strategic imperatives. Research studies on change initiatives in the private sector consistently find that effective leadership is essential to the success of major change efforts.\(^5\) Studies of organizational culture change – a concept usually associated with significant organizational reform – also find that leaders play a critical role in forming and transforming organizational cultures.\(^6\) Without strong leadership, no plan for an improved global movement system can succeed.

What makes the leadership challenge of motivating and guiding change in global movement systems so significant is its enormous scope, scale and complexity. We argue that leadership must be exercised on both an individual, organizational and global basis because of the networked and global nature of the system and the widespread cost of disruption. The challenge is enormous, but there is reason to be confident that leaders can improve global movement systems with a comprehensive vision and experience with change management. In addition, leaders must step forward to balance overarching system objectives when a disruption occurs – making difficult decisions under conditions of significant ambiguity.
Organizational structure – Private sector investments in human capital have also been hampered by a failure to understand the strategic nature of security and resilience in global supply chains. Layered security requires coordination among and across layers without compromising the independence of approach that protects the system against a breakdown. (See the Layered security subsection in Section III, “Applying a Global Movement Management framework.”) Changes in function among government agencies and within commercial enterprises have not been followed with changes in structure that will enhance mission accomplishment.

In government, bureaucratic structure often impedes information sharing, cooperation and coordination. Yet slow reaction time between sensing, understanding, deciding and acting is one of the key weaknesses that terrorists try to exploit. We cannot allow our organizations, by design, to hinder the qualities of rapid and adaptive decision making that are needed in the networked world in which we live.

Problems with organizational structure are not confined to the public sector. This can be seen, for example, in the role played by Chief Security Officers (CSOs) in corporations around the globe. Many companies have hired new CSOs since 9/11, made them report directly to the CEO, or increased the resources available to CSOs. For the most part, however, CSOs tend to have skill sets and responsibilities that are narrowly focused on physical and personnel security. While such skills are valuable, they fail to fully account for the strategic nature of security and resilience. Security and resilience encompass more than simply prevention and response, and investments made do not necessarily lead to greater operational costs. That is, investments in security and resilience can benefit core business processes, improve business performance and be a meaningful competitive differentiator.

In the 1990s, IT underwent the kind of transformation that needs to occur now with security. IT ceased being an obscure science and viewed only as a necessary investment for enabling technical and administrative work. Instead, companies learned how to deploy IT as a strategic asset and competitive differentiator. The move of Chief Information Officers from the back office to strategic roles where they had greater involvement in business strategy and implementation unleashed better performance and productivity growth.
A similar change must occur to elevate expectations for CSOs in commercial enterprises to drive business strategy that enhances the prospects for a company’s survival in the face of increased risk to the global movement systems on which it depends. A new reporting relationship for a CSO to the Chief Operating Officer (COO) or CEO of a corporation without a change in the vision, skills, strategy formulation and control over resources, misses the point of creating a position to manage the new kind of risks that will affect the long-term success of large commercial enterprises. Strengthening both leaders and organizations across sectors is a prerequisite of a more secure and resilient system. An essential component of the ability to improve leadership and management of organizations in every sector is the ability to train employees to improve their skills and performance.

Training – We have established that, since public and private sector employees are being asked to do new things in new ways post-9/11, it makes sense to train them to address these new requirements. In the private sector, when we ask employees in an organization to learn a language, master a new computer system, operate a complex machine, interpret a complex policy or manage a billion-dollar project, we typically provide them with the training they need to do so. Furthermore, the new environment also requires organizational transformation to achieve change on a comprehensive level. Here again, training is critical to success. Without widespread understanding and acceptance of the need to address new risks, employees are much more likely to obstruct change.

Better training is essential for employees in global movement systems to make good decisions when faced with anomalies, alarms or disruptions in the course of their work. For example, better training could have played a role in averting the attacks of 9/11, when airport screeners failed to resolve metal detector alarms triggered by the hijackers. Employees also need to be empowered so their judgment, experience and local knowledge can play a greater role in the decision making of the enterprises for which they work. Again in the case of the 9/11 attacks, an airport worker was deeply suspicious of hijacker Mohammed Atta but failed to act on his instincts and did nothing.
Training should cover a variety of important contributors to system security, resilience and efficiency. Training should address the cost of interventions – particularly ones that stop the flow of the global movement system, the legal and privacy policies governing interventions, and risk management as a fundamental driver of programs and operations. Risk management is a well-developed practice in some movement systems. For example, customs officials in many industrialized countries follow well-established standards and widely-recognized “best practices,” such as the World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade. Personnel should be trained on the system’s principles and on the specific risks and mitigation program addressed in any particular stakeholder’s operations. Moreover, training should include an effort to improve the supervisory and management skills of public sector employees. This is especially true in cases where decades of under-funding have reduced spending for training in the civil service to a trickle.

A strategic approach to human capital that involves significantly greater training will not only improve individual employees’ understanding of the important role they play in improving performance and reducing risk, it will also empower employees to take action. According to MIT’s Yossi Sheffi, “In an emergency, people have to be empowered to bypass the normal structure of information. Unless the organization has created the requisite culture of distributed decision-making power, there [will be] numerous barriers to deviations from the normal process.”

If we want the system to perform at the highest and best levels, then we need to invest in training for the people who do the work. We need to teach people to think outside of their own organizational culture norms. Yet governments rely largely on on-the-job training, personal initiative and trial-and-error to fill this gap. Similarly, corporate focus on security training has not reached a level where security is viewed as strategic and woven into the very fabric of a company’s operations. Security and resilience training have not risen to the same level as safety, audit and ethics training in most companies around the world. Given the risks, this simply is not sufficient.

Technology tools – Finally, the relationship between operators and the technologies they use should be improved. Technologies should serve to empower front-line personnel in the primary functions of global movement systems. This can be accomplished in three ways:
1. Unlock and share the data that is vital to a having full understanding of natural and man-made risk in global movement systems.

2. Take existing workflows into account when designing and implementing new technologies. New technologies should enhance the skill, capacity and judgment of people to take action; they should not be a burden or a distraction. To fight terrorism, we must help people to be able to distinguish normal activity from abnormal, to spot linkages and correlations that can help anticipate and prevent disruptions, and to help beneficial actors anticipate and interdict malicious actors before they strike. To enable people to better prepare for and respond to natural disasters, it means supplying vital information from a variety of sources and presenting them in a useful manner under conditions of uncertainty and urgent need. In both cases, co-locating people in the system who have authority with those who have specific knowledge to make timely decisions is critical. Technology and other equipment must be designed to provide data and additional information in context to support decisions on the front line.

3. Build technologies that serve the needs of individual actors in the system by providing specific, timely and granular information about other individuals in the system at the moment of interaction between the system and front-line employees.

These three steps will empower the individual as the baseline unit of action in global movement systems.

**Engage society on a more comprehensive basis**

Technology and the global economy give us the ability to have a different kind of dialog with individuals around the world than we did 50 years ago. Today, we are engaged in an exchange across cultural norms, customs and beliefs as mass media reaches virtually every corner of the world. This has both positive and negative consequences. Policies should incorporate an appreciation for the intended and unintended consequences of this influence and employ the ability to reach people directly through mass media. Leveraging a small part of this medium could help more people understand the benefits to them of global movement systems, the harm that terrorists inflict upon innocents, and the ways in which people can respond to everyday disruptions in a more informed manner. Improved understanding can strengthen intelligent immunity to malicious actors and improve response to natural disasters. This kind of outreach is happening today to combat AIDS, improve environmental policies and habits, and spread micro lending in countries around the world.
Moreover, creating a culture of preparedness improves the resilience of society as a whole. This means that information has to be shared with the public regarding what to do in the event of terrorist attacks or natural disasters and how to respond depending on the nature of the event. Too many officials fear that too much information will frighten the public or aid our enemies. But the more informed and self-reliant we are when the next attack or disaster strikes, the better off every nation will be.

Steps can be taken to promote adoption of a more strategic approach to human capital around the world. First, a governance process is needed to facilitate coordinated action among many stakeholders. We address practical recommendations to accomplish this in Chapter VI, “Governance: A coordinated approach.” Second, a new approach to technology is needed. As the scale and volume of problems increase from natural and man-made causes, people must be an integral part of the effort to sift through information, make a decision and act. People can make quick “reads” of situations that machines cannot.

Today, however, people have to adapt to the IT systems that have been developed. In the future, IT systems must better serve individuals to leverage their unique knowledge, skills and ability to adjust to disruptions, and to stop terrorists’ use of global movement systems. Therefore, technology needs to provide human operators with data and information that enhance decision making and to support rather than supplant human judgment. It should promote greater data interoperability between governments, and owners and operators of global movement systems while also providing robust tools and services for permissioning and visualization.

In addition, the governance systems we create should effectively leverage both people and technology with a strategy designed to lower the cost of the system through harmonization, even as we raise the level of security and resilience in it – an essential approach to engaging the business community in the effort to improve our intelligent immunity. The role of technology in creating intelligent immunity is addressed next in Section V, “Technology to enable information sharing.”
V. Technology to enable information sharing

Having the right information at the right time is essential to maintaining the smooth operation of critical global economic systems in the face of man-made or natural disruptions. Traditionally, this has meant maximizing knowledge within individual institutions. Companies improved their core operations by improving visibility into their own enterprises. Governments acquired and analyzed national and homeland security information within the confines of law enforcement, intelligence and military organizations. But the networked nature of risk in today's world means that the right information at the right time can come from many sources, often outside of the four walls of any one organization. This makes it imperative that governments, companies and individuals more effectively collaborate and share information to manage risk in the 21st century.

Policymakers, business leaders and individual citizens increasingly recognize the imperative for greater collaboration and information sharing. Companies have increasingly invested in information systems that improve data automation and enterprise visibility. Many companies have demonstrated success in strengthening integration with corporate supply-chain partners and even industry competitors. For their part, governments have begun to implement networked strategies. The U.S. military’s concept of network-centric warfare first appeared in the open literature in 1998. Calls for “network-centric homeland security” first emerged in 2004.

Similarly a networked information approach to global movement systems would enhance their intelligent immunity against disruptions. The great challenge, however, is that such systems embody a unique intersection of public and private interests. Global movement systems are largely owned by the private sector, and users are mostly companies and the general public. At the same time, the functioning, availability, security and stability of these systems are essential economic “public goods,” in which governments have significant economic, national security and public welfare interests. Society expects global movement systems to be like water, electricity and other utilities: People expect them to work and to be available on demand. When these systems fail, consequences are rapid, widespread and significant.
The public/private challenge posed by global movement systems has resulted in a situation where stakeholders are generally failing to take full advantage of technology and a wealth of information that is currently trapped locally and in silos of information to strategically address risk in global movement systems. Therefore, to promote intelligent immunity in global movement systems, we present a vision for unlocking terabytes of trapped information and promoting data collaboration between individuals, companies and governments on a large scale. Achieving that vision will make it easier for individuals to do their jobs, for companies to improve their performance and for societies to maintain the global economy in the face of man-made and natural disruptions. At the same time, a comprehensive technology vision for global movement systems will provide guidance to improve data management, enterprise awareness, information sharing and networked collaboration while also addressing concerns over privacy, information security and trust.

The technology strategy for global movement systems that we discuss in this paper includes three major components:

- Adoption of a “micro-macro” approach that combines both greater information granularity and greater information federation/aggregation
- Building the “connective tissue” that enables greater collaboration both vertically between individuals and organizations and horizontally among organizations
- Peer production enabled by unlocking information and sharing it more widely, helping to drive innovation to dramatically improve the performance, security and resilience of global movement systems.

In short: Unlock trapped information, share it broadly, and create new knowledge and innovation.

At the “micro” level, Web 2.0 (discussed below) and mobile technologies allow highly local information to be unlocked. Individuals are empowered to self-publish information and connect that information to one another and to enterprises like companies and governments. Also at the micro level, terabytes of currently trapped corporate data should be unlocked as a necessary step to both achieve Web 3.0 and dramatically improve enterprise visibility.
At the “macro” level, collaboration at scale will occur only when enterprise-class information sharing becomes as “turn-key” as the Web is today and when security and privacy concerns are addressed at the architecture and design layers. This will require protocols, tools and services in the following areas to become increasingly standardized, widely available and cost effective:

- Data harmonization, interoperability and aggregation
- Permissioning, anonymization and encryption
- Robust data analysis, visualization and modeling.

As this occurs, peer production will be able to generate significant innovation to improve performance security and resilience based on greatly improved awareness within global movement systems.

Micro-level Global Movement Management technology strategy

To address the risks posed by complex and interconnected movement systems, solutions must increasingly focus on individual or highly local threats and vulnerabilities. This micro approach requires the availability and collection of ever-more granular, specific and localized information about the individual actors, movements, transactions, handling and other patterns that occur within the global movement system.

Web 2.0: Empowering information from individuals

Web 1.0 marked the advent of the public Internet, in which the mass market adopted e-mail, instant messaging and chat as everyday communications tools and in which companies created a marketing and retail presence to serve consumers via the Internet. Web 2.0 refers to a second generation of Web-based communities and hosted services (e.g., social networking sites, wikis, etc.) that facilitate collaboration and sharing between individual users.

Governments are beginning to sense the potential of interconnected citizens and interconnected employees. Within government itself, officials are increasingly leveraging Web 2.0 tools to connect analysts within the intelligence community and to better leverage open-source information. The U.S. Department of Homeland Security is researching the possibility of using cell phones to detect hazardous biological, chemical and radioactive material. Department of Homeland Security officials believe privately owned cell phones, because of their ubiquity, could be outfitted in production with sensors to monitor the presence of
hazardous materials on a large scale – a transformation from search to surveillance – and that this could be done without the cost of installing static and cumbersome detectors.

Another area where linking individuals to government and corporate networks would create enormous value is in emergency response. During the 2005 London subway and bus bombings, camera-phone users posted to the Internet both still and video images of the aftermath of the explosions. Users also rapidly responded by creating a page on Wikipedia that changed, morphed and was sometimes more up-to-date than live newscasts. Consider the power of a YouTube™-like service to allow both victims and officials in disaster areas to upload important imagery and video footage that could aid situational awareness, improve communications and speed relief efforts after attacks or disasters.

According to a report commissioned by the White House after Hurricane Katrina in the United States in 2004, the “Achilles’ heel” of national preparedness is the ability to identify critical supplies and resources before a disaster strikes and finding and delivering them quickly afterward. After Hurricane Katrina, the commercial classifieds Web site Craigslist™ was the most widely used mechanism for listing missing family members and posting and finding housing. It was often more effective than similar government-provided services. Future disasters are also likely to require specialized response resources, many of which the government may not be in a position to supply.

To address the problem, federal, state and local governments could identify critical supplies and capabilities that they will need – e.g., vaccines, ventilators, generators, electric transformers, laboratory capacity, decontamination equipment, logistics, transport, warehousing – ahead of time and post their needs and requirements to an online marketplace. An eBay®-like online market mechanism to match regional and national-level disaster response needs with companies that can pledge assistance ahead of time or help out in realtime could help save dollars and lives. It would allow state, local and federal governments to inventory available critical assets rapidly and would be much faster than relying on government agencies to create a resource database on their own.
Web 3.0: Unlocking corporate information

There are differing views for what Web 3.0 will comprise. In one leading vision, the Web will evolve into a “Semantic Web,” which acts as a global database and where search has progressed to such a level of sophistication that it can find information based on plain-language queries such as, “I’m looking for a warm place to vacation and I have a budget of [US]$3,000. Oh, and I have an 11-year-old child.”

