

Industry Agenda

Building Resilience in Supply Chains

An Initiative of the Risk Response Network
In collaboration with Accenture

January 2013



© World Economic Forum

Accenture

2013 - All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

The views expressed are those of certain participants in the discussion and do not necessarily reflect the views of all participants or of the World Economic Forum.

REF150113

Contents

4	Acknowledgements
5	Foreword
5	Executive Summary
8	Introduction
9	Why Now? – Phase I Origin
9	Global Disruptions in 2012
11	Workshop Outcomes
12	Revisiting the Risk Landscape
13	An Evolving Risk Landscape
14	Risk Landscape across Europe, North America and Asia, 2012
15	Cyber Risk – An Emerging Concern
18	Building Resilient Supply Chains
19	What Is Resilience?
19	Challenges to Resilience
20	Resilience Measures
21	A Blueprint for Resilient Supply Chains
26	Recommendations
28	Workshop Participants
32	Appendices
40	Sources

Acknowledgements

Primary Authors

Gurpriya Bhatia
Project Manager, Mobility Industries, World Economic Forum
(on secondment from Accenture)

Charles Lane
Project Manager, Risk Response Network, World Economic Forum

Adrian Wain
Project Analyst, Accenture

Editors World Economic Forum

Elaine Dezenski
Senior Director, Head of Partnering Against Corruption Initiative
(PACI)

Sean Doherty
Director, Head of Supply Chain and Transport Industry

John Moavenzadeh
Senior Director, Head of Mobility Industries

Accenture (Strategic Partner and adviser)

Jonathan Wright
Managing Director, APAC Management Consulting-
Communications, Media and Technology Sector

Ronald Ash
Senior Executive, Health and Public Services

Rebecca Green
Manager, Operations Consulting

Special thanks to Ann St. John-Hall, Freelance Editor and Moritz Stefaner, Freelance Information Visualizer Contributors

Alexandra Brintrup
Supply Chain Resilience Expert, University of Cranfield

Allen Bruford
Deputy Director, Compliance and Facilitation Directorate, World
Customs Organization

Jose Holguin-Veras
Professor and Acting Department Head, Center for Infrastructure,
Transportation and the Environment, Rensselaer Polytechnic
Institute (RPI)

Anders Karlborg
Vice-President, Supply Chain, Huawei Technologies Co.

Karen Lim
Head, Trade Strategy and Security, Singapore Customs

Thomas Lin
Head, Office of Supply Chain Security Management, Hong Kong
Special Administrative Region

Miguel Jaller Martelo
Research Associate, Center for Infrastructure, Transportation and
the Environment, Rensselaer Polytechnic Institute (RPI)

Sean K. Moon
Acting Director, Transportation and Cargo Policy Development, US
Department of Homeland Security

Seth Stodder
President and Chief Executive Officer, Palindrome Strategies

Ella Smith
Intern, World Economic Forum

Wessel Van Kampen
Associate Director
Network of Global Agenda Councils
World Economic Forum

Nick Wildgoose
Global Corporate, Supply Chain Product Leader, Zurich Insurance
Group

Advisory Board

Peter Graham
Associate Partner and Global Leader, Border Security and
Immigration, IBM Business Consulting Services

Sylvain Levesque
Vice-President, Corporate Strategy, Bombardier

Gary S. Lynch
Managing Director and Global Leader, Marsh Risk Consulting,
Marsh

Robert Missen
Head of Unit C-3, Maritime and Land Transport Security, European
Commission

Yossi Sheffi
Professor of Engineering Systems; Director, Transportation and
Logistics, Massachusetts Institute of Technology

Pyers Tucker
Global Head, Strategy, Damco International

Zhu Gaozhang
Director, Enforcement and Facilitation, World Customs
Organization (WCO)

Foreword



Martin Senn
Group Chief
Executive Officer
Zurich Insurance
Group

Foreword by Zurich Insurance Group

International trade is vital to the world economy. Businesses that trade internationally are supported by interlinked global supply chains, which are vital to their competitiveness. But as a number of recent events highlight, these dynamic, complex systems are vulnerable to numerous risks. Because of their interconnectedness, even small, localized events can escalate rapidly and cause significant disruptions.

Phase I of the Supply Chain Risk Initiative (SCRI) culminated in the publication of the report *New Models for Addressing Supply Chain and Transport Risk*, which explored the supply chain risk landscape. And in tandem with the launch of the Phase I report at the Forum's Annual Meeting in Davos, the U.S. launched its first Strategy for Global Supply Chain Security. This strategy aims to protect our global supply chains and calls for an increased multi-stakeholder dialogue. It emphasizes the need to foster a resilient system that can absorb shocks and recover rapidly from disruptions.

Phase II of the Supply Chain Risk Initiative builds on this theme. This report endorses the requirement for a multi-stakeholder risk assessment framework and the need to build agile and adaptable strategies that will improve resilience and protect against a range of global disruptions.

Throughout 2012, there have been continuing concerns about external threats to supply chains from physical and non-physical factors such as IT failures, pandemics, natural disasters, or attacks involving weapons of mass destruction. But the message need not focus just on the threat of potentially unmanageable risks.

Government and industry experts can work together on key aspects of resilience - such as partnerships, policies, strategies and technological components governing supply chains - in order to build a foundation for a truly effective resilience framework. We support enhanced coordination with our industry partners, the international community and stakeholders around the globe to help transform this strategic vision into action.

A handwritten signature in black ink, appearing to read 'Senn', written in a cursive style.

Foreword



Elaine Dezenski
Senior Director,
Head of Partnering
Against Corruption
Initiative (PACI)

Foreword by World Economic Forum

The World Economic Forum is pleased to have engaged multiple industries, regions and governments in continued dialogue on the important topic of Supply Chain Risk. Although this topic originated with the supply chain and transport industry community in the Forum, interest has spread to a wider group of industries and public officials, reflecting the complexity of supply chain networks. Developing resilience as a core component of protecting and enhancing global supply chains is increasingly a priority for national and international organizations, and was the primary focus of our second phase of dialogue and research. The concept of resilience helps move beyond prescriptive regulatory frameworks- historically focused on singular risks- to more flexible and agile public-private partnerships that help organizations prepare and respond to a broad range of potential disruptions in the future. We hope that the concepts and ideas discussed in the Supply Chain Risk dialogue will serve as an effective resource and reference point for current and future work in supply chain risk management.

We acknowledge in particular the tremendous support and collaboration of Accenture in both Phase I and II.



John Moavenzadeh
Senior Director,
Head of Mobility
Industries
Officer, World
Economic Forum
USA

A handwritten signature in blue ink, appearing to read "Elaine Dezenski".