Such a vision of the Web will never be achieved unless more enterprise data is made interoperable and available and shared widely. Enterprise data – including both government and corporate data, but especially corporate data – is so important because 51 of the world’s 100 largest economies are companies, and 40 percent of world trade occurs within companies. But most current corporate data – millions of terabytes worth – is trapped. It is estimated that between 80-85 percent of all corporate data is not interoperable and not readily sharable.

One major reason for the widespread lack of interoperability of corporate data is the persistence of legacy systems or low levels of information automation. This challenge exists not just within smaller companies and developing countries. Even large companies in well-established industries must continue to upgrade and increasingly automate essential business systems. For example, an IBM study of maritime cargo found that in a “typical” global trade, 35 documents change hands, and data within those documents is re-entered some 1,393 times. This repetitive data re-entry and re-keying accounts for 78.5 percent of all data from trade documents.

Achieving intelligent immunity for global movement systems requires companies to increasingly automate business processes and help ensure that new technologies are designed to enhance, not complicate, the performance of front-line employees. It also requires the increasing integration of physical security measures and logical security measures for IT systems. It would recommend a growing coordination between physical and logical security, and call for the growing integration of the five traditional security functions and the five emerging security functions discussed in Section III, “Applying a Global Movement Management framework.”
Greater access to enterprise data – e.g., manifest, provenance and chain-of-custody data; tracking data; travel and immigration data; and risk-scoring data – is the cornerstone of building intelligent immunity into critical economic systems. It can help decision makers predict, identify and prevent disruptions better, and react more quickly and with more informed judgment. Succeeding in this effort will not only help reduce the likelihood of disruptions but can also allow systems to be more resilient. By allowing more nuanced reactions to disruptions, damage can be isolated, unintentional self-inflicted damage that stems from overreacting to events can be significantly reduced, and systems can recover more quickly.

For example, if a bomb exploded in a shipping container, having robust and searchable data could allow authorities to quickly determine the container’s country of origin. With that information, the global trade system could quickly isolate, interdict and inspect only those shipments with containers from that country. Or imagine a terrorist detonating a tanker truck containing chlorine in Manhattan. Without comprehensive system awareness, a likely reaction would be to overreact and close all tunnels and bridges and inspect virtually every tanker truck. Instead, if local officials could quickly query the databases of trucking companies and chemical suppliers, they might be able to determine the precise location and estimated arrival time for ten inbound chlorine trucks. In that scenario, they could target their interdiction and prevent the shutdown of all bridges and tunnels. Such systemwide awareness would allow companies and governments to isolate disruptions, prevent self-inflicted damage and prevent individual events from shutting down entire sectors, as happened with U.S. aviation after 9/11.

**Macro-level Global Movement Management technology strategy**

A proliferation of micro level data will not be beneficial and could create an overload of information unless data can be federated/aggregated and analyzed at a macro level to enable people to make sense of it. When aggregated and properly analyzed, it becomes easier to identify regular patterns or trends in data against which irregular activity or other outliers can be more readily identified. Better and more information collection at the micro level, if aggregated, analyzed and presented well at the macro level (both within and across enterprises and sectors), can provide a new level of strategic awareness within and across companies and governments. In turn, greater enterprise knowledge can improve the ability to detect, prevent and respond to disruptions. At the same time, selectively sharing
proprietary information can catalyze innovation through the open-source development – or “peer production” – of new techniques to reduce risk and improve commerce.

Achieving this macro approach will require overcoming a number of significant challenges: technology itself (e.g., cost of new investments, persistence of legacy systems, compatibility of different systems), company concerns about competitive issues and liability, and issues of organizational culture and trust.

First order benefits: Enterprise visibility and risk management

Corporate officials have, for some time, recognized the promise of greater enterprise visibility to improve core business operations and reduce fraud. However, the adoption of many of these technologies has occurred only sporadically since companies will always view such investments within a portfolio of options. Not only must a company have the capital to invest, but selected projects must present the most clear-cut return on investment (ROI) when compared to alternatives.

In the mid-to-late 1990s, for example, the technology and telecommunications investment boom saw the creation of a number of satellite-based asset-tracking systems. They had limited success and adoption, however, owing to a combination of cost, performance and ROI issues. Over time, continued technology change has driven the cost of such systems down. The greater risk of fraud and intentional attacks has also increased the appeal of such systems.

Enterprise visibility and information sharing have benefits at multiple levels. Individual companies can clearly benefit from the right investments in systems that improve visibility and information sharing within the enterprise. An example of this is the implementation of RFID tracking technologies within the supply chains of big-box retailers. Many companies also find it beneficial to share information with competitors in the same industry. An example of this is the Postal and Shipping Coordination Council, which comprises a number of major airfreight shipping competitors.

Sharing information can also provide mutual benefits for companies and governments. Recent efforts have sought to increase government’s access to commercial data from global movement systems and to improve information
sharing both within the government and between the government and non-governmental stakeholders regarding critical maritime, aviation, immigration and other movement systems. Many airfreight companies have made tracking information widely available to their customers and some have even increasingly opened their international databases to government officials for counterterrorism purposes. Large players in maritime cargo shipping will increasingly automate their data, and nascent initiatives are underway to share shipping information more broadly. Airlines are using watchlist data from the federal government to screen passengers, and employers are checking employees against watchlists for hiring purposes.

Second order benefits: Innovation from peer production

While the idea of making proprietary corporate data available on the Internet makes many CEOs and company general counsels nervous, the move can have significant benefits that far outweigh any competitive risk. Take, for example the case of Goldcorp. The small Canadian gold-mining firm faced strikes, a shrinking market, and high costs, and it was feared that the 50-year-old mine had run dry. Unless the company discovered new deposits on its existing property, the company would not survive. Company geologists searched the remotest parts of the mine and found evidence of extensive deposits, but after several years of exploration, the company could not find sufficient new deposits to keep the company in business.

Desperate, the Goldcorp CEO took inspiration from the open-source development of Linux. Against the long-held assumption that companies don’t just give away proprietary data, he published on the company’s Web site nearly 50 years worth of all the company’s survey, geologic and other relevant data on the 55,000-acre property. The company announced the Goldcorp challenge in March 2000, offering US$500,000 in prize money to whoever could use the data and point them to potential untapped reserves.

Within weeks, Goldcorp received hundreds of submissions, not only from geologists, but from mathematicians, military officers, graduate students and consultants, who applied capabilities – mathematical modeling, advanced physics, computer simulation and visualization – that exceeded what was practiced within the mining industry. Contestants identified 110 targets on Goldcorp’s property,
half of which had not been identified by the company’s own analysis. More than 80 percent of the new targets yielded significant deposits, amounting to eight million ounces of new gold and cutting years off exploration time.\textsuperscript{77}

The widespread availability of information technologies gives everyone the tools to collaborate and create value. The open and mass collaboration between people and firms to create value and innovation is called peer production.\textsuperscript{78} For firms and governments seeking to promote intelligent immunity in global movement systems, the proposition is simple: “There are always more smart people outside of your enterprise boundaries than there are inside... [T]rust-based relationships with external collaborators... [can] create value more effectively than hierarchically organized businesses.”\textsuperscript{79} According to proponents of peer production, the speed with which a complex project is perfected is directly proportional to the number of informed people working on it.\textsuperscript{80}

If Web 3.0 were to include the unlocking of currently trapped corporate data, it would unlock the possibility of using peer production to revolutionize the security of global movement systems. Not only would mass collaboration help identify opportunities to improve efficiency and reduce vulnerability, it could also catalyze an active developer community, which would create new tools and applications to help enterprises better analyze, visualize and manage their complex systems. Empowering a broad community to link to, analyze and potentially publish to corporate or governmental data could yield powerful and unexpected results.

**Necessary conditions for Global Movement Management’s technology vision**

The public Internet evolved from the Advanced Research Projects Agency Network (ARPANet), which began as a U.S. Department of Defense project in 1962. While it established and relied on a set of common communications protocols,\textsuperscript{81} it remained a niche network until a series of tools for self-publishing and search – e.g., HTML, HTTP, Web browsers – became widely available in the 1990s.\textsuperscript{82} The Internet’s growth was also enabled by abstraction. An electrical outlet can be thought of as “abstracted” from a power plant: To use the power service, you only need to know where the outlet on your wall is and have a plug that fits the socket. The same concept exists on the Internet: Standardized and easy-to-use tools and protocols make it possible for average people to “plug in” and take advantage of complex underlying systems.
As with the shift from the original Internet to the commercial Web, Global Movement Management’s micro-macro approach to unlocking and sharing information more widely will not be viable without cost-effective and standardized tools and protocols. The sheer volume of data, the persistence of legacy systems, and the sensitive nature of much of the private and corporate data in the global movement system mean that Web 3.0 will face greater challenges than Web 1.0 and Web 2.0. Certain conditions will be essential to catalyze and enable the sharing of sensitive data in order to strengthen global movement systems. These conditions must address privacy concerns at the individual level, competitive concerns at the company level and classification concerns at the governmental level. Such conditions include the development and standardization of robust protocols, tools and services for:

- Data harmonization and interoperability
- Permissioning, security, anonymization and encryption
- Data analysis, modeling and visualization, which allow users to readily see trends, anomalies and meaning in what would otherwise be incomprehensible aggregated data.

Figure 7 illustrates the Global Movement Management’s micro-macro technology strategy to address modern risk in global movement systems. It also shows the protocols, tools and services that need to become increasingly standardized to enable information sharing between public and private stakeholders on a significant scale.
Data harmonization and interoperability

Enterprises, whether they are companies, government agencies or countries, are at different stages of technology adoption. They have deployed virtually every conceivable type of system: paper-based systems, homegrown proprietary systems, fully open-source software systems, and systems outsourced to third-party vendors. Given the range of deployed technologies and systems, many enterprises suffer from hidden or missing data, or data that is stored in a highly protected proprietary format, stuck on paper or that simply is not recorded. To enable a diverse range of enterprises to effectively share information at scale, they will need widely available and affordable tools and services to harmonize their data, publish it more broadly and make it interoperable.

At the least, companies need to get their own houses in order before their data can be useful to others. For some companies, this could mean redesigning databases with better metadata tagging through the use of new data standards (e.g., XML or Extensible Business Reporting Language [XBRL]). For other companies, it could mean staying with legacy systems but deploying middleware or service-oriented architectures (SOAs) to translate and harmonize their data, making it more broadly compatible with data from other sources. Companies with older or more manually based processes, and even paper-based recordkeeping, could utilize third-party providers of services to key or scan data into electronic format and add more automation to their systems over time. This potentially would enable today’s under-automated companies as well as entire market sectors to make the leap to having and being able to use interoperable data.

However, greater automation within enterprises will not solve the challenge of data interoperability. Nor is it possible to simply mandate that everyone adopt a single database format. One common approach to harmonizing data across enterprises is to write software programs that translate between individual databases. While practical when dealing with only a few databases, such an approach quickly becomes impractical as the number of data sets grows. For example, if every hospital on a shared network used its own database scheme, the number of data schemes that each hospital would have to coordinate would become unmanageably large. As depicted in Figure 8, as the number of databases goes up linearly, the number of potential connections (any two) increases exponentially.\(^3\)
Another, more efficient approach to data interoperability would be to search for the common elements that exist even between the most disparate data sets. For example, within a given economic sector – such as banking, retail, and medical – there is always some natural overlap between the data used by different enterprises. Focusing on these commonalities and overlaps can provide the core of a solution for harmonizing disparate data sets.

In the 1990s, for example, a major real estate and travel conglomerate needed to find a way to better manage customers across the range of its properties, many of which it had recently acquired. If someone rented a car from their rental car division and stayed at one of their hotels, the company wanted to be able to offer better service and reduce fraud. Any individual traveler on a trip created the same information – e.g., name, address, phone number, payment method, travel dates – for transactions with hotels, car rental companies and other travel properties.

While there were logical overlaps in the data within the conglomerate’s properties, each division had their own separate technology systems. By building a series of filters to pull common data out of non-conforming databases, the company, for the first time, was able to rapidly obtain a unified view of a single customer across multiple properties. With a unified view of the customer, they were able to provide better customer service and build a more cohesive technology architecture over time.
This approach to data harmonization is consistent with Global Movement Management’s core principles: While all critical flows have unique characteristics and are technically complex, at the most basic level, all flows are more alike than they are different and can be analyzed within a common framework. Global Movement Management’s approach to harmonizing and coordinating different databases is similar:

• Focus on the common elements as the core of the solution for better information sharing.

• Choose solutions that leverage legacy technologies by creating interoperability among them rather than seeking to replace legacy technologies outright with new systems.

• Take incremental steps toward information sharing instead of “big bang” approaches to encourage user buy-in, engender user trust, and significantly reduce disruptions to existing workflows and organizational cultures.

Another technique to make data interoperable is through metadata tagging. Metadata is a small set of data that describes another larger set of data. Metadata tagging provides an additional layer of abstraction that allows new meaning to be given to underlying data. For example, financial authorities around the world are increasingly requiring companies to standardize their financial reporting using XBRL. XBRL provides automatic metadata tags for underlying data, making large volumes of data highly interoperable and making it much easier to automate data searches, queries and other analyses.

Permissioning, security, anonymization and encryption

The widespread sharing of corporate data to improve the intelligent immunity of global movement systems raises a number of data sensitivity issues: privacy issues for individuals, proprietary or competitive issues for firms, and sensitive national security or law enforcement issues for governmental authorities. Many of the initiatives to share information between government authorities and the private sector, particularly in the area of homeland security, have encountered problems, in part, because there is a low level of confidence in the privacy protections built into such programs. There are very few best practices or widely accepted standards in place for protecting data while it is in storage or transport. There are few, if any, best practices or commonly accepted standards to govern the sharing of private sector data with the government for homeland security and counterterrorism. Thus, there is a low level of confidence in how government
officials use commercial data for homeland security and counterterrorism, a low level of confidence in redress systems and measures if mistakes are made, and a high level of concern over the protection of individual privacy rights when it comes to the sharing of commercial and government data.

To overcome these issues, a comprehensive regime of identity, permissioning, security, anonymization and encryption needs to be established. The protocols, tools and services for the selective publication, access to and viewing of data need to be standardized, widely available, reliable and easy to use. Technologies and services that allow enterprises to set up robust but easy-to-use permissioning and backed up by strong identity and credentialing technologies would significantly address many of the concerns that currently impede information sharing.

Data access could take several forms. It could be:

- Mediated bilaterally between two entities that want to use data for sharing or collaborating
- Based on group, industry or sector membership (e.g., “chemical manufacturers” or “airlines”)
- Based on functions (e.g., “financial analyst,” “customs”)
- Open, but safe-guarded through aggregation. For instance, cell phone companies can generate traffic congestion maps based on aggregated data on cell phone usage. Someone could observe the traffic information without having the ability to drill down into the phone records of an individual customer.
- Open, as in the case of Goldcorp’s methods described earlier.

Controlling who is allowed to access what data in which enterprise or in which shared community space will be key to building trust in the system. Some users may have view-only access to one company’s database, while others might have full read/write access to a range of enterprises. Permissioning enables enterprise and individuals to share data and services, all in a dynamic manner. Permissions can be turned on and off as the situation demands or opportunity arises. The kind of widespread information sharing across companies, governments and individuals envisioned by Global Movement Management could be thought of as an openly accessible network of many semi-closed networks. To be sure, some data will be openly visible or available, but much of it will require permissions in order to drill down and see more detailed data or to see data at all. Web 3.0 for global movement systems will comprise a common community like the Web, but permissions will be needed to explore many parts of the neighborhood.
Additional layers of security will also be essential. For example, basic encryption of data should become standard practice for any sensitive data, both when it is stored and when it is transported. Encryption would mean that if information is stolen, lost or obtained by unauthorized users, it is unreadable.

A particular type of encryption, anonymization, is of particular interest. Anonymization allows information to be rendered unreadable by humans while it continues to be readable and able to be analyzed by machines. This allows organizations to share, analyze and compare sensitive information more easily while allowing organizations to maintain custody of their data and help ensure security.

As an example, say that public health officials have concerns about a new highly infectious strain of a common disease. Public officials might want to examine tens of thousands of hospital and health insurance records to see if they can identify potential cases of the disease that went unidentified. Private doctors would be challenged to take the time to look through the files themselves, but they would also be reluctant to hand over patient records to public officials for analysis, citing privacy concerns. If the health records were automated and electronically available, anonymization tools could convert the files from “clear text” (e.g., human readable) to a coded form where patient names and other identifying information would not be visible. That way, doctors could provide the data to national officials without worries that patient privacy might be compromised. If national officials found symptom matches, only then would they be allowed to inquire about and decode the actual patient information, based on having the right permissions.

Currently there is no widely accepted or standardized concept of operations (CONOPS) for privacy protection and sharing sensitive data. By providing a CONOPS for pervasive security and permissioning as well as creating the standards and services to easily enable security and permissioning, Global Movement Management’s technology vision could go far to address many of the privacy issues faced by governments and companies when they aggregate and use private data.
Global Movement Management’s micro-macro approach to technology and information sharing could help make widely available the necessary tools and services for the robust permissioning, encryption and anonymization of sensitive data. It could help drive standards that make sensitive data more protected in storage and transport, and it could provide a robust CONOPS for the sharing of sensitive data between the public and private sectors. It could also increase confidence in privacy protections and allay fears about data and identity theft. It could encourage companies to make data more secure as a normal and everyday business practice. Data will be anonymized, encrypted or permissioned so that if it is lost or stolen, it is not “clear text” data that can be used or misused by anyone who ends up with it.

To make all of this possible, a CONOPS for government use of commercial data needs to build privacy protections into the architecture of information sharing. Permissioning, anonymization and encryption need to be built into critical layers and stages of any information sharing processes and relationships. Global Movement Management’s technology strategy could go far to increase the confidence of the members of the privacy policy community and citizens concerned with privacy issues. The standardization and widespread adoption of tools and services for permissioning, anonymization and encryption could help remove a major roadblock to greater cooperation on security related information-sharing efforts between the public and private sectors. One place to start could be to convene a summit between privacy advocates, enterprises that share commercial and consumer data with governments, and government officials to begin to agree on the performance requirements of a comprehensive permissioning and privacy regime. In addition, pilot programs should experiment with various technologies and identify and promote best practices learned from such programs. Such initiatives are discussed in Chapter VI, “Governance: A coordinated approach.”

**Data analysis, modeling and visualization**

There is an enormous difference between data and knowledge. Take, for example a map, which provides a robust graphical interface between the map’s user and a complex array of underlying data. If someone replaced the map with the hundreds of printed pages of all the underlying longitudinal, latitudinal, topographic and other data represented in the map, it would be virtually useless even though it contained all of the data. The same holds true for corporate data. If it is not
effectively represented with robust visualization tools and user interfaces, it quickly loses its value.” Analytical and visualization tools allow users to readily see trends, anomalies and meaning in what would otherwise be incomprehensible data. Good graphic design coupled with robust analytical tools and compelling visualization can help distill an otherwise overwhelming volume of facts, figures and ideas in the shortest time with the least “ink” in the smallest space.”

In the Global Movement Management vision of Web 3.0, enterprises will need to be able to aggregate data and visualize how goods and information move through systems. New user interfaces and enterprise dashboards will enable data analysis and faster anomaly detection. Having reliable access to data reduces friction in industries and enables new business models to be created. Robust analytical and visualization tools will enhance people’s ability to forecast and predict markets, information flows and anomalies and will help enable them to take action when alerted to anomalies or disruptions.

Data that is more widely available, interoperable and better aggregated can enable owners, operators and managers of global movement systems to build computer visualizations and computer-based models to represent and simulate the complex operations of their physical systems and business processes. With such tools, managers and employees will have greater visibility and awareness of their enterprise’s operations, which will allow them to identify opportunities for improvement and areas for risk.

Visualization tools will allow decision making that is better informed and more timely. Simulation models can allow decision makers to improve performance and optimize business processes by testing changes, new initiatives and alternative scenarios within a virtual environment without incurring the cost of experimenting with actual changes in realworld systems. Agent-based models can help predict how policy or process changes will affect the performance of complex systems with multiple stakeholders based on how individual stakeholders react and behave under changed conditions. Finally, simulation and modeling environments can be used to provide robust training and human-capital development opportunities while minimizing the cost and disruption of taking line employees offsite for classroom training or tabletop exercises.
How will greater information sharing for global movement systems happen?

Dramatically improved information sharing for global movement systems will not occur without the wide availability and eventual standardization of the necessary protocols and technologies we have discussed. Yet no single company or government can ensure that these technologies are developed, adopted and standardized. Technology tools and services will need to be developed, and standards and protocols need to be established; then the technologies need to be adopted incrementally in companies, economic sectors and governments. As with the evolution of the Internet and the Web, pockets of innovation and adoption will have to develop, and success will result from a collection of initiatives, innovation, successes and failures within different sectors. Some technologies may be developed by entrepreneurs and adopted simply to improve business performance. Technology adoption also can find support in government requirements and pilot programs. In addition, technology adoption might occur in response to a specific event or disruption within an individual industry.

Greater information sharing for global movement systems will not come about as the result of the intentional design of a central authority. Rather, it will occur as the growth of the Internet did – by the self-interested actions of individuals and sectors. It will occur as the result of successful distributed pockets, or “inkspots,” of success, and it will grow as these pockets are increasingly linked together.

The development of such technologies depends on support from investors and companies, and their implementation depends on support from customers. The broad-based market opportunity related to this vision of Web 3.0 to improve global movement systems is significant.

For example, while the market has had limited success in the past with promoting more widespread information sharing via asset tracking, three things suggest that the next wave of tracking technologies will be more successful:

• Pervasive security concerns after 9/11
• The success of big-box retailers that use comprehensive asset tracking
• The continued decline in costs for data storage and bandwidth.

The desktop security software market could look small compared to a tools and services market to support enterprise-class permissioning, anonymization and encryption of currently trapped corporate data. Indeed, the private sector could
create a market for large-scale data interoperability, data aggregation services and analysis, visualization, and modeling tools.

In the past, such technologies would likely have been built as custom applications for individual clients. Today, however, enterprises do not need to replace existing systems or invest in completely new systems since technology is increasingly available as middleware and services (see Figure 9).

![Figure 9. Technology as services.](image)

Traditionally, critical enterprise functions were performed in the “back office” by what were highly proprietary technology systems that were not intended, nor readily capable of, communicating with the systems of other offices or other organizations. Over time, software vendors began to realize that certain functions did not have to be built from scratch for each individual client. That is, components performing certain functions – e.g., billing, benefits, payroll – could be treated as commodity components that could, with slight modifications, be reused over and over again for different clients. Deploying such applications within a particular form would often require these applications to talk to pre-existing databases. Middleware could act as a “translator box” between a database and a user, translating the source data into a form that can be understood by another application or by a user. Companies and governments have been gradually updating their systems and deploying middleware to transition gradually from legacy systems.
More and more enterprises also are shifting from buying expensive hardware and software to the more cost-effective practice of buying technologies as on-demand services. Such services include storage capacity, processing power, application technologies, operating systems, security, access control and backup, on a remote and outsourced basis.

SOA provides a common way to access services. For example, SOA is a way of designing systems that can be reconfigured easily, are fast to adapt, can be cost-effective and can leverage previous investments in legacy systems. Services should be thought of as reusable components that represent individual business tasks that, when chained together, create a single business process (e.g., billing, credentialing). Services architectures work because they build reusable functions that can be deployed regardless of existing legacy architectures.

Final thoughts
Collaboration and cooperation between public and private interests are critical to achieving intelligent immunity in global movement systems to help make them more resistant to man-made and natural disruptions. To foster this ambitious but critically important undertaking, Global Movement Management calls for a strategic approach to technology that unlocks micro information that is owned by individuals and trapped within companies.

The Global Movement Management’s technology strategy also calls for a macro approach that gives stakeholders in global movement systems the confidence to connect, collaborate and share even sensitive information at scale. That sharing will only occur when protocols, tools and services that protect sensitive information, build trust, and allow robust analysis and visualization of federated data become standardized, cost-effective and widely available. When that occurs, peer production can drive a new wave of innovation to improve the performance, security and resilience of many of the critical systems that both support and maintain societies as well as drive the global economy.
VI. Governance: A coordinated approach

Today’s complex web of global movement systems lacks a coordinated governance mechanism to address networked risk to global movement systems. Governance is the collection of institutions, rules, standards, norms, decision-rights, practices and processes that administer, coordinate and/or direct activity within a system or enterprise. In terms of IBM’s Global Movement Management initiative, governance is the means by which a diverse and interdependent community of global stakeholders pursues improvements to the performance of global movement systems.

Bridging the current governance gap in global movement systems requires that participants in the global movement systems embrace a more comprehensive set of factors to understand the actual risks, costs and benefits that accrue to an organization in a networked environment. Our research shows that similar challenges have been met before by effective organizations in the international community that can serve as a model for establishing a new governance framework for intelligent immunity while leveraging a number of existing international organizations.

Establishing a new global movement systems organization to improve coordination

Similar to how the North Atlantic Treaty Organization (NATO) was created and expanded as an alliance between countries to improve military cooperation and security, and the General Agreement on Tariffs and Trade (GATT) and the World Trade Organization (WTO) were created to advance trade liberalization, the international community would benefit from a new organization to improve the performance and risk management of global movement systems. Therefore, we propose that a Global Movement Management Organization (GMMO) be established. A new GMMO would help the international community to develop new systems of security, trust, organizational culture and skills, and to build governance structures to improve the management of global movement and global integration.

Today there are 7,350 international governmental organizations and 51,509 international non-governmental organizations. These organizations carry out a range of functions in the areas of security, the environment, the economy and human welfare (see Figure 10). To help visualize the existing governance gap,
notice how Security and Trade are at opposite corners in the following figure. No single organization has as its mission the goal of strengthening the global movement system to serve a greater set of stakeholders and their legitimate interests in trade facilitation, security and resilience.

Figure 10. Few international governmental and non-governmental organizations address global risk as it is today.

Governance efforts to improve commerce and better manage global risk should focus on achieving three main goals:

- Promote activities that align security and resilience with commercial imperatives in global movement systems.
- Improve international cooperation and harmonization among public and private stakeholders to strengthen global movement systems.
- Integrate security and resilience with a deliberate effort to connect traditional and emerging security functions globally and enfranchise Tier 3 economic entities.
More specifically, the GMMO and similar efforts by other existing organizations would contribute to a set of measurable goals not currently addressed by the array of entities shown in Figure 10. Governance for global movement systems also applies existing practices in new ways. For example, system performance would be improved through a balanced set of measures to enable accountability and to report performance more effectively. Strategic objectives of an international Global Movement Management governance regime could include:

• Increasing the efficiency of the global trade and travel system by X percent in five years
• Increasing the quality of anomaly detection by X percent in five years
• Improving global chokepoint resilience
• Decreasing the global risk of man-made events by X percent to help lower insurance premiums and other associated costs.

Total quality management suggests “that which is measured also improves.” The same principle applies in the area of governance and system performance in intelligent immunity. What is measured, however, matters as much as that something is measured at all. For example, while a wide range of security efforts and programs have been implemented since 9/11, performance can be difficult to define. The challenge of managing and making use of information is an area that holds promise and would benefit from a more constructive governance framework to measure how this is accomplished. In cases where security initiatives have clear commercial benefits, measurements can often involve traditional business metrics like operational efficiency or revenue or profit increases that result from the measures taken. In other cases, investments and changes will have a “cost avoidance” benefit that may be difficult to measure and should therefore be treated differently. As MIT’s Yossi Sheffi explains, “Costs avoided do not show up on any financial statement, or in any incentive system, and costs incurred [for security outlays] are visible… How do you put a value on avoiding a problem that you don’t have because you spent money to avoid it?”

The GMMO could work with other international organizations, donor governments and companies to address the “digital divide” between the global movement systems of Tier 1 and Tier 3 countries as part of supporting the proposals for dramatically improved information sharing set forth in Section V. Beyond providing individuals with computers, an international governance organization could facilitate and support the provision of technology to Tier 3 companies and governments so they can better automate transactions and
information to more fully participate in global commercial flows. This could be modeled on efforts currently underway by the United Nations Foundation health data systems program, which is working in partnership with a major cell phone provider and mobile network operator to use handheld, open source software to digitize developing countries’ public health information.\(^{95}\)

The GMMO also could consider providing fee-based services to both Tier 1 and Tier 3 countries. For example, smaller companies and the customs organizations of developing countries could pay the organization a modest fee to migrate information from their non-automated or poorly automated systems into an interoperable and shareable form. Providing such a service would allow Tier 3 players to become more equal participants in the data-sharing activities of Tier 1 companies and countries.\(^{96}\) The GMMO might also provide fee-based analysis and storage of data, processing capacity, or visualization tools and services for governments and companies of all sizes. The end result would be that Tier 1 participants are able to interact more effectively with Tier 2 and 3 participants to mutual benefit.

**Governance models**

A survey of popular types of governance organizations that have managed similarly challenging networks reveals four primary governance models (see Figure 11). These options may be used in combination with others or used at different stages of the development of a governance function for improving the performance of global movement systems.

**Figure 11. Four primary governance models for global movement systems.**

<table>
<thead>
<tr>
<th>Prime Mover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dominant participant(s) act based on best practice that delivers both efficiencies and security/resilience to mandate or incentivize compliance by others in the network.</td>
</tr>
<tr>
<td>Legitimate authority extends rules to participants in the network with a degree of accountability.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bottom-Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equally distributed authority, shared risks and advantages, ceding of some sovereignty. This approach typically emerges in relatively nascent relationships and networks without clear or decisive advantages among any single or few participants.</td>
</tr>
<tr>
<td>Legitimacy based strongly on accountability and decentralized decision making.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NGO/IGO/IO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party entity – usually concerned first with a public good – comprised of participant representatives with weighted or consensus-based decision-making.</td>
</tr>
<tr>
<td>Legitimacy is established early, but functioning governance mechanisms evolve slowly with inconsistent membership across the network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaborative environment of participants that include both public and private sector and multiple international organizations. Shared interest of public good and private sector benefits typically stimulate this approach.</td>
</tr>
<tr>
<td>Legitimacy established and confirmed through self selected participation and distributed authorities.</td>
</tr>
</tbody>
</table>

Source: IBM Global Business Services.
A dual-track approach to bridging the governance gap involves both leveraging existing organizations and creating new ones where necessary. We discuss options for leveraging existing organizations later in this section. As for creating a new governance regime for Global Movement Management, we believe that such an entity can be modeled after key elements in two existing entities: the Internet Corporation for Assigned Names and Numbers (ICANN) and the Port State Control framework.