A handwritten signature in black ink, appearing to read "John Moavenzadeh".

Executive Summary

Global supply chains and transport networks form the backbone of the global economy, fuelling trade, consumption and economic growth. Disruptions to supply chains can prove costly, as highlighted most recently by Hurricane Sandy. According to research conducted by Accenture, significant supply chain disruptions have been found to cut the share price of impacted companies by 7% on average.

The World Economic Forum's Supply Chain Risk Initiative first started exploring systemic risks and vulnerabilities to global supply chains and transport networks in 2011. The initiative's phase I report, *New Models for Addressing Supply Chain and Transport Risk*, launched at the World Economic Forum Annual Meeting 2012 in Davos-Klosters, examines the systemic supply chain risk landscape and the possibility of these risks causing serious disruptions to global supply chains. It highlights the need to shift focus from reactive to proactive risk management. At the same time as the launch of this report, the US government launched its Strategy for Global Supply Chain Security, calling for a global multistakeholder dialogue to effectively safeguard supply chains.

Throughout 2012, concerns have remained about external threats to supply chains (such as natural disasters and demand shocks) and systemic vulnerabilities (such as oil dependence and information fragmentation). Additionally, growing concern around cyber risk, rising insurance and trade finance costs are leading supply chain experts to explore new mitigation options. Accenture research indicates that more than 80% of companies are now concerned about supply chain resilience.

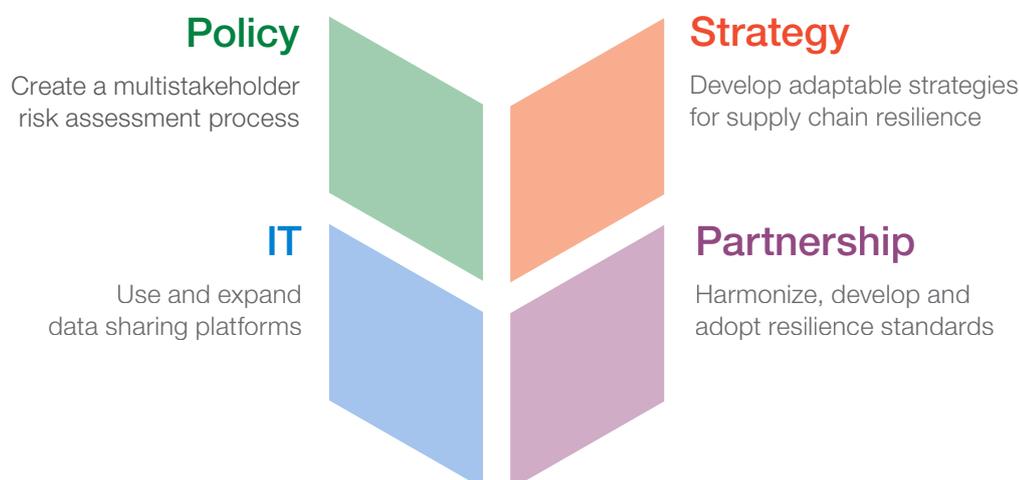
This report, **Building Resilience in Supply Chains**, developed during phase II of the initiative, explores government and industry sector views on systemic supply chain risks and building a resilience framework to manage them. The report findings are based on expert level workshops and data gathering throughout 2012. Notable differences in perspectives stem from government responsibility for public security and long-term risks compared to industry's focus on ensuring that supply chains work effectively on a day-to-day basis. Differences in regional perspectives, attributed

to differences in disruption histories and growth expectations, also point to the need for a harmonized resilience framework. However, the top risk concerns in Europe, North America and Asia in 2012 showed little change from the previous year apart from a sharp rise in concern about extreme weather. Of emerging non-traditional risks, cyber risk is perceived to have the greatest implications for supply chains.

The workshops and dialogues have produced suggestions on how to ensure that business and government approaches to building resilience are complementary. Three "must have" requirements have emerged from our analysis: the need for a common risk vocabulary; improved data and information sharing across supply chain actors; and building greater agility and flexibility into resilience strategies. This led to the creation of an overall blueprint for resilient supply chains based on four core components: partnerships, policy, strategy and information technology (IT). This blueprint underpins a set of recommendations to guide multistakeholder engagement.

Systemic risks have global geographic scope, cross-industry relevance, uncertainty as to how and when they will occur, and high levels of economic and/or social impact requiring a multi stakeholder response. These risks are also magnified by the way supply chain systems are configured; and cannot be mitigated by individual actors. Risk management must be an explicit but integral part of supply chain governance. To achieve this, several steps are recommended:

- Institutionalize a multistakeholder supply chain risk assessment process rooted in a broad-based and neutral international body
- Mobilize international standards bodies to further develop, harmonize and encourage the adoption of resilience standards
- Incentivize organizations to follow agile, adaptable strategies to improve common resilience
- Expand the use of data sharing platforms for risk identification and responses



1. Introduction



- Phase I of the Supply Chain Risk Initiative called for an urgent need to review supply chain risk management practices to cope with a new era of increased volatility.
- Throughout 2012, systemic risks and vulnerabilities, including extreme weather events, political unrest and cyber risk, continued to be a top concern for supply chain managers globally.
- Three “must have” requirements to develop a resilience framework have emerged: the need for a common risk vocabulary; improved data and information flow across supply chain actors; and building greater agility and flexibility into supply chain systems.

Why Now? – Phase I Origin

its Annual Meeting 2012 in Davos-Klosters, and in collaboration with academic, industry and government experts, the World Economic Forum launched **New Models for Addressing Supply Chain and Transport Risk**.¹ This report ranks the top potential risks and vulnerabilities in global supply chains, and offers recommendations for business and government to address them.

A key takeaway from meetings in Davos-Klosters was the urgent need to review risk management practices for a new era of increased volatility (see figure 1).

In tandem with the launch of the phase I report, the United States Secretary of Homeland Security Janet Napolitano launched the first US Strategy for Global Supply Chain Security and called for increased global dialogue on risk and resilience.