ICANN

ICANN provides governance for the Internet. Like the governance challenge posed by global movement systems, the establishment of ICANN represented a process by which a broad community of public and private stakeholders worked together to design a lasting governance framework. ICANN has been flexible enough to evolve with the commercial, societal and legal challenges and yet durable enough to be valuable at the international level where different cultures and legal systems require a simple and consistent means of interoperating without imposing unwanted changes to existing customs and values.

As the authority responsible for assigning names and coordinates as unique identifiers on the Internet, including domain names and IP addresses, ICANN was essential to the Internet’s success. Today it is managed by an international board of directors drawn from a range of technical, business, academic and non-commercial communities. The non-proprietary and “open” nature of the Internet protocols encourages vendor interoperability, and the lack of central control allows the network to grow organically. Because the Internet is a distributed network of voluntarily interconnected networks, its governance mechanisms are non-invasive, distributed and largely guided by market-driven standards and protocols.

ICANN is a U.S.-sanctioned, private-sector-led body created in 1998 to manage a number of key aspects of the rapidly growing Internet. Internet governance had originally been managed by the U.S. military and National Science Foundation, with input from a range of public and private stakeholders. The World Wide Web experienced explosive growth in the late 1990s, making the Internet a revolutionary new mass-market communications medium and commercial engine. With this unexpected and sharp growth in use and purpose, it became clear that managing this system with a top-down mandate from the U.S. government would no longer suffice.
By acknowledging that the Internet was becoming “an international medium for commerce, education and communication” and that the “traditional means of organizing its technical functions need[ed] to evolve as well,” a governance model was proposed. By issuing a framework document and tasking an executive branch agency (the U.S. Department of Commerce) with facilitating public comment and stakeholder input, ICANN began to emerge. Recognizing the need for a new governance regime, the Department of Commerce invited the Internet’s wide range of stakeholders to develop an acceptable governance structure from scratch. The first of the “Internet constitutional conventions,” which were organized by the International Forum on the White Paper (IFWP), was held in 1998 in Reston, Virginia. Similar meetings followed around the globe to contribute to the design of a new Internet governance body. This approach was taken because “the Internet’s structure was so distributed, and the organizations that built it were so diverse and so informal, however, that no single group, not even the U.S. government, possessed the legitimacy and authority to pull it together on its own.”

In this way, ICANN represents a precedent. The U.S. government delegated to, yet still ultimately controlled, a quasi-private governance regime over a critical system with myriad disparate stakeholders.

Port State Control framework

The Port State Control framework is the result of collaboration among several countries and the international private sector to set and uphold standards for the safety and security of global shipping. The governance model developed for Port State Control provides a useful example of managing private data in a highly competitive environment that concerns several public sector interests. In addition to codifying safety standards, the Port State Control governance framework distributes responsibility for managing protocols and processes through authorities applied across the maritime domain.

In 1978, a number of maritime authorities in Western Europe signed on to the Hague Memorandum for the enforcement of shipboard living and working conditions. A massive oil spill in March 1978 off the coast of France occurred just as the Memorandum was to go into effect. International political pressure demanding that regulations also apply to the safety of shipping quickly followed.
The Paris Memorandum of Understanding (MOU) on Port State Control was the result. The new MOU created a governance framework to enable member countries and the privately owned ships flying their flag to govern compliance with a range of agreed-upon international statutes aimed at security, safety and trade facilitation in global maritime trade. The MOU functions on the basis of several operational and administrative principles that align member states’ regulations and accepted protocols with common practices.

The MOU was adopted in January 1982 by 14 European countries, and went into effect on July 1, 1982. Today, the Paris MOU region includes the European coastal states and the coastal states of the North Atlantic basin from North America to Europe. Port State Control is carried out by a Port State Control Officer (PSCO). The PSCO is a trained individual, authorized to conduct inspections under the maritime authority of the Port State and in accordance with the Paris MOU. All PSCOs are credentialed by their maritime authorities. Through the SAFE Framework, the WCO established a similar framework for global supply chain security standards and best practices. Similar to the Paris MOU, the SAFE Framework is not governed in a top-down fashion, as each country is free to adopt its own standards and policies. However, the SAFE Framework – again, like the Paris MOU – does establish a broad set of standards and mechanisms, such as the collection of advance information and pre-shipping screening, by which governments have agreed to work together to avoid imposing inconsistent requirements on global businesses.

Commercial ships are selected daily for inspection throughout the region. To facilitate selection, a central computer database is consulted by PSCOs for information about ships and for the reports of previous inspections within the Paris MOU region. The database, called SIRENAC, receives data from each inspection report whether or not violations are found. The SIRENAC database, which accepts data from shippers about their crew, cargo and structural integrity, shares that information with permissioned members of the governance framework, who are responsible to the users of the maritime trade systems.

A Global Movement Management governance model would benefit from the example of how the Paris MOU established a comprehensive framework of global supply chain security standards and best practices, covering both government-to-government arrangements as well as government-to-business partnerships. This
framework served to lift standards for supply chain security and harmonize rules for international trade.

**Setting the foundation for a GMMO**

Certain industries and sectors of the global economy lend themselves to a more rapid adoption of the human capital, technology and governance approaches outlined for Global Movement Management. As noted earlier, these may begin as sector-specific distributed pockets or “ink spots” of success or regional initiatives that evolve and eventually connect across sectors and geographies. The same governance principles described here apply to both small-scale versions of Global Movement Management and, ultimately, to a global version. As in the case of governing the Internet via ICANN and global shipping safety standards and information sharing with the Paris MOU, a combination of public and private sector leadership is required to set this governance process in motion. Also, importantly, trust is a critical factor at every stage.

The U.S. government could assume a leadership role in this process as it did with the maturing of the Internet. At that time, the Clinton Administration issued a proposal as part of the implementation of its “Framework for Global Electronic Commerce.” As referred to as the “Green Paper,” it was first published as a draft framework available for public comment. The Green Paper proposed the creation of a new, private sector not-for-profit corporation that came to be ICANN with an expert and globally representative Board of Directors. Similarly, for the process of establishing the necessary conditions for the human capital, technology and governance requirements for global movement systems, the U.S. government should issue a draft framework and invite stakeholders and the public to contribute to the way forward.

The draft framework for Internet governance via ICANN described the basic governance characteristics considered necessary for the challenge. Each would be a suitable topic for the first steps in establishing a GMMO. In fact, in crafting a new Green Paper for managing global movement systems, the following topics from the original Green Paper would serve as a useful foundation:

- The Need for Change – Explain the impetus behind establishing a more effective system.
• The Future Role of the U.S. Government – Explicitly state the limited and temporary role that this would be.

• The Principles – Update the principles of the original Internet – stability, competition, private, bottom-up coordination, representation – to reflect the principles we discuss later in this section: trusted and representative, enabling, limited, expert, incremental, self-sufficient, decentralized, inclusive, incentives-driven, metrics-oriented and adaptive.

• The Coordinated Functions and The Competitive Functions – Describe the daily operations of the governance structures, including the Board of Directors.

• The Transition – Stakeholders would partner with the public sector and assume governance responsibility to be placed in the private sector.

• The Process – Invite consideration and comment by the entire stakeholder community of interest to manage the process by which a GMMO should evolve.85

Structure
The President could appoint a chairperson with responsibility for coordinating a new Green Paper for Global Movement Management. The paper could be drafted jointly by a White House task force comprising representatives from the Department of Commerce, Department of Treasury and Department of Homeland Security. Similar to the way in which the first Green Paper emerged, this task force would proceed in consultation with the public. In addition to traditional public notice venues like the Federal Register for soliciting public opinion, four expert groups could represent main constituencies on central issues to inform the development of a governance organization and the drafting of this new Green Paper. These would include three advisory groups and a council as follows:

• A Private Sector Advisory Group composed of industry leadership from a number of sectors and trade associations representing an appropriate cross-section of the global economy, not only the United States. This group should include participation from large and small stakeholders that, combined, represent a community of interest that uses a range of business processes from the paper-based to the highly automated to cover the span of potential participants.86

• An International Partnership Advisory Group representing existing non-governmental organizations with relevant interests and competencies, such as the WCO, the International Maritime Organization and the International Monetary Fund.
• A Financial Advisory Group with representation from the central banks of Tier 1 through Tier 3 countries in addition to regional development banks.

• A Privacy Protection and Information Assurance Council to advise on privacy protection standards, a system for adapting to different legal systems and how to address new privacy concerns as they emerge. The Ombudsman would eventually serve as an independent watchdog entity for the operation of the new governance organization.

These same groups could evolve to form an important part of the organization itself. Based on the characteristics we described and the relevant models of ICANN and the Paris MOU, the GMMO could be structured as shown in Figure 12.

Figure 12. Proposed GMMO structure.

In addition to the advisory groups and council described above, the GMMO could serve the stakeholder community through three sub-organizations modeled on the structure of ICANN. For the purposes of global movement systems, these sub-organizations could include:

• Global Movement Systems Development and Support Organization to support efforts to improve information sharing between stakeholders in global movement systems. The services could include automation, interoperability, anonymization, encryption and analysis, etc. As part of the Support function,
this organization would also train users, owners and operators of the global movement systems, where appropriate.

- **Strategic Human Capital Organization** to identify and support the emerging techniques for managing in a networked environment. Those techniques may include improved collaboration, latitude to reach across and outside organizational boundaries, investment in organizational transformation, new and more flexible structures, relevant technology enhancements, and improved training for managerial and supervisory skills.

- **Standards Organization** to advise the Board of Governors, the CEO and others on the standards to guide global movement system activities of the Development and Support and the Strategic Human Capital Organizations. Standards could be technical, legal or workforce oriented. Much of the work of the Standards Organization would be at the direction of the three Advisory Groups, where appropriate, and the Privacy Protection and Information Assurance Council.

**Key characteristics**

Establishing a GMMO requires governance procedures to administer it, human capital investments to cultivate and lead it, and technology to support it. Regardless of the eventual organizational format of a GMMO, it should embody several key characteristics. A Global Movement Management governance regime should be:

- **Trusted and representative** – The organization must be trusted by the full range of participants, from developed (Tier 1) to nascent (Tier 3) economies, markets or individual participants. The operations of the organization must be open to public review and monitoring to correct problems when they arise and to help ensure that the daily operational decisions and protocols reflect the ideals and approach expressed in the original intent. Participants must be comfortable sharing proprietary and sensitive information, confident that the information is protected. Finally, the organization and its management or leadership must be accountable to the stakeholder community.

- **Enabling** – Nascent participants disadvantaged by low-tech, non-interoperable or simply small-scale infrastructure and resources also must be accommodated in a way that enables those participants to contribute to and benefit from the GMMO to the same extent that Tier 1 members do.

- **Limited** – GMMO participants agree to a level of collaboration that results in mutual benefit among competitors, clients and partners by sharing information critical to the flow of global trade and travel. While a governance mechanism
is required to manage this process, the participants are considered sovereign members in the same way as the United Nations and other multinational organizations consider their members to be self-selecting and driven by competitive advantage, increased security, heightened economic performance, or all three.

- Expert – A governance mechanism needs to have the knowledge, skills and abilities to expertly serve the global trade and travel stakeholder communities by consulting subject matter experts from those communities. Helping to ensure the expected gains – in whatever form – requires the ability to add value in a complex environment of corporations, countries and other collaborators.

- Incremental – Membership and/or scope of responsibilities may begin on a small scale so the governance structure can develop optimally. However, incremental growth should be undertaken through a deliberate and measured approach to better promote a level of collaboration that results in mutual benefit.

- Self-sufficient – This organization must have the resources to be self-sufficient over time, if not at the start. This can be accomplished through a number of means depending on the way in which the structure is initiated. (See “Dual-track GMMO approach” below.)

- Decentralized – Not only is it impractical in today’s information age and global economy to do otherwise, but by decentralizing the governing structures across the globe, the entire enterprise gains from a wider range of expertise and knowledge. There is a reason why ICANN uses numerous advisory groups around the world. Better intelligence and more accurate decisions translate into legitimacy and power in the marketplace and policymaking communities.

- Inclusive – To the extent that the governance structure will include Tier 3 countries and companies, it would provide funding from member countries in proportion to their interest in the system and their ability to pay, similar to the World Bank’s financial structure. The justification for this is that as more participants are able to contribute information and relevant infrastructure, the adoption of standards and norms will be facilitated. Thus, the overall benefits to the participants increase.

- Incentives-driven – Participants would have an incentive to improve their facilities, processes and business practices because these investments would result in increased efficiency, harmonization among trading partners and greater system resilience to manage risk more successfully.
• Metrics-oriented – A set of incentives or regulations must first align with a defined evolutionary process for members to adopt. Tier 1 countries and corporations would need an agreed-upon roadmap for more comprehensive improvements, whereas aspirants in Tier 3 should have a standard and transparent set of benchmarks for relative parity that would enable participation, as described above.

• Adaptive – This organization also must be adaptive to continually evolve with the needs of the stakeholder community and the challenges posed by a dynamic environment. Consistent with the characteristic that such an organization should be trusted, it would maintain a capability to be monitored for progress and efficacy. This capability would include a reform and reorganization function to help ensure its adaptability as needed.

**Dual-track GMMO approach**

As mentioned earlier, bridging the governance gap involves a dual-track approach: 1) creating new organizations where necessary, and 2) leveraging existing organizations. We also believe that a governance framework for Global Movement Management would gain momentum on a distributed basis where commercial incentives or government efforts favor action. Several different approaches could be taken for initiating this process, each of which has occurred in one form or another in the international system.

**Creating new organizations**

One approach we propose for establishing the governance framework needed for global movement systems includes creating new organizations. A new organization, like the GMMO, may be initiated in a number of ways. These include Consensus of the Leaders, Cell Division, Venture Model, and Foundation or Donor Model:

• Consensus of the Leaders – The policy apparatus of a significant portion of influential non-governmental organizations and national governments could be engaged to define and create the structure. The Financial Action Task Force (FATF) began this way. The FATF was established in 1989 by the G7 group of industrialized nations to generate political will and collaboration in support of legislative and regulatory efforts. These efforts were necessary for the protection of public and private sector interests in combating international money laundering, both as a public good and as a business function on the part of the worldwide banking industry. As an inter-governmental entity, the FATF
has established almost 50 recommendations that include procedures, standards and protocols for anti-money-laundering initiatives around the world. Today, 34 countries and their banks participate in FATF.

- **Cell Division** – In certain domains, a dominant governance structure already exists. For example, the WCO reconciles widely diverse practices in global trade relationships by determining standards for everything from ship classifications to the form and type of information an exporter must submit to participate in the global economy. The charter, decision-making mechanisms and financial framework of the WCO could simply be replicated to create a similar structure to provide the foundation for the GMMO.

- **Venture Model** – A private sector or a non-profit investor could establish a global movement management network as a service for a fee. The rules of participation would include adherence to a set of bylaws and ownership by the stockholders in a blind trust such that initial investors help establish it, but the operation would be undertaken by a third party. In this scenario, the fee for service would likely be minimal, but the scale could become significant as the value proposition of increased efficiencies and more robust resilience appeal to a growing community of participants/customers. This model would resemble a virtual utility whereby its investors would create ownership in a public good. Charging fees would require approval of a board in an oversight capacity similar to how most public utilities are governed.