Global Disruptions in 2012

Fallout from natural disasters and emerging threats continued to grab headlines throughout 2012. Systemic vulnerabilities in supply chains, such as oil dependence and continued armed conflict in the Middle East, remain.²

In November 2012, Hurricane Sandy closed ports and airports in the north-eastern USA and prompted the worst fuel shortages since the 1970s. Small-scale rationing was introduced and Jones

Act exemptions³ were issued to allow deliveries by foreign tankers. Cost estimates for repair and preventative measures topped US\$ 70 billion.⁴

The impact of Thailand’s floods persisted into early 2012, affecting the automotive and high-tech industries. More than 1,000 factories were hit, with subsequent insurance claims reaching US\$ 20 billion. As a result of the flooding, Thai GDP growth projections decreased from 2.6% to 1%.⁵ Flooding continues to be a concern with up to one-quarter of Thailand’s provinces affected by floodwaters in 2012.⁶

In the US, severe prolonged drought has caused crop failure and the lowest water levels the Mississippi river has seen in two decades. US\$ 180 billion of goods moves along this artery each year, with each barge carrying the equivalent of 530 rail cars. For every foot (30.5cm) drop in the water level, barges must offload 185 tonnes of cargo.⁷

Famine in the Horn of Africa was brought under control but questions remain about the world’s inability to prevent a foreseeable tragedy. More than 13 million people, mostly women and children, were affected by this crisis, yet it was mainly man-made. Early warning signs were inadequately addressed. The difficulty of balancing security and other risks also became clear, requiring some relaxation in policies in order to facilitate the flow of humanitarian supplies through supply chains controlled by militia groups.⁸

Figure 1: Increased volatility

Source: Christopher, Martin, M. Holweg, (2011). ‘Supply Chain 2.0’: managing supply chains in the era of turbulence, *International Journal of Physical Distribution & Logistics Management*. Vol. 41 Iss. 1, pp. 63-82.

Increased volatility is the new normal for globalized and interconnected supply chains. Supply chain risk management approaches configured for more stable times now need to be updated.



On a global level, cyber risk to supply chains has become a priority issue. Concern is growing about systematic attacks on financial institutions leading to reduced ability to make and receive payments. The effects would be extremely severe across industries and regions alike.⁹

The high cost of disruptions has led insurers to reduce coverage and increase premiums. Trade finance, another traditional buffer, is under pressure from Basel III reforms.¹⁰ Supply chain managers want to better understand the new rules in order to reduce premiums and target coverage effectively.

Phase I sought to explore supply chain risks and establish a common conceptual framework. It distinguished between external disruptions and intrinsic vulnerabilities. The expert group agreed that the most likely triggers of global supply chain disruptions are natural disasters, conflict and sudden demand shocks, while the major vulnerabilities are dependence on oil and problems with visibility and control. The group put forward a list of the **top five risk management priorities** (see figure 2) for both business and government.

Phase II has engaged a broader global group of government and industry decision-makers, to address three areas in more detail:

- Strengthening the framework for global risk assessment
- Developing a blueprint for resilience across supply chains
- Exploring data and information sharing as a key element of resilience

Data gathering was conducted via the World Economic Forum's Supply Chain Risk Radar survey and through a series of regional workshops (see figure 3 and figure 4).

Figure 2: Top five risk management priorities

Owner	Recommendation
Public	Improve international and inter-agency compatibility of resilience standards and programmes
Private	More explicitly assess supply chain and transport risk as part of procurement, management and governance processes
Joint	Develop trusted networks of suppliers, customers, competitors and government focused on risk management
Joint	Improve network risk visibility through two-way information sharing and collaborative development of standardized risk assessment and quantification tools
Joint	Improve pre- and post-event communication on systemic disruptions and balance security and facilitation to bring a more balanced public and private sector collaboration

Figure 3: The Supply Chain Risk Radar

The survey-based Supply Chain Risk Radar looks to prioritize aspects of supply chain disruptions, vulnerabilities and resilience as a basis for multistakeholder dialogue.

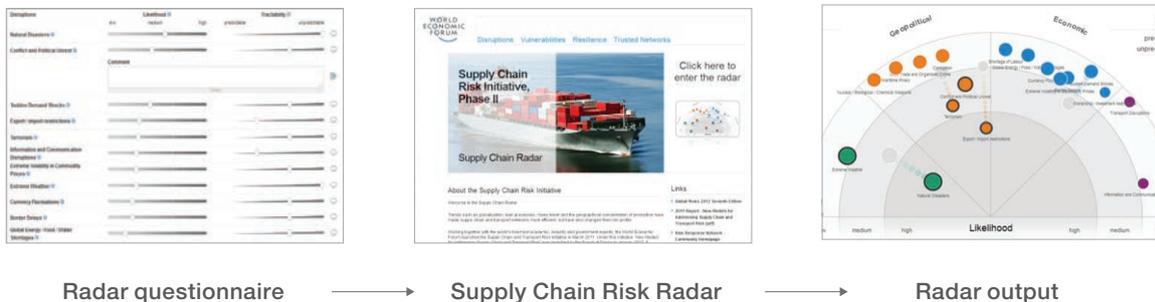


Figure 4: Regional workshop series

Six workshops during 2012 brought government and industry together to explore the most important factors for resilience in global supply chains. Workshops were structured to: deepen collective understanding of the risk and threat landscape; work towards a blueprint for a resilient global supply chain; and improve transparency across supply chains.



Workshop Outcomes

Three overarching requirements for building resilience emerged:

1. The need for a common risk vocabulary across industries and throughout the private and public sectors
2. The need for better information flow with a clear distinction between credible information and subjective risk assessments
3. The need for flexibility and the ability to recover from supply chain disruptions when they cannot be prevented

“

Our economic security depends on global supply chain systems and a common global understanding of risk.

”

David Heyman, Assistant Secretary for Policy, US Department of Homeland Security

2. Revisiting the Risk Landscape



- The evolving risk landscape has brought supply chain risk to the forefront of government and industry agendas.
- Systemic risk impacts have the potential to be magnified by the way supply chain systems are configured; they cannot be mitigated by individual actors.
- Of emerging non-traditional risks, cyber risk has the greatest implications for supply chains.

An Evolving Risk Landscape

Unlike localized or company-specific risks, system-wide risks are those which significantly disrupt supply chains across multiple operations and a wide geographic area. Similar to the Forum's Global Risk Report, this report series has focused on the evolving landscape of these global systemic challenges.

Systemic risks are created or magnified by the way supply chain systems are configured. So they are not easily resolved by individual actors. In today's globalized and interconnected world, any major disruption – from a disease to a fire – has the potential to cascade through supply chains and permeate other systems. Rather than treat them all as supply chain risks this report focuses on circumstances where supply chain set-ups concentrate or amplify disruptions.

The 2008 rice crisis¹¹ and the 2009 auto manufacturer bailout are examples of broad, systemic supply chain risk events where failure was sufficiently feared to prompt drastic action. Whether the disruptions caused by the Icelandic ash cloud, Japanese tsunami or Thai floods reached this level is hotly debated. However, these events undoubtedly generated much work for supply chain managers and received plenty of media coverage.