- **Foundation or Donor Model** – This is similar to the way the World Bank was formed. All stakeholders would donate funds to a foundation that would achieve critical mass and then deliver a significant bottom line. In this case, the bottom line would be the evolving Global Movement Management network. It is conceivable that this process would take longer, favor the bigger players, at least initially, and adopt a cumbersome management mechanism.

The founding of the Paris MOU represents a Consensus of the Leaders, but it also shows the potential for a Cell Division evolution because it is scaleable to other sectors of global trade and travel. Due to the global and distributed nature of what is being proposed, this new governance organization for global movement systems could be developed regionally first. The path taken by those who established ICANN would apply well in North America as a means for designing a governance regime based on the key characteristics we described earlier. A similar effort could be undertaken by the European Union, while its counterparts in Asia, Africa and the Middle East would be responsible for their own efforts.
Because these efforts would use, as a blueprint, the same set of principles and core characteristics, similar to those identified here, the result would be networked and compatible coverage of global movement systems.

In what could be called an “ink spots” process, certain sectors or stakeholder groups could support the foundation of a Global Movement Management framework where it is directly beneficial even at an early stage. By starting in this way, best practices emerge on a bilateral or otherwise limited basis. As countries and industries within flows participate, the “ink spots” model has the potential to expand in a way that is interoperable with other sectors and flows if consistent standards are applied. Eventually, this process would achieve the global scope necessary for the full benefits of Global Movement Management to be realized. However, system efficiencies and enhanced security and resilience factors can be improved for participants even on a small scale.

Leverage existing organizations

The other half of the dual-track approach we propose for creating a GMMO includes leveraging relevant existing governance regimes and encouraging other international organizations to adopt the promotion of intelligent immunity in global movement systems as a high priority mission of their own. Doing so will help promote adoption of a more strategic approach to technology and human capital around the world to enhance the security, efficiency and resiliency of global movement systems. Therefore, we propose the following:

• The World Census and Statistics Organization could empower people around the globe by providing information about the performance of global movement systems. Metrics to measure the efficiency, security and resilience of the system should be developed and implemented widely. More informed users of the system and, in the case of democratic countries worldwide, better informed taxpayers, can hold their governments accountable for performance results. New organizations chartered for this purpose, such as IBM’s Managing for Progress initiative, have already garnered substantial international attention, prototyped initial technology and attracted participants from a number of leading institutions worldwide.

• The Group of Eight Most Industrialized Countries (G8) could introduce policy proposals to inform their citizens of the things they can do to enhance security and resilience of global movement systems as part of emergency management and public service notices already in existence. These could include a simple
“Report Suspicious Activities” hotline modeled after the statewide programs in place in New York and New Jersey.

• The International Standards Organization could incorporate more of a strategic human capital approach into their ISO 9000 standard as part of the overall effort to harmonize standards for business processes and technology. The training standard should include the use of simulation training and gaming technologies to create virtual environments where front-line inspectors and law enforcement personnel can get much needed practice dealing with malicious actors, and can learn to work with each other in a more decentralized and coordinated fashion.

• The International Federation of Red Cross and Red Crescent Societies and their national member societies could create a basic training course for people around the world regarding the role that individuals can play in improving overall security and resiliency. These organizations could also provide knowledge and training on how to prepare for and respond to natural disasters and other high-consequence disruptions. Such a course could complement existing widespread public education programs such as CPR and EMT courses. It would stimulate a higher level of knowledge and preparedness in society starting at the level of individual citizens and would be appropriate for both developed and developing countries.

For example, the courses could include requirements for basic food, shelter, clothing, communication and medicine to serve a family for the period of time it is likely to take emergency management systems to kick in. Other private sector training companies, colleges and universities could follow suit as demand grows, providing course opportunities on a fee-for-service basis using public health curricula and emerging homeland security programs for content. A program for elementary and secondary education could provide an age-appropriate baseline for understanding elementary responsibilities of citizenship and personal responsibility in an emergency. Education and outreach by trusted public information outlets, including the Red Cross, state and local authorities, and media outlets should speed acceptance.

Financial incentives for adherence to the new global standards should be increased as follows:

• The World Bank, Asian Development Bank and the Inter-American Development Bank could launch initiatives to improve security that provide investment money in developing countries contingent on the adoption of improved security practices. Such initiatives could be modeled on the U.S.
Millennium Challenge Corporation. The Millennium Challenge Corporation criteria could also be extended to include more emphasis on trade facilitation, security and resilience in global movement systems.

- The European Union and NAFTA could apply portions of existing tariffs to fund a “road user charge” to more directly tie activity to benefit for local infrastructure. Signatories to the system could then decide whether to designate a portion of these funds for investment in infrastructure, technology and human capital in direct proportion to use by the members states.

- The leaders of leading insurance companies could seek to adopt the ISO 9000 standards and related Red Cross/Red Crescent certifications as a means to group risk and price accordingly. The presumed reduction in risk for early adopters of these standards would create a financial incentive for others to take the course and gain certification. This insurance discounting process would be comparable to what we have in the United States for driver education and associated reduction in the cost of auto insurance.

- The WCO could create a forum for the 50 largest companies in the world to harmonize directly with their corporate counterparts on a business-to-business basis with WCO and government review. Participants could work toward bilateral innovations to help lower their costs and then request approval by relevant customs organizations. Participants would naturally start at the highest value end of the set of possible system improvements. The WCO could then share these promising practices among the other participants and use the case studies as a basis to propose systemwide reforms. This process, if successful, could be expanded to include other global movement systems over time.

- The U.S. National Institute of Standards and Technology (NIST) could consider modifying the Malcolm Baldrige National Quality Award’s Criteria for Performance Excellence to incentivize leading firms and organizations in all sectors to optimize commerce, security and resilience. This would encourage the adoption of security and resilience as critical new attributes of quality in the manufacturing, transportation and financial services industries. The resulting value to corporate performance, enhanced brand value for competing firms and sharing of promising practices would further create incentives for adoption of new standards.
• The WCO, WTO and Interpol could cooperate in creating a global incident database of disruptions to global movement systems, including incident analyses and after-action reports. This effort could be augmented with methods for assessing or grading strengths and weaknesses of global movement systems that could lead to a clearinghouse function for peer-validated best practices in enhancing the security, efficiency and resilience of global movement systems as a basic public good. Access to some of the output of this effort would have to be limited to verified and properly permissioned level officials. The functionality and services provided by the Memorial Institute for the Prevention of Terrorism, which was created as a resource for first responders and homeland security and counterterrorism practitioners, would represent a small-scale model.115

**Universal system for scoring risk**

If not undertaken by an existing organization, an additional task of the GMMO would be to lead the development of a universal system for scoring risk. Such a system would be akin to the universal credit scores provided for companies by S&P and Moody’s and to sovereign credit risk assessments that large banks provide for countries. Another example is the Risk Preparedness Index that accounting firms use to assess cyber security at financial institutions.116 The GMMO could spearhead the creation of a comprehensive risk-scoring system and methodology that could be applied universally to companies, countries, economic sectors and individual movement systems.
VII. Moving forward

We believe that the holistic Global Movement Management strategy presented in this white paper can be an essential component to successfully addressing the asymmetric and highly networked nature of risk in the movement systems that make today’s global economy work. We foresee a new relationship emerging between the public and private sectors as they increasingly recognize their common interests as stakeholders in the global movement system. Private companies and individuals, governments and non-governmental organizations can work in concert to improve the health of critical global movement systems to help make them more resistant to harm or disruption – an approach we call intelligent immunity. To accomplish this, we recommend that policymakers, managers and employees incorporate the concept of intelligent immunity into their core strategies for human capital, technology and governance and into how they conduct their businesses every day. This will help protect and improve global movement systems and, therefore, help make the global economy more secure and resilient.

We believe that the first step to promoting intelligent immunity in global movement systems is achieving widespread understanding of the benefits and risks of economic and security interdependence that exist between individual companies, sectors and countries. Since individual movement systems and individual economic sectors around the world are inextricably linked, a greater recognition of the risks and responsibilities that accompany mutual interdependence will promote greater cooperation among stakeholders. The business justification for aligning activities across sectors will grow stronger, and stakeholders will see benefits to better coordination and cooperation ranging from improvements to the bottom line to brand strengthening and reputation-building in the area of social responsibility.

We also believe that new business analysis, accounting, capital budgeting and financial reporting tools will emerge to measure the benefits of greater security and resilience within and among systems. For example, the creation of a universally recognized Risk-Preparedness Index would provide a benchmark against which owners and operators of critical global movement systems could be assessed. This would allow key aspects of intelligent immunity in global movement systems to be priced into the market, for example, through the risk premiums charged to companies by insurance providers. This would help business leaders and security managers to move beyond simple traditional ROI calculations and better quantify and capture the business case

for investments that increase security, promote resilience and reduce supply chain vulnerability.

We anticipate the need for a more strategic approach to people and training to promote intelligent immunity in the global movement system. Traditional approaches to risk management and human capital are largely based on exception-based management controls. In contrast, an approach to risk management in global movement systems based on intelligent immunity will rely to a much greater degree on empowerment and trust. A more strategic approach to human capital will require companies and governments to invest more in employee training, to better arm front-line employees with the right information at the right time, and to empower them with the confidence in their own authority to make decisions based on their own informed judgments and local knowledge. In addition, a more strategic approach to human capital will allow companies and governments to discover more innovative ways to improve efficiency, security and resilience. This sea change in the approach to risk management and human capital can help make traditional bureaucratic and hierarchical organizational cultures within government and many companies more flexible, dynamic and innovative in the face of modern risks.

To better empower individuals and to support intelligent immunity overall, we envision a technology strategy for global movement systems that includes three major components:

• Adoption of a micro-macro approach that combines both greater information granularity and greater information federation/aggregation
• Building the “connective tissue” that can help give stakeholders in global movement systems the confidence to connect, collaborate and share even sensitive information at scale
• Peer production that results from unlocking information and sharing it more widely, helping to drive innovation and dramatically improving the performance, security and resilience of global movement systems.

We believe that adopting a peer production strategy will yield several benefits. It can help address significant issues of trust and privacy that currently impede information sharing. It can play a key role in the evolution of Web 3.0. It can help drive the kind of robust enterprise awareness and collaboration among the public and private sectors needed to address 21st century risk. Finally, it can open the door to significant commercial opportunities for the entrepreneurs, investors and companies that provide the solutions to make this technology vision work.
Finally, we propose a new approach to governance that takes lessons from proven approaches and existing successful organizational models in the international system while combining them in a new way to better address the types of risks that confront the world in the 21st century. Global Movement Management’s approach to governance will advance the efforts of existing non-governmental organizations to strengthen the global movement system. It also will serve as a basis for creating a new international organization, the GMMO, to help fill the governance gap that exists today.

The GMMO will enable governments and companies from around the globe to work together to achieve their common interest in improving the performance, security and resilience of the global movement system. The GMMO will provide a venue for the public and private sectors to discuss critical public policy issues beyond the confines of national tax and regulatory policy. In addition, the GMMO can provide a forum for cooperation between business competitors and between interdependent economic sectors that currently may lack sufficient coordination. Finally, the GMMO can pave the way for better synchronization of policies, business practices and technology standards to help guide efforts.

One of the most important goals of the GMMO will be to provide mechanisms for Tier 3 countries to better integrate themselves into cooperative efforts to strengthen global movement systems. Such mechanisms will include data automation and integration services as well as initiatives to secure investments by international aid and development organizations.

Much is at stake in the global movement system. It is not just the trillions of dollars in global trade or the economic welfare of billions of people, but the very fabric of society itself – its values, cherished ideals and unique character. The prospect and advantages of being able to harmonize global movement systems are not only encouraging and a real opportunity for innovation but, we think, critically necessary to strengthen commerce, security and resilience in the face of globalization and technology change.

The Global Movement Management framework we propose in this paper as a comprehensive approach to risk management can help improve public policy, facilitate international and public-private cooperation, guide investment decisions, create commercial opportunities, and promote best practices to address asymmetric threats and respond to both natural and manmade disruptions. The challenge is immense, the opportunity expansive, and the time for business leaders, government officials and the international community to move forward is now.
About the authors

W. Scott Gould
Vice President, Public Sector Strategy and Growth
IBM Global Business Services

Dr. Scott Gould directs strategy formulation for the Homeland Security, Intelligence and Federal Civilian line of business in IBM Global Business Services. Previously, he was CEO of The O’Gara Company, where he provided strategic advisory and investment services in the homeland security market. A Naval Intelligence reservist, Capt. Gould was recalled to active duty for Operation Noble Eagle and Enduring Freedom, where he served as Deputy to the Director, Naval Criminal Investigative Service (NCIS). He has served as the CFO and Assistant Secretary for Administration at the U.S. Department of Commerce and as Deputy Assistant Secretary for Finance and Management at the U.S. Department of the Treasury.

As a 1993-1994 White House Fellow, Scott served in the Export-Import Bank of the United States and in the Office of the White House Chief of Staff. He is a fellow of the National Academy of Public Administration and a former member of the National Security Agency (NSA) Technical Advisory Group. He has participated as a panel member on homeland security issues for the Council on Foreign Relations and the Center for Strategic and International Studies; he also has served as a guest lecturer at Harvard University. Scott is a former member of the Malcolm Baldrige National Quality Award Board of Overseers. He also is co-author of the previous white paper, “Global Movement Management: Securing the Global Economy,” co-author of the book “From Vision to Reality: Aligning Business and Government Interests in Maritime Domain Awareness and Global Movement Management” and co-author of a forthcoming book from the Brookings Institution entitled “The People Factor.” Scott holds an A.B. degree from Cornell University and M.B.A. and Ed.D. degrees from the University of Rochester.
Daniel B. Prieto directs the Global Movement Management initiative for the Homeland Security, Intelligence and Federal Civilian practice in IBM Global Business Services. He is Project Director for the Council on Foreign Relations (CFR) Independent Task Force on Civil Liberties and National Security, Senior Advisor to the Commission on the National Guard and Reserve, adjunct Senior Fellow at the Reform Institute and at the George Washington University, and a member of the Markle Foundation Task Force on National Security in the Information Age. Dan has served as Research Director of the Homeland Security Partnership Initiative and been a Fellow at Harvard University’s Kennedy School of Government, where he also served as a graduate-level lecturer. He has been a Fellow at the CFR and has served on the professional staff of the Homeland Security Committee in the U.S. House of Representatives. As Director of Corporate Development for America Online and as an investment banker with JP Morgan, he served as an advisor on over US$125 billion in transactions in the technology, media, and aerospace and defense sectors. He is co-author of “Neglected Defense: Mobilizing the Private Sector to Support Homeland Security” and contributing author to “Threats at Our Threshold: Homeland Defense and Homeland Security at the Turn of the Century,” “The Forgotten Homeland” and “Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability.” He has testified before the U.S. Senate, and his commentary and analysis have appeared widely, including in The New Republic, The Washington Post, Chicago Tribune, Bulletin of the Atomic Scientists, Wall Street Journal, TIME Magazine, USA Today and The Atlantic Monthly as well as on CNN, FOX, BBC and National Public Radio. Dan holds a B.A. from Wesleyan University an a M.A. from the Johns Hopkins University School of Advanced International Studies (SAIS).
Jonah J. Czerwinski
Managing Consultant, IBM Global Business Services
Senior Fellow, IBM Global Leadership Initiative

Acronyms

ARPAnet Advanced Research Projects Agency Network
BCBS Basel Committee on Banking Supervision
C3I2 Command, Control, Communications and Information Integration
CBP U.S. Customs and Border Protection
CCC Customs Cooperation Council
CEO Chief Executive Officer
CONOPS Concept of Operations
COO Chief Operating Officer
CSI Container Security Initiative
CSO Chief Security Officer
CTBTO Comprehensive Nuclear-Test-Ban Treaty Organization
C-TPAT Customs-Trade Partnership Against Terrorism
DHS Department of Homeland Security
ECOSOC Economic and Social Council of the United Nations
EDI Electronic Data Interchange
FAO Food and Agriculture Organization
FAST Free and Secure Trade
FATF Financial Action Task Force (Against Money Laundering)
FOE Friends of the Earth
G8 Group of Eight Most Industrialized Countries
GATT General Agreement on Tariffs and Trade
GDP Gross Domestic Product
GESAMP Joint Group of Experts on the Scientific Aspects of Marine Environmental Protection
GFW Global Fund for Women
GICHD Geneva International Centre for Humanitarian De-mining
GMM Global Movement Management
GMMO Global Movement Management Organization
HRW Human Rights Watch
IAEA International Atomic Energy Agency
IAIS International Association of Insurance Supervisors
IASB International Accounting Standards Board
IATA International Air Transport Association
ICAO International Civil Aviation Organization
ICANN Internet Corporation for Assigned Names and Numbers
ICBL International Campaign to Ban Landmines
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICC</td>
<td>International Chamber of Commerce</td>
</tr>
<tr>
<td>ICCA</td>
<td>International Council of Chemical Associations</td>
</tr>
<tr>
<td>ICFTU</td>
<td>International Confederation of Free Trade Unions</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>ICS</td>
<td>International Chamber of Shipping</td>
</tr>
<tr>
<td>ICSC</td>
<td>International Council for Science</td>
</tr>
<tr>
<td>IFAD</td>
<td>International Fund for Agricultural Development</td>
</tr>
<tr>
<td>IFPMA</td>
<td>International Federation of Pharmaceutical Manufacturers &amp; Associations</td>
</tr>
<tr>
<td>IFWP</td>
<td>International Forum on the White Paper</td>
</tr>
<tr>
<td>IGO</td>
<td>Intergovernmental Organization</td>
</tr>
<tr>
<td>ILO</td>
<td>International Labor Organization</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>IMO</td>
<td>International Maritime Organization</td>
</tr>
<tr>
<td>IO</td>
<td>International Organization</td>
</tr>
<tr>
<td>IOC</td>
<td>International Olympic Committee</td>
</tr>
<tr>
<td>IOM</td>
<td>International Organization for Migration</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organization of Securities Commissions</td>
</tr>
<tr>
<td>ISA</td>
<td>International Seabed Authority</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ISPS</td>
<td>International Ship and Port Facility Security Code</td>
</tr>
<tr>
<td>ITLOS</td>
<td>International Tribunal for the Law of the Sea</td>
</tr>
<tr>
<td>ITTO</td>
<td>International Tropical Timber Organization</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>IUCN</td>
<td>World Conservation Union</td>
</tr>
<tr>
<td>IWC</td>
<td>International Whaling Commission</td>
</tr>
<tr>
<td>IWHC</td>
<td>International Women's Health Coalition</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MSF</td>
<td>Médecins Sans Frontières (Doctors without Borders)</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NCIS</td>
<td>Naval Criminal Investigative Service</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OHCHR</td>
<td>Office of the High Commissioner for Human Rights</td>
</tr>
<tr>
<td>OMT</td>
<td>Operations Management Team</td>
</tr>
<tr>
<td>OPCW</td>
<td>Organization for the Prohibition of Chemical Weapons</td>
</tr>
<tr>
<td>OS&amp;D</td>
<td>Overages, Shortages and Damages</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Record</td>
</tr>
<tr>
<td>POE</td>
<td>Point-of-Entry/Point-of-Exit</td>
</tr>
<tr>
<td>PSCO</td>
<td>Port State Control Officer</td>
</tr>
<tr>
<td>RPI</td>
<td>Risk Preparedness Index</td>
</tr>
<tr>
<td>SAFE</td>
<td>WCO Framework of Standards to Secure and Facilitate</td>
</tr>
<tr>
<td>SAFE Port Act</td>
<td>Security and Accountability For Every (SAFE) Port Act</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-Oriented Architecture</td>
</tr>
<tr>
<td>SRO-WA</td>
<td>Sub-Regional Office for West Africa</td>
</tr>
<tr>
<td>TEU</td>
<td>Twenty-foot Equivalent Units</td>
</tr>
<tr>
<td>UNDCP</td>
<td>United Nations International Drug Control Program</td>
</tr>
<tr>
<td>UNEP</td>
<td>United Nations Environment Program</td>
</tr>
<tr>
<td>UNESCO</td>
<td>United Nations Educational, Scientific and Cultural</td>
</tr>
<tr>
<td></td>
<td>Organization</td>
</tr>
<tr>
<td>UNFPA</td>
<td>United Nations Population Fund</td>
</tr>
<tr>
<td>UNHCR</td>
<td>United Nations High Commissioner for Refugees</td>
</tr>
<tr>
<td>UNICEF</td>
<td>United Nations International Emergency Children's Fund</td>
</tr>
<tr>
<td>UNIDO</td>
<td>United Nations Industrial Development Organization</td>
</tr>
<tr>
<td>UPU</td>
<td>Universal Postal Union</td>
</tr>
<tr>
<td>US-VISIT</td>
<td>United States Visitor and Immigrant Status Indicator</td>
</tr>
<tr>
<td></td>
<td>Technology</td>
</tr>
<tr>
<td>WCO</td>
<td>World Customs Organization</td>
</tr>
<tr>
<td>WFP</td>
<td>World Food Program</td>
</tr>
<tr>
<td>WHO</td>
<td>World Health Organization</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organization</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapons of Mass Destruction</td>
</tr>
<tr>
<td>WMO</td>
<td>World Meteorological Organization</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
<tr>
<td>WWF</td>
<td>World Wildlife Federation</td>
</tr>
<tr>
<td>XBRL</td>
<td>Extensible Business Reporting Language</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
Glossary of key terms

Architecture – A plan, depiction or description of the manner in which a system is designed and constructed, including identification of components, depiction of functions and description of relationships between components.

Enterprise knowledge management – Making efficient use of human and institutional knowledge within an organization or across multiple organizations that comprise a logical enterprise or system (processes, relationships and technology). The identification, coordination/integration and presentation of information from documents, reports and other sources in a way that facilitates the ability to search and analyze information for meaningful relationships to improve decision making.

Governance – The use of institutions, rules, standards, norms, practices, processes and collaboration to administer, control, coordinate and direct activity within a system or enterprise. Governance includes setting expectations, granting authority, and verifying compliance and performance. Governance includes virtually all normative aspects of the system and the mechanisms used to communicate, effect and oversee those aspects. Governance can come from governments in the form of regulation or policy, from non-governmental organizations in the form of standards or best practices, from across industry in the form of self-regulation or established best-practices, or from within companies in the form of business rules, company policy or operational practices.

Information sharing – The range of activities that improve the ability of multiple parties to exchange data, content and other information in a way that increases knowledge, improves decision making and enhances enterprise/system performance.

Resilience – The ability to recover quickly from, or to resist being affected by, some shock or disruption; the quality or state of being flexible. Other useful, discipline-specific definitions include:

• Networking – The ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.
Engineering – A measurement of resistance to disturbance and rate of return to steady-state equilibrium following a perturbation. This definition assumes that system behavior remains within a stable domain that contains the steady state and concentrates on stability near an equilibrium steady state. This definition focuses on efficiency, control, constancy and predictability – all critical attributes for fail-safe design and optimal performance.

Ecological – The magnitude of disturbance that can be absorbed before the system changes its structure by changing the variables and processes that control behavior. This definition emphasizes conditions far from any steady states, where instabilities can induce a “quantum” move into another regime of behavior (i.e., to another stability domain). This definition focuses on persistence, adaptability, variability and unpredictability.

Risk – The probability of harmful consequences resulting from interactions between threats and vulnerable assets. Conventionally, risk is expressed by the relation Risk = Likelihood x Severity. More specifically, in the case of intentional disruption:

\[ \text{Risk} = \text{PA} \times (1 - \text{PE}) \times \text{C} \]

Where:
- \( \text{PA} \) is the likelihood of adversary attack (threat)
- \( \text{PE} \) is security system effectiveness
- \( (1 - \text{PE}) \) is adversary success (vulnerability)
- \( \text{C} \) is magnitude of loss due to the attack (consequence).

Security – The establishment and maintenance of measures designed to: 1) identify and reduce or prevent threats to the integrity and well-being of objects (i.e., people, goods, conveyances) and systems, 2) reduce the vulnerability of objects (i.e., people, goods, conveyances) and systems to activities that would adversely affect their integrity, performance or well-being, and 3) limit or mitigate the consequences of adverse activities or events.

Trade and travel facilitation – The simplification and harmonization of international trade and travel procedures and the information flows associated with them needed to expedite the movement, release and clearance of objects (i.e., people, goods, conveyances) in transit.
Appendix A: Global Movement Management Analysis of the Maritime Cargo Sector

To illustrate a sample component system analysis for building intelligent immunity into maritime cargo flows, we apply the five categories discussed in Section III, which are: 1) five key objects of value, 2) five questions, 3) five chains of movement, 4) five traditional security functions, and 5) five emerging security functions. These elements are addressed below. (Also see the sidebar, “Global Movement Management the maritime cargo sector” in Section III, “Applying a Global Movement Management framework.”)

Five key objects of value
The object can be categorized as cargo, with information and conveyances in supporting roles.

Five questions

What is the object? – The object is a maritime shipping container. Its contents are listed on the bill of lading; however, they are not verified until the end of the supply chain, either when the goods are inspected by a customs officer or the container is opened by the importer.

Where is the object? – Knowledge of the object’s location is not in realtime. This information is recorded at control points and transmitted to other players in the supply chain. In between, there are relatively few measures in place to keep an object from being diverted.

When did the object leave/When is it scheduled to arrive? – Customers typically know when an object ships and when it is expected to arrive. Because the object is not being tracked in realtime and because data recorded at control points is frequently paper-based, knowledge of where a shipment is at any given time is extremely limited, and timely updates regarding delays are difficult to obtain.

How is the object being conveyed? – The object is likely being transported by truck or train over land and by ship at sea. The ship the object travels on is likely to be known; however, information about the trucks and drivers is likely to be limited to operators at the choke points that received or dispatched the truck.
Is the object secure? – Figure 13 reveals a notable trend in ranking the relative risk to the container or cargo from export (left) to import (right). The security of maritime cargo is directly related to its visibility, and, generally, the level of shipment visibility is significantly lower the closer it is to its point of origin. This is true because such a large number of players are involved in manufacturing, packaging, gathering, collecting, consolidating, packing and transporting goods before they ever get placed on a boat for shipment. Adding to the risk are the overall conditions in the country of origin, which will, obviously, vary widely. Different export countries will all exhibit vast differences, for example, in manufacturing and packaging quality controls and security procedures; quality of recordkeeping; levels of corruption and crime; quality of law enforcement; technology infrastructure; and political, geographic, and social conditions.

If the risk of tampering, fraud or insertion of contraband into shipments is generally higher closer to its point of origin, risk is also higher, as a general rule, when an object is at rest. “Dwell time” is a disadvantage from the standpoint of all participants in the supply chain. Commercial interests lose valuable time, and public sector authorities consider this a peak point of vulnerability for the cargo or its container. A Chinese Customs official informed IBM that 8–10 percent of all cargo being exported from China is lost or damaged from the container-stuffing site to being loading on a vessel. This is a staggering figure, considering that Chinese exports accounted for nearly 40 percent of global total exports by volume in 2005.

Five chains of movement

Supply chain – Though no two international maritime cargo shipments are ever exactly the same, Figure 13 depicts the key aspects of a “typical” shipment. Time in transit is represented along the top axis in days. The vertical axis identifies every individual participant in the cargo supply chain, such as the exporter, customs, and shipping and trucking companies. Horizontal blue arrows denote the physical flow of cargo, and vertical red lines indicate flows of data among stakeholders. At a high level of summary, and moving from left to right through Figure 13, the activity in the first third of the picture represents the export process; the middle third represents the cargo in transit at sea; and the last third shows the import process at the receiving country.
Figure 13. Global Movement Management analysis of a generalized international maritime cargo supply chain.

Source: IBM Global Business Services.
The very first stage of this flow, at left, occurs prior to the movement of actual cargo and may take 30 days or more to complete the legal, trade and financial documentation required before the physical movement of the international maritime trade can begin to take place. Trade documents and physical event transactions are plotted sequentially from left to right. In areas where several activities are plotted across the same short time period, Figure 13 indicates that the shipment is waiting for custody transfer or is in a holding pattern while the activities depicted take place.

Figure 13 shows areas of risk, areas of existing policy focus and opportunity areas to improve operations either through changes in business practices, changes in policy, improved technology, improved information sharing or some combination thereof.

The overlaid colored boxes and ovals indicate points of vulnerability as well as points of opportunity where performance and security could be improved. Boxes indicate areas where efficiency and security of trade data are of concern. The vertical red box at the left encompasses an area representing a high level of information security vulnerability owing to the wide range of actors involved and a low level of data automation and interoperability. The area within the orange box experiences a medium level of information security vulnerability and supply-chain inefficiency owing to inadequate data automation and interoperability. As time passes, overall risk decreases from a peak period as signified by the fading red ovals surrounding the cargo and its conveyance. These points are addressed in further detail in the Information Chain discussion below.

*Value Chain* – The goods are more valuable when they arrive at the import country than before they leave the export country. Because the goods in question are finished products, however, their value is relatively stable across the chain.

*Information Chain* – The area at the left of Figure 13, from Day -30 to 0, and within the vertical red box depicts the creation and exchange of information about a shipment that occurs before the movement of physical goods actually begins. These transactions involve multiple stakeholders, dozens of documents and hundreds of individual data elements. The documents originating in this period of time before physical shipment represent 60-70 percent of all data exchanged in any end-to-end trade flow.
Despite modern technologies, much of the vast amounts of information exchanged during this pre-shipment period occurs across inefficient, non-interoperable legacy systems, electronic data interchange (EDI) systems, e-mails, faxes, phone calls and even hard-copy paper documents, which are handed off from one party to the next. As each sequential document is created, redundant data from upstream sources is re-keyed along with new shipment data. The points in the supply chain highlighted by the orange box include data and document exchanges, which begin when the maritime shipping container reaches the export port of load and end when the shipment has arrived at the port of destination on the import side. These transactions include exchange of bills of lading, export/import customs declarations and customs entry. The data and documents exchanged at these points in the shipment cycle are, again, largely inefficient and characterized by data redundancies and manual processes. The high volumes of data contained in these documents and the relative importance of the information make accurate and effective communication and data exchange of utmost importance to traders.