Thailand is the world's second largest computer hard drive supplier, hence the flooding there spread fear among global computer manufacturers.¹² Analysts predicted that worldwide hard drive production would fall by as much as 30% in the final quarter of 2011; computer manufacturers reacted by scrambling to snap up existing inventories. The long-term impact is still evident in the increased cost of computer hard drives. Accenture research on dynamic operations has shown that supply chain disruptions can reduce shareholder value in affected companies by 7% (see appendix 1).¹³

These events and others have forced political and business leaders to pay attention to supply chain risk. This new focus requires an updated framework for evaluating and responding to risks. It also raises some questions: Have supply chain managers exacerbated the problem by outsourcing risks for easier day-to-day management, thereby creating hidden pools of risk concentration? Do government security efforts under- or overreact to the issues? Have they reduced flexibility to a point where global supply chain actors are less able to respond to disruptions?

Given trends such as globalization, lean processes and geographical concentration, organization risk profiles have changed without necessarily increasing or decreasing the risk. A large number of potential failure modes, combined with common sense and learning from failure, typically lead to a fairly high probability of minor failures, such as slight delays, and a very low probability of catastrophic failures (see figure 5).

Traditionally, businesses have been concerned with mitigating the impact of high-probability failures, while governments and policy-makers have been concerned with low-probability disruptions, such as extreme weather events, which can cause system-wide failures.



Risk management has to be embedded within an organization from top to bottom and has to include a consistent set of key performance indicators.



Nick Wildgoose, Global Corporate, Supply Chain Product Leader, Zurich Insurance Group

Global Risks Report – 2013 – Key Highlights

The World Economic Forum's yearly Global Risks report is developed from an annual survey of over 1,000 experts from industry, government, academia and civil society who are asked to review a landscape of 50 global risks. The top five risks highlighted in the report are:

1. Severe income disparity
2. Chronic fiscal imbalance
3. Rising greenhouse gas emissions
4. Water supply crisis
5. Mismanagement of population aging.

In 2012, the respondents rate "severe income disparity" as the risk most likely to manifest over the next 10 years, and "major systemic financial failure" as the risk having the highest impact if it were to manifest.

This year's Special Report takes the first steps towards developing a national resilience measurement with regard to global risks. It explores the use of qualitative and quantitative indicators to assess overall national resilience to global risks by looking at five national-level subsystems (economic, environmental, social, governance, infrastructure) through the lens of five metrics: recovery, response, redundancy, robustness and resourcefulness.

A pioneering effort to construct a diagnostic framework that applies the concept of "resilience" to assess national preparedness for global risks, the national resilience rating will help decision-makers think about resilience in supply chains and mitigate the impacts of systemic risks

For additional information, see the Global Risks 2012 report at: reports.weforum.org/global-risks-2012/

See also the Risk Response Network website at: www.weforum.org/community/risk-response-network

Figure 5: Simple risk profile

Source: World Economic Forum

Supply chains are configured so that they can deliver the maximum intended value even if there are several high probability operational type risks. However, in the event of a low probability high impact systemic failure, a supply chain can not only fail to deliver its intended value but may also result in losses or negative value.



But systemic risks and operational vulnerabilities are linked. Risk management must be a shared responsibility between the public and private sectors, between industries, and between functional decision-makers in companies. Recognizing that each has a different initial time perspective, incentives and expertise, cooperation becomes a greater imperative and must be facilitated by a common understanding of the issues.

Across a risk landscape that includes volcanoes, strikes, lean supply chains, counterfeiting and terrorism, lack of communication and organizational silos can be toxic. A common risk assessment framework can deepen collective knowledge of both low- and high-probability supply chain risks and helps align organizational agendas around the most important challenges to address.

Risk Landscape across Europe, North America and Asia, 2012

In 2012, the Supply Chain Risk Initiative conducted a detailed survey across Europe, North America and Asia via the World Economic Forum's Supply Chain Risk Radar. The aim was to understand how the risk landscape varied across the three regions and compared with the top five global risks from 2011. Survey respondents considered global risks and their potential to cause system-wide disruptions in global supply chains (see figure 6).

When the 2012 responses are compared to the survey conducted by the Forum in 2011, four of the top five risks remain unchanged. However, *extreme weather* emerged as a more prevalent concern with an overall ranking of number two in the top five global risks.

The emphasis on *natural disasters* and *extreme weather* is perhaps unsurprising given recent high-profile events such as the 2011 earthquake and tsunami in Japan, the 2011-2012 floods in Thailand, and Hurricane Sandy in North America in November 2012. However, it may indicate a worrying tendency to focus on the most recent problem, even among the sophisticated

contributor group. According to analysis conducted by Swiss Re, 2011 was the most costly year on record globally in terms of economic losses caused by natural disasters, totalling up to US\$ 370 billion.¹⁴

Conflict and political unrest and *terrorism* were ranked as the next areas of concern by the expert group. Examples cited included the 2011 Arab Spring and the on-going social turmoil in Europe and South Africa, which led respectively to oil price increases and labour strikes.

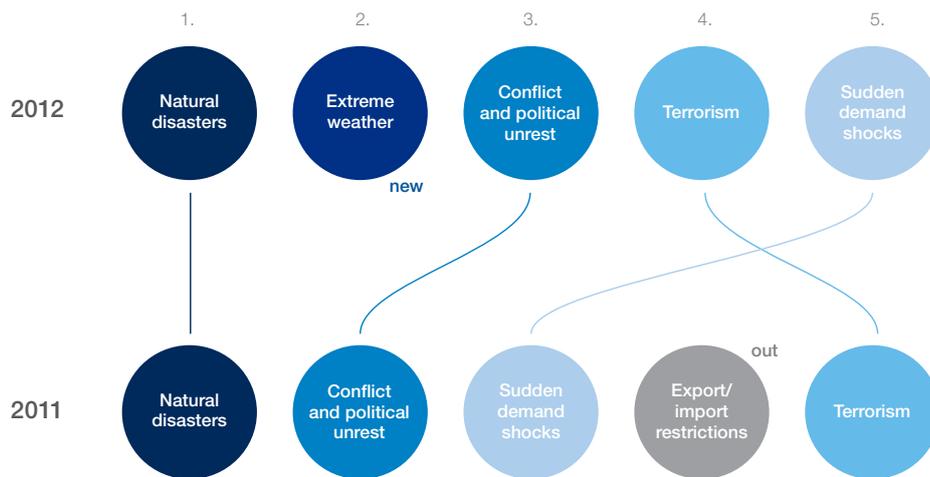
North American respondents had a notably higher level of concern about terrorism than Europeans and Asians. Unsurprisingly the policies and regulations in the region have a high degree of prescription in terms of addressing this risk of terrorism. However, this dynamic appears to be changing. In 2012, respondents indicated that security measures and supply chain systems are increasingly co-designed to facilitate rather than disrupt trade. This is reflected in the US Global Supply Chain Security Strategy which points to a broader range of risks affecting supply chains:

- Pandemic effects on border crossings and workforces
- Earthquake disruptions to mainland routes
- Bombing of major supply chain nodes
- Trade barriers to raw material and specialized products
- Cyber disruptions to supply chains

Sudden demand shocks ranked fifth globally. Examples of negative demand shocks include the decline in demand for raw materials for construction after the US housing bubble burst in 2008.¹⁵ Given events such as the 2008 financial crisis, the on-going Eurozone turmoil, and declining growth in emerging economies, economic risk and its impact on demand continue to be a top concern for decision-makers across public and private sectors.