Despite the imperative for accurate and timely data, an IBM study of industry common practices indicated that in a “typical” global trade, 35 documents change hands. But, due to antiquated and poorly coordinated and connected systems, and as noted in Sections III and V, the data within those 35 documents needs to be manually re-entered in disparate technology and other recordkeeping systems approximately 1,393 times. This repetitive data re-entry and re-keying accounts for 78.5 percent of all data from trade documents.

The lack of visibility into downstream data and transactions makes critical trade documents and associated supply chain stakeholders susceptible to alteration, inaccuracy or loss of information. Shipment delays, late fees, stockouts and increased costs for rushed shipments are typical risks in the modern maritime shipping industry. These risks are made worse by the largely paper-based and manual processes for managing information in the maritime cargo sector. Such risks can be reduced dramatically with enhanced communications, increased electronic data and document exchange, and greater automation of business processes.

**Metadata Chain** – Information about international container movements is categorized and compiled at only the highest level. Shipments are measured
in Twenty-foot Equivalent Units (TEUs), meaning that a standard forty-foot container would be listed as two TEUs. Information about the contents of the container, its origin and destination would also be recorded.

**Policy Chain** – Since September 11, 2001, a series of new government policies and public sector–private sector initiatives to enhance security and supply chain efficiencies have been implemented. These include:

- The Customs-Trade Partnership Against Terrorism (C-TPAT)
- The 24-Hour Rule
- The Maritime Transportation Security Act
- The International Ship and Port Facility Security Code
- The Container Security Initiative.

A more detailed listing and description of these programs can be found in Appendix B, “Additional detail on maritime security programs.”

Of these efforts, the most successful has been securing the physical port, as opposed to the container or the overall supply chain. The Maritime Transportation Security Act (MTSA) has succeeded in bringing US ports up to a base level of compliance with generally accepted physical security measures. The International Ship and Port Facility Security (ISPS) code has had a similar though lesser effect internationally. However, most megaports around the world have agreed to meet higher standards codified in the voluntary but more stringent Part B of the code. For security of the supply chain, the C-TPAT program is generally recognized as the right model but has been hampered by limited oversight and the failure to provide a genuine “green lane” preference for companies that are part of the program.

**Five traditional security functions**

**Facility Security** – The ISPS code and the MTSA have been effective instruments for promoting facility security both in the US and overseas. Security risks are lower after inland transport when containers are at the port and on vessels. Container yards in the port are typically well lit and under a high degree of surveillance. Additionally, containers stacked 10–15 boxes high provide inherent protection.

The threat of terrorism and WMDs is reduced to a degree after the container exits the port of discharge, as measures have been taken since 9/11 on the part of
ports, federal governments, and state and local law enforcement officials to target, scan, inspect, and identify threats. But terrorists will have succeeded if a dirty bomb, for example, is not detected until a container reaches a European Union or U.S. seaport. Proactive measures must be taken in risk management and risk assessment, enforcement, and resiliency in order to best prepare for and respond to maritime security threats.

**Conveyance Security** – After a container is stuffed at the export site, it is typically carried by a trucking company to a railhead or directly to the port, for loading onto an ocean vessel. It is at points throughout this inland transport – truck stops, rail yards, open road or rail track – that a container is most susceptible to exceptional events. Truckers can be delayed by mechanical problems; trains run off schedule; rail yards have little or no security; deviants plan infiltrations at truck stops and rest areas. Modern maritime containers are locked and equipped with a uniquely numbered door seal; however, demonstrations show that skilled criminals or terrorists can open container doors in fewer than ten seconds, without ever breaking the container’s seal or visually compromising the integrity of the container itself. While usually safer and more visible than overseas inland trade routes, transport corridors within the European Union and United States are still susceptible to pilferage and damage. On the ocean vessel itself, space optimization measures allow for stacking tens of containers in cargo bays and on deck, making it difficult for even skilled pirates to gain access to cargo on vessels at sea or berthed at the wharf.

**Credentialing, Identity Verification, Provenance** – For port facilities, initiatives are underway to help ensure that workers pass background checks and that their identities are verified upon entry to the port and secure areas. For containers, verification of contents does not take place until they are unloaded for inspection or at their final destination, representing a weakness in the security regime.

**Screening and Inspection** – Screening and inspection functions are typically conducted at the port of entry by import country customs officials. The Container Security Initiative (CSI) is an effort to move these functions to the port of embarkation; however the success of this program has been uneven. Secure Freight is a U.S. government initiative to confirm data about the contents of shipping containers through a network of screening, scanning and information-sharing processes in coordination with foreign ports.
Interdiction and Enforcement – In the event that a container in transit is thought to contain a nuclear weapon or other device, responsibility for interdicting the vessel carrying the container would fall to the Coast Guard. However, once the vessel is stopped from landing at a U.S. port, there is no clear plan for where the ship would be brought in for the container to be offloaded and inspected away from population centers. Proposals for constructing an offshore platform to stop and inspect ships with cargo were tabled as being cost-prohibitive. The problem of interdiction is one of the drivers for securing shipments prior to embarkation.

Five emerging security functions

Enterprise-wide Training – Generally, enterprisewide training is lacking in the maritime container trade. Responsibility for security rests almost exclusively with dedicated security personnel, and security is considered a cost and a delay factor, rather than a value producer.

Tracking – Realtime or near-realtime tracking of containers is in its infancy. Most data collected at control points in the supply chain is not disseminated to the wider network in realtime.

Risk Analysis – Risk analysis of container traffic is performed by U.S. Customs using their Automated Targeting System (ATS). ATS has not been shown to be effective in several studies conducted by the Government Accountability Office (GAO) due to the fact that the data being analyzed is of poor quality. Shipping companies generally do not make risk determinations for the containers they carry.

Enterprise Awareness and C3I2 – Because data is not aggregated and digitized in realtime, use of this information for both Enterprise Awareness and Command and Control functions is highly limited. Both security and efficiency could be increased by creating Enterprise Awareness and a robust technology platform for C3I2 functions.

Resilience and Response – While many security measures have been taken, the maritime cargo system is not as secure or resilient as it could be. After an attack, policymakers will, for some time, likely have a severely limited ability to assure the public that the system is safe. This may force policymakers to take extreme measures of opening and inspecting virtually every container, fundamentally crippling the performance of the supply chain and dramatically increasing the cost and reducing the availability of transport.
Appendix B: Additional detail on maritime security programs

The terms below are applicable to maritime security programs:

_C-TPAT (Customs-Trade Partnership Against Terrorism)_ – Joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security.

_Container Security Initiative (CSI)_ – A U.S. Customs program created in 2002 to implement screening of targeted containers at overseas ports before they arrive in the United States.

_The 24 Hour Rule_ – Requires that U.S. Customs must receive cargo information from carriers 24 hours before cargo intended for the United States is loaded on a ship at a foreign port. This new rule took effect on December 2, 2002.

_The Advanced Trade Data Initiative (ATDI)_ – A supply chain management system security program designed to work with C-TPAT. The ATDI is a component of the U.S. Customs and Border Protection’s (CBP’s) effort to “push the border out.” The ATDI program works hand-in-hand with the private sector to obtain information on U.S. imports as far upstream as possible. The information is then used to validate and track container shipments throughout the supply chain process. The information is used to target containers as far upstream as possible, minimizing friction during the shipping process and reducing the risk of delays in clearing borders due to security concerns.

_The Maritime Transportation Security Act (MTSA)_ – Landmark legislation that significantly reduced vulnerabilities to the nation’s maritime transportation system. This law is the American equivalent of the International Ship and Port Facility Security (ISPS) code and was fully implemented on July 1, 2004. MTSA directed the Department of Transportation and Department of Homeland Security to identify vessels and facilities that pose a high risk of being involved in a transportation security incident in addition to making vulnerability assessments of U.S. port facilities and vessels. The bill also required that private sector owners and operators of vessels and facilities submit a security plan to the Department of Homeland Security and the Department of Transportation.
SAFE Port Act (The Security and Accountability For Every Port Act) – Focuses on enhancing port security and was signed into law by President Bush on October 13, 2006.

Smart and Secure Trade Lanes Initiative (SST) – Industry-driven in cooperation with government agencies supply chain security initiative that consists of improved secure business practices, advanced technologies and supply chain security authorities in a global end-to-end information network across multiple global trade lanes.

Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework) – Strategy developed by the World Customs Organization to secure the movement of global trade in a way that does not impede, but rather facilitates, the movement of global cargo.

Transportation Workers Identification Card (TWIC) – A joint effort between the Transportation Security Administration and the U.S. Coast Guard to create a standard biometric ID for all port workers and truck drivers carrying cargo to and from U.S. ports. The program is in the initial stages of implementation and may later be expanded outside the port domain.
Appendix C: Direct and indirect benefits of security investments

Investments made in intelligent immunity for global movement systems will have both direct and indirect benefits. These benefits are highlighted in Figure 14.

<table>
<thead>
<tr>
<th>Security investment</th>
<th>Direct benefits</th>
<th>Indirect benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical security</td>
<td>• Controlled access keeps out unauthorized personnel</td>
<td>• Customer recognition of the firm’s safe and secure environment as an expertise, increasing customer loyalty</td>
</tr>
<tr>
<td></td>
<td>• Protection of intellectual property, capital equipment and personnel</td>
<td>• Fewer thefts and overages, shortages and damages (OS&amp;D) by virtue of having a more secure facility</td>
</tr>
<tr>
<td></td>
<td>• Protection of product integrity</td>
<td>• Reduced equipment damage and operating costs (therefore, potentially lower insurance rates)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fewer safety incidents and catastrophes</td>
</tr>
<tr>
<td>Personnel security</td>
<td>• Thorough background check eliminates malicious actors from hiring pool</td>
<td>• Customer loyalty, increased sales revenues, higher market share</td>
</tr>
<tr>
<td></td>
<td>• Periodic follow-up checks for employees in sensitive positions</td>
<td>• Employee commitment and belief in company’s concern for employees</td>
</tr>
<tr>
<td>Transportation and conveyance security</td>
<td>• Reduces theft losses</td>
<td>• Cost avoidance of non-product-related costs (indirect costs)</td>
</tr>
<tr>
<td></td>
<td>• Reduces adulteration of product</td>
<td>• Crime and vandalism rates fall</td>
</tr>
<tr>
<td></td>
<td>• Reduces chance of cargo vessel misuse (weapon delivery system)</td>
<td>• Fewer disruptions to the supply chain, more cost savings compared with avoided losses</td>
</tr>
<tr>
<td></td>
<td>• Protects conveyance equipment, vessels</td>
<td>• Less capital required for inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reduced transportation cycle time</td>
</tr>
<tr>
<td>Asset visibility and tracking</td>
<td>• Provides positive location status, preventing unauthorized departure from official and expected path</td>
<td>• Lower theft and losses</td>
</tr>
<tr>
<td></td>
<td>• Time-definite and controlled chain of custody</td>
<td>• Faster recalls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fewer delayed shipments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Better planning, enabling lower working capital needed for inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Less OS&amp;D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protection of brand name</td>
</tr>
<tr>
<td>Building organizational infrastructure awareness and capabilities</td>
<td>• Builds awareness of security concerns</td>
<td>• Increases problem prevention through recognition by employees</td>
</tr>
<tr>
<td></td>
<td>• Role of security in daily operations and virtually every assignment</td>
<td>• Early intervention, reducing impact of a disruption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Improves the ability to respond with early awareness</td>
</tr>
<tr>
<td>Collaboration among supply chain parties</td>
<td>• Improved coordination along supply chain increases security</td>
<td>• Platform for broader alignment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enables creation of a more secure supply chain network for common problem-solving, resource sharing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Communication among supply chain partners, potentially reducing coordination costs</td>
</tr>
<tr>
<td>Security investment</td>
<td>Direct benefits</td>
<td>Indirect benefits</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Supplier selection and investment           | • Facilitates coordination of multi-company security activities (initiatives, sting operations, incident investigations)  
• Security breaches easier to spot with standard systems  
• Higher levels of security with common procedures  
• System-level and supplier security improvement | • Improves the efficiency of ship, train, truck, terminal operations; cuts international shipping times  
• Platform for collaboration within an industry leading to standards that raise level of performance  
• Process discipline enables compliance (quality, safety, process), higher performance  
• Common processes reduce confusion, raise predictability, improve staff backup  
• Reduces non-security losses |
| Voluntary security compliance               | • European Union’s Authorized Economic Operator program helps ensure a base level of supply chain security assessment  
• Customs specialists working in specialized security programs may observe risk of security breach before breach can occur  
• C-TPAT membership provides member companies with information about industry “best practices” in supply chain security  
• Sweden’s StairSec program leads to higher inspection rates of uncertified cargo, increasing likelihood of early warning and prevention | • Establishes a “mandatory” fundamental standard across industry for supply chain security via a “voluntary” program  
• Platform for collaboration and alignment within an industry that leads to industry standards, raising overall level of performance in quality, service, and cost  
• C-TPAT supply chain specialist assists firm as the U.S. Customs and Border Protection’s (CBP’s) liaison for validation, security issues, procedural updates, communication and training  
• Faster border throughput times from fewer inspections and “green lane” flow, which may raise service levels, enabling lower working capital  
• Process discipline enables compliance (quality, safety, process), higher levels of process performance |
| Proactive investments                       | • Technology provides increased ability to track, monitor and observe material flows, preventing unauthorized departure from official and expected path | • Ability to customize the application to the benefit of the firm  
• Increases process efficiency through technology  
• Visibility investments give realtime awareness of supply chain delays, location and status |
| TQM                                         | • More consistent security procedure execution  
• Application of Six Sigma may lead to disciplined loss reduction efforts  
• Lower losses  
• Higher-performance employees emphasize security  
• Process design standardizes security processes  
• Design supply chain with fewer handoffs, keeping product moving | • Discipline increases, enabling compliance (quality, safety, process)  
• Reduction in safety stock, lead-time variance, and lower OS&D  
• Better process knowledge and management from additional data, greater visibility to discern bottlenecks and congestion |

Endnotes

1 A public good is defined as a society-wide good such as national defense and environmental sustainability that is normally provided by governments by way of taxation since no market forces exist to provide public goods. Additionally, it costs little or nothing for an extra individual to enjoy a public good while the costs of withholding that good or depriving any individual of it are high.


7 This is known as dynamic instability, a key component of chaos theory, which was discovered by physicist Henri Poincare in the early 20th century.


11 In the United States, for example, the 9/11 attacks disrupted trade flows across the Canadian and Mexican borders, which soon resulted in the shutdown of much of Ford Motor Company's manufacturing, as parts shortages halted the company's near-just-in-time deliveries.


21 Ibid.


23 Ibid. This reference applies to this whole paragraph.

24 See http://en.wikipedia.org/wiki/2003_Italy_blackout

25 This is known as dynamic instability, a key component of chaos theory, which was discovered by physicist Henri Poincare in the early 20th century.

26 The electric grid provides a powerful example of cascading effects. A sustained and widespread power outage would affect a range of other sectors, including transportation systems, wastewater treatment, and food and water supplies. Disruptions in these sectors would then spill over into other sectors. See the sidebar, "Seven types of risks to global movement systems."


29. Interview by Daniel B. Prieto, Vice President of IBM Global Business Services, with a senior Egyptian counterterrorism official.