Figure 6: Top five disruption triggers (2011-2012)

Source: Supply Chain Risk Radar survey results. World Economic Forum, 2012.



Cyber risks to global supply chains

In the World Economic Forum’s *Global Risks* report published in 2012, a survey of 469 executives and risk experts revealed emerging concern around three non-traditional risks: social contract disintegration, inflexible and uncoordinated regulation, and cyber risk.

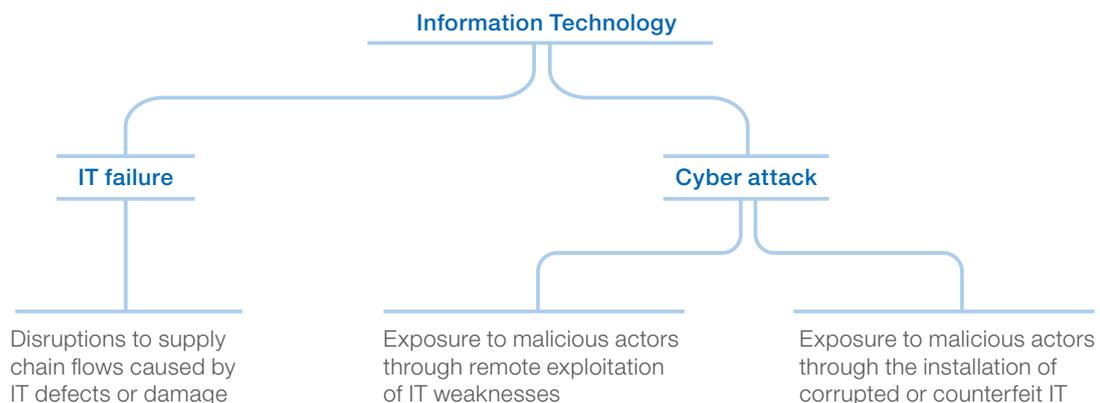
When these findings were discussed in the regional workshops hosted by the Supply Chain Risk Initiative throughout 2012, cyber risk stood out as the most pressing non-traditional risk within a supply chain context, and perhaps the only issue where a seemingly small failure could cause rapid and widespread disruption. Complexity compounds the risk even more, as information technology (IT) has enabled supply chains to evolve into interdependent material, financial and information flows. While this increases efficiency, it also exposes supply chains to cyber risk (see figure 7), which if realized in one flow, can hinder other flows and thereby result in system-wide failure.

In response, large economies such as the US and Germany have already established national cyber security divisions designed to counteract cyber-attacks.¹⁶

“
Within the last two years the world has witnessed devastating catastrophes of enormous scale, whereby global supply chains were disrupted, affecting businesses and livelihoods across the globe.
 ”

Allen Bruford, Deputy Director, Compliance and Facilitation Directorate, World Customs Organization

Figure 7: Cyber risks to global supply chains



The World Economic Forum's report on cyber resilience¹⁷ presents a Cyber Risk Framework which could be applied to supply chains to show cyber risk exposure, vulnerabilities, and the value at risk (see figure 8). Beyond accidental failures, cyber threats include hacktivism, criminal activity, governmental attacks, terrorism and corporate espionage.

Technology processes and people are the main vulnerabilities of a virtual system. Potential risks range from infrastructure damage to reputational and intellectual property impairment. These vulnerabilities and risks become even more worrying with the growing importance of non-physical supply chains to macroeconomic processes.

Example: British Telecom

In 2004, a minor short circuit hit British Telecom. The resulting IT failure caused 130,000 users' telephone, fax and internet systems to lose connectivity; 31 bank branches closed down due to stalling of data centres; automated teller machines collapsed; and emergency hotlines were inaccessible. The damage due to this minor short circuit was estimated at more than US\$ 7 million per day.¹⁸

Implications for Supply Chains

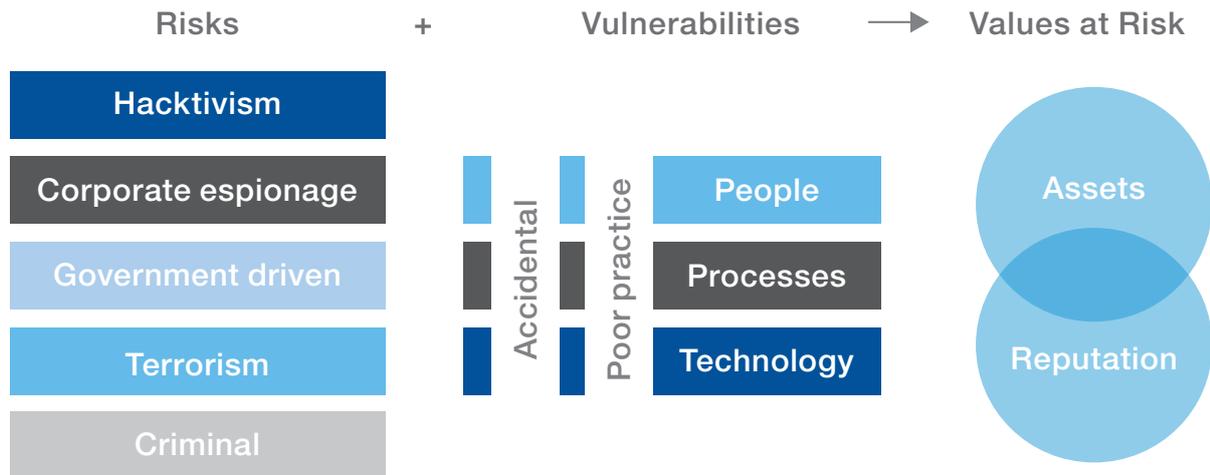
Many traditional supply chains are evolving into digital supply chains. This trend is evidenced by the double digit compounded annual growth rate (CAGR) predicted for e-book sales (30%)¹⁹ and electronic health record systems (12.6%).²⁰ At the same time, innovations such as 3D printing promise to shorten at least some linkages in the physical supply chain.