31. It is worth noting, however, that in most instances, terrorists have not entered the United States illegally but have entered the system legally, thereby working within the U.S. immigration system to enter the United States.


42. For further explanations of hawala financing see, for example, testimony by Patrick Jost for a hearing entitled “Hawala and Underground Terrorist Financing Mechanisms” before the Senate Committee on Banking, Housing, and Urban Affairs, Wednesday, November 14, 2001. http://banking.senate.gov/01_11hrg/111401/jost.htm


44. We slightly refined the original six security and resilience business functions (Risk Management, Credentialing, Inspections, Tracking, Enforcement/Interdiction and Command/Control/Integration) in IBM’s previous Global Movement Management paper and added four new functions: Facility Security, Conveyance Security, Enterprise-wide Security Training, and Resilience Engineering & Response Planning. We renamed some functions and divided the ten functions into the five traditional security functions and five emerging security functions discussed.


**See http://www.unescap.org/ttdw/Publications/TFS_pubs/pub_2398/pub_2398_fulltext.pdf**

**Unpublished internal IBM study by Glenn, Thomas, Senior Managing Consultant, IBM Global Business Services. Global Supply-Chain Management Solutions.**


**“9-11 Commission Report.” National Commission on the Terrorist Attacks on the United States, 20 September, 2004. http://www.9-11commission.gov/report/911Report_Ch1.htm. “Nawaf al Hazmi set off the alarms for both the first and second metal detectors and was then hand-wanded before being passed. In addition…video footage indicates that he was carrying an unidentified item in his back pocket, clipped to its rim. When the local civil aviation security office of the Federal Aviation Administration (FAA) later investigated these security screening operations, the screeners recalled nothing out of the ordinary…We asked a screening expert to review the videotape of the hand-wanding, and he found the quality of the screener’s work to have been ‘marginal at best’. The screener should have ‘resolved’ what set off the alarm; and in the case of both Moqed and Hazmi, it was clear that he did not.”**

**Hench, David. “Ticket Agent Haunted by Brush with 9/11 Hijackers.” Portland (ME) Press Herald, 6 March, 2005. http://www.atca.org/singlenews.asp?item_ID=&comm=0. “Michael Tuohey, a U.S. Airways ticket agent checked in 9/11 hijackers Mohammed Atta and Abdul Aziz Alomari for their flight from Portland International Jetport. Tuohey held himself at least partly responsible as he was suspicious of them but ignored his instincts and did nothing. The Portland police chief whose detectives interviewed Tuohey after the attack, said he would have been surprised if anyone in Tuohey’s position had taken action. ‘At that point in time, the United States of America was not under attack…You can’t beat yourself up… What was he going to report, and who was he going to report it to?’”**

**The Framework of Standards to Secure and Facilitate Global Trade is a global initiative aimed at securing and facilitating the global trading system on a multilateral basis and making this regulatory structure more uniform. Adopted in June 2005, The framework, commonly called the SAFE Framework, established a comprehensive framework of global supply chain security standards and best practices, covering both government-to-government arrangements as well as government-to-business partnerships, in order to lift standards for supply chain security worldwide and to harmonize the “rules-of-the-road” of the global economy.**


**“A wiki is a “medium which can be edited by anyone with access to it, and provides an easy method for linking from one page to another. Wikis are typically collaborative websites, though there are now also single-user offline implementations.” See http://en.wikipedia.org/wiki/Wiki**


**See Wilson, Michael. “Loved Ones Turn to Web for Searches in Flood Zone.” New York Times. 1 September, 2005.**


“…the Holy Grail for developers of the semantic Web is to build a system that can give a reasonable and complete response to a simple question like: I’m looking for a warm place to vacation and I have a budget of [US$]3,000. Oh, and I have an 11-year-old child.”


According to the U.S. National Academy of Science, 80 percent of business is conducted on unstructured data, 85 percent of all data stored is unstructured, and there is a 60 percent annual growth rate for unstructured data. Also see White, Colin. “Consolidating, Accessing and Analyzing Unstructured Data.” Business Intelligence Network. December, 2005. According to White, 80 percent of business is conducted on unstructured information (Gartner Group), and 85 percent of all data stored is held in an unstructured format (Butler Group). http://www.b-eye-network.com/view/0. Also see Connor, Deni. “Start-up to index e-mail, other unstructured content.” Network World. 1 August, 2005. “The Enterprise Strategy Group estimates that as much as 80% of the data on the network is unstructured and Gartner says this will increase from nearly 4 million terabytes today to as much as 15.2 million terabytes in 2009.”


Sheffi, Yossi. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, MIT Press, 2005. p. 138. For example, Intel and other high technology companies joined together in 1997 to create the Technology Asset Protection Association. The Critical Materials Council monitors the global supply chain for semiconductors and potential disruptions ranging from material shortages to political disruptions. Data sharing among casinos gives participating casinos access to a facial recognition database that helps them identify cheats and card counters. Collaboration between spirits distillers showed common losses for all of them on one delivery route, a pattern that would not have been identified without mutual cooperation. Industry association efforts include the Retail Industry Leaders Association (RILA), the Toy Industry Association, and the Postal and Shipping Coordination Council, which comprises competitors UPS, FedEx and DHL.


The Q8.com service is used primarily by shippers to share data with other companies and the government within a permission-based system to gain better visibility into parts of their supply chain. Participants who share their information also find more efficient treatment from the security officials in port who access the same data to confirm risk targeting. It is a start, and this model may incentivize the first movers by rewarding them with an advantage. In 2006, the example is also discussed in detail in Friedman, Thomas, “The World Is Flat: A Brief History of the 21st Century.” Farrar, Straus and Giroux, expanded and updated edition, 2006.

Ibid.


Ibid.

Benkler, Yochai. “The Wealth of Networks: How Social Production Transforms Markets and Freedom,” Yale University Press. 2006. The benefits of peer production are well established in the software world. Under the traditional model, source code is guarded by a core group of developers. Under a model where anyone can participate (e.g., a “bazaar model”), source code is released on the Internet for anyone to work with and modify.


The ARPA Net used a protocol named Network Control Program (NCP). NCP was the predecessor of TCP/IP, where IP (Internet Protocol) defines the packets that transport data between nodes, while TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) establish the protocols by which data is transmitted.

The internet only took off after HTML allowed the ready conversion of text to Web pages, HTTP enabled easy Web publishing and retrieval, and Web browsers allowed users to easily display, access and search information across many Web sites. Over the course of the public Internet’s first decade, it successfully accommodated the majority of previously existing public computer networks. Within 15 years of the first Web page, the Internet is now a “network of networks” comprising millions of smaller domestic, academic, business and government networks. As of 10 June, 2007, 1.13 billion people use the Internet (see Internet World Stats at http://www.internetworldstats.com/stats.htm).

The greatest number of connections possible in a network with N nodes is N (N-1)/2 – also called Reed’s Law.

For instance, a card catalog entry for a book in a library is described by only a few simple data elements (title, author, classification, etc.) in a fixed format. What happens when someone wants to use new “tags” or “labels” to describe a book which do not conform to the original classification system? Metadata tagging allows a new taxonomy and new labels to be layered onto existing classification systems. In the library book example, a travel book might have the Dewey-decimal data of title, author, travel and publication date. With metadata tagging, a user could layer on other descriptive elements that have meaning for that user: “books with a red cover,” “books my mother likes,” “books I recommend to my friends.” By being able to retain formal data labels while allowing for the creation of additional, e.g., “informal”, descriptive labels, previously “trapped” or incompatible data can become sharable and interoperable because it would no longer be bound by its original and less flexible taxonomy, data label or meaning.

The U.S. Securities and Exchange Commission (SEC), the U.K.’s Financial Services Administration and the Chinese Securities Regulation Commission are adopting XBRL for financial data reporting, and stock exchanges in Frankfurt, Madrid, Melbourne, Seoul, Shanghai, Tokyo and Toronto are all implementing XBRL. It is expected that the SEC will eventually require public companies filings in XBRL. XBRL operates like a “bar code” for financial statements. It tags items in financial statements so data items are easily retrievable and more readily understandable. If, for example, you apply the tag for revenue to the revenue line of an income statement, a tool that can read XBRL would identify the item as revenue, how it is defined, what currency it is in, what period it covers and for what company. This allows users of financial statement information to electronically retrieve data in a matter of seconds and do it at scale much more efficiently. In the recent past, junior analysts on Wall Street would have to laboriously comb through printed reports and manually reenter that data into spreadsheets to perform analyses. Now, when data is defined in context in an XBRL document, only a simple query is needed to ask a system to find all financial data for a given company or a range of companies. For example, a user could simply ask for operating profit numbers for software companies with revenue over US$100 million.

See http://www.xbrl.org: “Computers can treat XBRL data ‘intelligently’: they can recognize the information in a XBRL document, select it, analyze it, store it, exchange it with other computers and present it automatically in a variety of ways for users. Companies can use XBRL to save costs and streamline their processes for collecting and reporting financial information. Consumers of financial data, including investors, analysts, financial institutions and regulators, can receive, find, compare and analyze data much more rapidly and efficiently if it is in XBRL format. Data can be transformed into XBRL by suitable mapping tools or it can be generated in XBRL by appropriate software.”

Technologies that back up identity services include the Department of Defense Common Access Card system and biometrics.


As another example, see http://www.smartmoney.com/marketmap which shows a highly-effective realtime visual
summary of the minute-by-minute movements of hundreds of individual stocks and dozens of economic sectors in one efficient picture.


The United Nations Foundation is working with a major cell phone provider and mobile network operator to address healthcare challenges in Africa by collaborating with the WHO and national health ministries to build digital health data systems. These systems are powered by data gathered by on-the-ground health professionals equipped with personal digital assistants (PDAs) and flexible epidemiological surveillance software. The partnership launched a major program in June 2006 to fund training, software and mobile computing devices for the full complement of health data officers in Burkina Faso, Kenya and Zambia to support the fight against measles, through the non-governmental organization DataDyne. WHO and local ministries believe that the new systems will result in a more effective and efficient measles control effort. Following a three-country rollout, the program will create new digital health systems in over 20 other measles-affected countries in Africa, while working to make technology tools available to health workers fighting other diseases, such as malaria, and to integrate additional applications, such as health mapping. For additional information on the United Nations Foundation program see: http://www.unfoundation.org/vodafone/health_data_systems.asp, http://www.unfoundation.org/files/pdf/2007/EpiSurveyor_Polio_Kenya.pdf, and http://www.youtube.com/watch?v=g4SoENpkbXg

Tier 3 in the context of Global Movement Management refers to a global economic grouping of nations with economies smaller than G8 or second-tier economies of developed and larger developing economies. In terms of private sector entities, this would include small- to medium-sized enterprises as opposed to multinational corporations.


The Clinton Administration issued “A Proposal to Improve the Technical Management of Internet Names and Addresses” as part of the implementation of its “Framework for Global Electronic Commerce.” Referred to as the “Green Paper,” it was first published in the Federal Register on 20 February 1998 to provide an opportunity for public comment. The Green Paper proposed the creation of a new, private sector not-for-profit corporation to be managed by an expert and globally representative Board of Directors.


ICANN today is a not-for-profit corporation headquartered in Marina Del Ray, California, and managed by a professional staff with oversight from a Board of Directors representing numerous Internet technical and policy stakeholders. ICANN also receives input from an at-large “advisory” committee composed of interested parties from the international community, and it holds public meetings around the world to encourage international input into Internet governance decisions.


The current member states of the Paris MOU region include Belgium, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Russian Federation, Slovenia, Spain, Sweden and the United Kingdom.


IBM formed a coalition of private sector representatives as part of the research that shaped this paper. The Global Movement Management Coalition is a group of companies and non-governmental organizations focused on
improving the security and resilience of the global economic systems. The Coalition was created in 2006 to assert private sector leadership in addressing this challenge and to organize the expertise of a range of stakeholders in the system. This Coalition could be charged with forming the private sector advisory group.

Models for this type of cooperation exist at the international and multinational levels. A grant- or loan-making mechanism may work similar to the U.S. Defense Security Cooperation Agency (DSCA) that enables countries with a shared interest in security to build more effective and interoperable defense capabilities through training, capacity building and materiel sales or grants. Similarly, when the G8 established the Counterterrorism Action Group (CTAG), it established a multinational organization charged with focusing on connecting mutual interests and shared strengths while “building political will, [and] coordinating capacity building assistance where necessary.” Adopting a process similar to the DSCA at the global level should focus more broadly on the improvement of capacities and competencies that relate to trade, security and resilience within the Global Movement Management context. A Global Movement Systems Development and Support Organization could be responsible for issuing loans and assistance to Tier 2 or Tier 3 countries to target investments that improve their security, resiliency and trade facilitation over time, thereby developing nascent players to contribute to and expand the playing field for other participants. A combination of WCO assessments and other political risk measures used today by the quasi-government Overseas Private Investment Corporation and the Export-Import Bank would help ensure that funding is closely tied to global economic market standards (e.g., transparency, rule of law, anti-corruption).

Other incentives would include greater facilitation by customs and duties officials capable of verifying contents and information provided, therefore improving targeting of those malicious actors who represent a threat. Greater harmonization delivers other untapped efficiencies in the areas of data exchange, work flow and communications in general. Finally, one could anticipate potentially lower insurance rates as risk is determined with greater veracity. Effective measures to reduce exposure to risk or mitigate its consequences also can help lower insurance rates.

To measure progress, the organization would use a “managing for progress” set of outcome-oriented metrics and Web-based reporting systems to track a range of enhancements in security, resilience and trade facilitation. In addition to the inherent benefit of improved infrastructure and accessibility, a type of Baldrige Quality Award process may be useful to identify best practices and to evaluate annual competition for quality in terms of security, resilience and facilitation.

Examples today would include the Q8.com service used primarily by shippers to share data with other companies and the government in a permission-based system to gain better visibility into parts of their supply chain. Participants who share their information also find more efficient treatment from the security officials in port who access the same data to confirm risk targeting. It is a start, and this model may incentivize the first movers by rewarding them with an advantage.


ISO 9000 is a group of standards focused on quality management systems that is maintained by the International Standards Organization.

“The Malcolm Baldrige National Quality Award was created by Public Law 100-107, signed into law on August 20, 1987. The Award Program, responsive to the purposes of Public Law 100-107, led to the creation of a new public-private partnership. Principal support for the program comes from the Foundation for the Malcolm Baldrige National Quality Award, established in 1988.” From the National Institute of Standards and Technology’s (NIST’s) Web site. http://www.quality.nist.gov/Improvement_Act.htm

“The Baldrige Criteria for Performance Excellence provide a systems perspective for understanding performance management. They reflect validated, leading-edge management practices against which an organization can measure itself. With their acceptance nationally and internationally as the model for performance excellence, the Criteria represent a common language for communication among organizations for sharing best practices. The Criteria are also the basis for the Malcolm Baldrige National Quality Award process.” From the National Institute of Standards and Technology’s (NIST’s) Web site. http://www.quality.nist.gov/Business_Criteria.htm.

**See www.MIPT.org.

**The Risk Preparedness Index was developed jointly by accounting firms PricewaterhouseCoopers, Ernst & Young LLP, Deloitte & Touche LLP, KPMG International and AIG International Inc. in 2004 as part of the Global Security Consortium. See “Big four accounting firms join in cyber-risk effort: They’re creating an index to gauge firms’ preparedness.” Computerworld. March 22, 2004.