This transition poses risks to certain supply chain actors – notably logistics providers whose role could shift markedly within an evolving digital supply chain. It also introduces new cyber risks to the supply chain itself. Supply chain actors need to demonstrate they can master digital resilience to assure the upsides of digital supply chains, such as greater accessibility and faster fulfilment times.

Given the growth in non-physical supply chain flows, their inherent cyber risks must be understood and incorporated into overall resilience approaches.

Figure 8: Supply chain cyber risk vulnerabilities

Adapted from: *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience*. World Economic Forum, 2012.



3. Building Resilient Supply Chains



- Supply chain managers traditionally focus on reducing cost and increasing reward. As a result organizational standards may not be aligned with building resilience.
- C-suite executives are struggling to find a balance between managing risk and building resilience across organizations.
- Public policies can be further developed to incentivize resilience across supply chain actors.
- A blueprint for resilience offers a practical framework for joint action.

What Is Resilience?

Phase I of the World Economic Forum Supply Chain Risk Initiative focused on understanding how supply chain vulnerabilities exacerbate disruptions: for example, how reliance on oil leads to extreme volatility in commodity prices (see appendix 2). Phase II introduces the concept of a blueprint for resilience to address these vulnerabilities and respond to the broad range of potential disruptions.

Within a supply chain context, our experts suggested that resilience can be defined in a number of ways (see figure 9). However, all converge on a common theme, which is the ability of the system to return to its original state after a major disruption.

Challenges to Resilience

Despite fears that injecting resilience into the supply chain will create cost and reduce possible rewards, most experts surveyed believe that efficiency and resilience can coexist without major negative impact and ideally, should be complementary.

Yet managers still focus on reducing cost and increasing reward. It is hard to sell risk management as a competitive advantage.

Executives and corporate boards are increasingly concerned about managing a variety of risks. But ensuring that risk management priorities permeate an organization via incentive structures can be

a challenge. Elevating systemic risk management concerns as a priority for industry bodies, to find collaborative solutions, is equally difficult.

Supply chain managers primarily want to increase reliability of delivery and achievable value. Meanwhile, the public sector must reduce the impact and respond to significant disruptions. These goals may or may not be mutually supportive.

Several business innovations and trends of recent decades have succeeded in reducing higher probability, profit-sapping risks:

- Lean supply chains, by design, lay bare the causes of frequent failures, forcing organizations to learn and design reliability into their processes
- Globalization provides opportunities for diversification of supply
- Specialized production and scale accelerate learning and the ironing-out of risks
- IT-enabled visibility gives advance warning of problems and enables decentralized solutions

These advances sometimes help to manage the less likely major systemic upsets too. However, in some cases they can amplify risks. Lean supply chains can shut down in hours, and learning from past events is of little use for once-in-a-generation failures. A global supply chain affects far more people. Supply concentration and IT reliance cause havoc if critical nodes fail.

Despite these challenges, a blueprint for resilient supply chains can assist in aligning and organizing priorities to address the most problematic global supply chain risks.

Figure 9: Definitions of resilience

“Resilience is the ability of a global supply chain to **reorganize and deliver its core function** continually, despite the impact of external and or internal shocks to the system.”²¹

“[...] the ability of a system to **return** to its original [or desired] state after being disturbed.”²²

“[...] the ability to **bounce back** from large-scale disruptions.”²³

“[...] being **better positioned than competitors** to deal with – and even gain advantage from – disruptions.”²⁴

“[The] ability to **maintain output** close to potential in the aftermath of shocks.”²⁵

“Resilience is about **building capacity, through the collective and simultaneous efforts** of those in and out of government towards a shared result.”²⁶

“

More than 80% of companies are concerned about supply chain resilience.

”

Resilience Measures

As a starting point for developing a blueprint for resilient supply chains, experts across regions and sectors were asked to determine a priority rank of 11 possible measures of resilience (see appendix 3). The results were debated in workshops and discussions, including differing regional and sectoral perspectives to derive the top five joint resilience measures (see figures 10 and 11).

Key regional differences

North America and Europe identified harmonized legislative and regulatory standards as the top priority. Respondents from Asia, on the other hand, consider improved information sharing between government and business as the top priority for building supply chain resilience.

Respondents from Asia also prioritized improved alert and warning systems more than their western counterparts. Inadequate capacities to provide early alerts for earthquakes, tsunami and flooding impacting Asia in 2011 may have contributed to this prioritization.

European and North American respondents emphasize building a culture of risk management across suppliers as a top priority. This is less valued in Asia, where the growth opportunities in emerging economies elicit high risk strategies for maximum return.

Also many Asia-based supply arrangements are typically younger and more fluid, resulting in weaker lines of communication through which a culture of risk management can be established.

- For a detailed explanation and examples of each of these measures, please see appendix 4.
- For a detailed regional prioritization of these and other measures, please see appendix 5.

Public sector specific priorities

North American and European public sectors are interested in tiered classification of firms and procedures to allow preferential treatment during times of disruption. However, governments in Asia are traditionally less motivated by this: high levels of competition in the region can result in high rates of supplier substitution on the assumption that equally capable suppliers can be rapidly integrated. North American and European public sectors have placed more emphasis on retaining partnerships – hence companies are placed under more scrutiny to assess their long-term reliability.

- For an aggregated prioritization of each of these and other measures, please see appendix 6.
- For a detailed explanation and examples of each of these measures, please see appendix 7.

Private sector specific priorities

For the private sector, two priorities emerged: the use of exercises to stress-test assumptions and plans; and trade resumption plans, protocols and lines of authority to redress major concerns. These matter because of the diversity of supply chain configurations available to businesses, the criticality to their bottom line of selecting the correct one, and the need – when a disruption happens – to prevent loss of market share to more resilient or unaffected competitors. Some private sector players also fear the complexities and unintended side-effects of government action.

- For an aggregated prioritization of each of these and other measures please see appendix 8.
- For a detailed explanation and examples of each of these measures, please see appendix 9.

Figure 10: Aggregating regional and sectoral perspectives

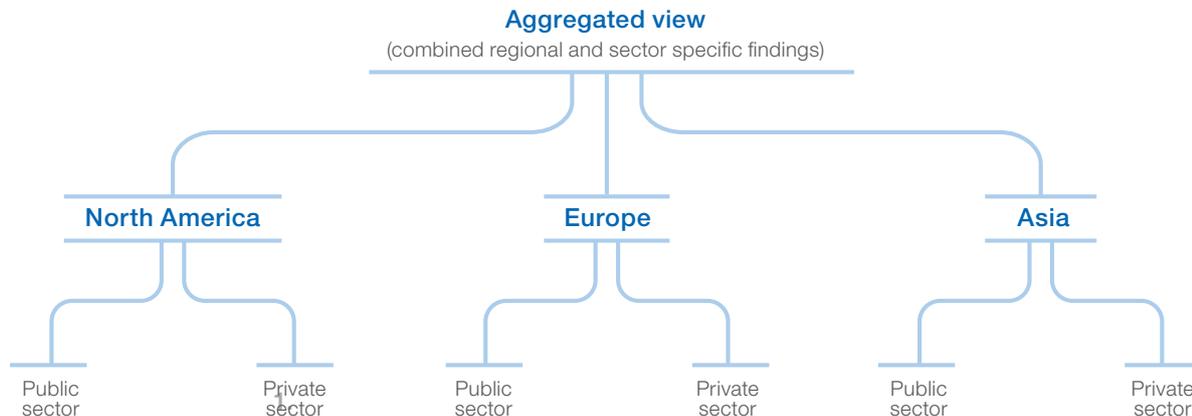


Figure 11: Top five joint resilience measures – Aggregated view

Priority	Resilience measures
1	Improved information sharing between governments and businesses
2	Harmonized legislative and regulatory standards
3	Building a culture of risk management across suppliers
4	Common risk assessment frameworks
5	Improved alert / warning systems

A Blueprint for Resilient Supply Chains

The degree of supply chain resilience is typically assessed by the extent to which value is reduced or harm is caused, and the speed with which normal operations can be restored.

At a systemic level, the concern is to what extent the regulatory and business environments enable and provide incentives for micro-level resilience measures.

The workshop series revealed a widely held view that public sector supply chain risk actors are predominantly focused on at-the-border security as a risk. And, as the resilience response, they focus predominantly on (private sector) transparency.

Too little attention is paid to the other levers by which resilience can be encouraged or enforced. For example, competition authorities could pay more attention to the availability of independent component sources much deeper in the supply chain. Currently they are seen as over-focusing on consumer facing brands.

At the other end of the chain, consumers are under-involved in setting resilience priorities. Consumer testing of tolerance levels and trade-offs is needed to update corporate and government assumptions; consumers often care more about knowing definitely when their order will be fulfilled than they do about speedy fulfilment.

The current diversity in sectoral and regional approaches to resilience itself contributes to resilience by providing multiple alternatives for testing.

Despite regional and sectoral differences, supply chain experts saw the need for an overall blueprint for resilient supply chains. The proposed blueprint contains four core components: partnerships, policy, strategy and information technology (IT). Each component comprises a number of properties (see figure 12) that map the journey towards resilience and provide a means for measuring progress along it.

Figure 12: The blueprint for resilient supply chains

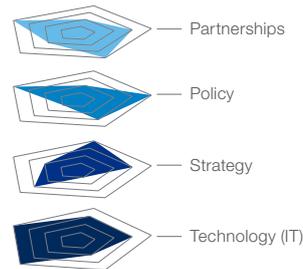
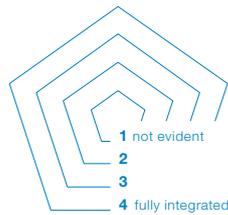
Source: World Economic Forum

Using the blueprint

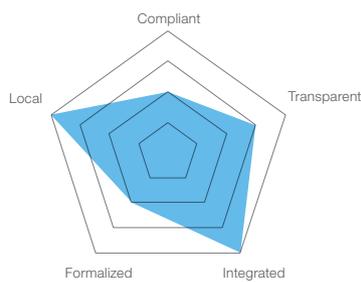
Supply chains of all forms and functions can use the blueprint to structure targeted resilience building efforts.

The lower scores towards the centre of spider charts below show, for an illustrative supply chain, that resilience building efforts should focus on building collaborative policies and agile strategies.

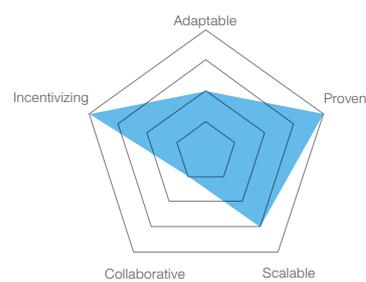
Scores represent an illustrative supply chain.



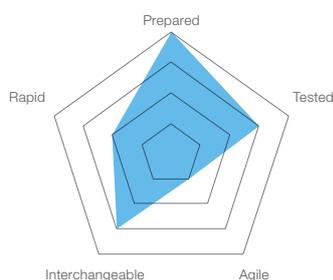
Partnerships



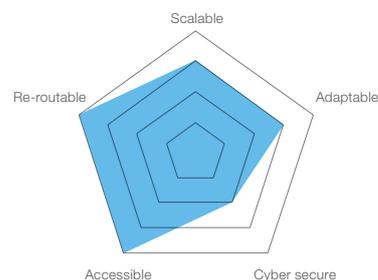
Policy



Strategy



Technology (IT)



Partnership resilience

Supply chain trends show a move away from agnostic outsourcing towards long-term partnerships. In such relationships, resilience can be built via improved security, information sharing and knowledge exchange (see examples below).

At a broader level, better knowledge of a partner can enable more targeted risk management; this is already the basis of authorized economic operator programmes developed by customs authorities worldwide (see appendix 4). Both government- and business-driven partnerships must retain open architectures with harmonized standards to allow accessibility and competition.

The World Economic Forum's Partnership Against Corruption Initiative has identified that partnerships need to be broadened to incorporate greater transparency with small- to medium-sized enterprises (SMEs) and more local actors across supply chains, especially in new and emerging markets.

The resilience benefits these partnerships provide link directly to mitigating risks of corruption and bribery. The B20 recommendations include an Anti-Corruption Action Plan.²⁷ Engaging SMEs continues to be a top priority. Various forms of partnerships are already in place between governments and business and in business to business transactions. Those such as C-TPAT, which are linked to a set of incentives for business engagement, have proven to be quite effective mechanisms for strengthening partnerships across supply chains.

Creating common security protocols

Example: C-TPAT

US C-TPAT (Customs-Trade Partnership Against Terrorism) is a voluntary initiative to strengthen and improve overall international supply chain and US border security. It enables international supply chain businesses to improve and verify the security guidelines of their business partners within the supply chain.²⁸

Engaging in collaborative logistics

Example: TradeXchange®

TradeXchange® is a multi-agency initiative led by Singapore Customs, Economic Development Board and Infocomm Development Authority of Singapore. It is a neutral platform upon which shippers and freight forwarders can seamlessly exchange information and launch collaboration efforts. Synchronizing information flows across multiple supply networks enables flexibility and rapid collective response to supply chain anomalies.²⁹

Participating in mutual learning

Example: Kyohokai Association

Established in 1943, the Kyohokai Association has grown to include 221 Toyota Motor Company suppliers. The association, which spans Toyota's tier 1 through tier 3 suppliers, regularly convenes to share opinions on supply chain issues.³⁰

“

Optimising resiliency and efficiency requires discipline, analytics, decision modelling, and the involvement of a broad cross-section of business, technology, and operation leaders both inside and outside the organisation.

”

Gary S. Lynch, Managing Director and Global Leader, Marsh Risk Consulting, Marsh

Partnership Against Corruption Initiative

Systemic risks to supply chains often focus on extreme events such as a natural catastrophe, which has been identified consistently as the number one risk in the Forum's supply chain risk assessments. However, creeping risks, such as pervasive entrenched corruption, are also of major concern. In 2012, corruption moved from 13th place to 9th in the Forum's ranking of risks affecting global supply chains.

Dealing effectively with corruption requires a multi-pronged approach that includes governments, business and civil society. As the leading global CEO voice on anti-corruption, the World Economic Forum's Partnering Against Corruption Initiative (PACI) must help its members unravel some of the complexity around these issues from a business perspective. One area that is critical is improving transparency across complex supply chains.

A lack of transparency across complex supply chains and far-flung subsidiaries is a constant challenge and one that has been identified by many companies engaged in the initiative as an area in need of improvement. Subsidiaries and external supply chain partners are often small- and medium-sized enterprises (SMEs) that may lack the resources and compliance know-how to manage risks, particularly with corruption and bribery.

There is no plausible deniability for business leaders when it comes to understanding the risks associated with their supply chains. While standards of transparency vary widely from country to country, they also remain largely outside of the control of organizations to influence on their own when it comes to working in new and emerging markets.

Transparency is a critical component in building supply chains that are resilient in the face of corruption. If, for example, business-to-business transactions can be made through agreed upon elements of an "integrity pact" and in a digital environment, then business organizations can help each other set and uphold common standards for solicitation and identify anomalies in the system much more quickly. PACI members can work together to create incentives for local SME networks to adopt measures for transparency. This creates a web of trust and that helps build resilience into complex systems, and in turn, helps businesses mitigate a range of risks and potential shocks to their operations.

For additional information, see the Partnership Against Corruption Initiative at: www.weforum.org/issues/partnering-against-corruption-initiative

Policy resilience

Regulations, almost by definition, restrict freedom of action and therefore may inadvertently reduce the flexibility required for building stronger resilience. On the other hand, governments can shape actions to benefit the public, whether through trade, security, investment or other policies that directly or indirectly affect resilience.

Governments can also foster the cooperation and marshal the resources needed for major responses. Experts agree that governments should aim for maximum flexibility during times of disruption while providing incentives for resilient behaviour during times of stability. A government's ability to intervene *in extremis* should be calibrated to avoid rewarding poor risk preparation or too-big-to-fail supply chain developments. Governments also often act as information brokers; and administrations that are able to provide strong information flow are viewed as real guardians of resilience.

The strength and redundancy of infrastructure is typically a strong component of resilience, and extra capacity is usually hard to add quickly. So governments have a responsibility to encourage the development of alternatives to potential choke points. In combating security threats, good policy means consulting supply chain practitioners about how best to minimize knock-on disruptions.

Example: Singapore

Singapore is increasingly viewed as a logistics hub of choice within Asia owing to its trade-friendly political structures. In 2011, the World Bank listed Singapore as the leader in supply chain performance, with punctuality being a key strength.³¹ Three factors that distinguish Singapore as the Asian hub of choice stem from the country's dynamic and collaborative approach to trade policy:

- 1. Accommodating the dynamics of global trade** - Singapore Customs developed five strategies under its Customs 2015 outlook. These strategies explore the ways in which Singapore Customs could respond to environmental drivers and will continually be adapted to respond to new developments.
- 2. Cross-border collaborative efforts** - Singapore Customs has signed mutual recognition arrangements with Canada, China, Japan and Korea to strengthen the global supply chain and facilitate legitimate trade.
- 3. Quick responses to external shocks** - Singapore has been actively involved in developing international supply chain standards, such as the World Customs Organization Trade Recovery Guidelines and the Asia-Pacific Economic Cooperation area's Trade Recovery Programme.

On 11 April 2012, US Secretary of Homeland Security Janet Napolitano and Singapore's Deputy Prime Minister Teo Chee Hean signed a joint statement reaffirming the commitment of both countries to strengthening global supply chains to ensure they operate effectively in times of crisis, recover quickly from disruptions, and facilitate international trade and travel.

Enabling Trade: Valuing Growth Opportunities

Tariffs are no longer the main deterrent to international trade. As supply chains become global and tariffs come down overall, several other aspects along the supply chain provide greater friction to companies and countries in their goal of promoting trade and economic growth. This broader view of supply chain barriers to trade, based on the World Economic Forum's Global Enabling Trade Report, focuses on market access, border administration, transport and telecommunications infrastructure, and business environment.

Analysis of trade barriers suggests that addressing supply chain barriers has a larger effect than carrying out simple tariff liberalization. A reduction in supply chain barriers creates income gains multiple times larger than tariff elimination as the former eliminates wasted resources, whereas the latter reallocates resources within the economy with a more moderate reduction in deadweight loss.

Studies show that incremental reductions in barriers to trade may have no impact unless they are combined with a series of other improvements. This is because company decisions are binary – to trade or not to trade within a specific country – depending on the conditions faced. The basic investment thesis will vary by industry, so a proper understanding of an industry's supply chain is paramount when driving public policy.

Governments must address trade barriers in a structured and coherent manner. They need to understand their comparative advantage, decide where they want to go and develop a specific strategy to remove the relevant set of barriers. Conversely, companies must learn to better assess supply chain risks by taking into account all possible cost effects of the four basic supply chain barriers. When making decisions on which markets to produce and sell in, companies should recognize that costs and risk associated with supply chain barriers may offset more obvious savings, such as lower labour costs.

In the past, international trade negotiations have focused on a "silo-approach" in which issue areas are addressed in isolation. However, addressing global supply chain barriers requires a more holistic approach that spans a variety of sectors and subsectors that are relevant for trade logistics. Such a "whole of the supply chain" approach is suitable for both multilateral and regional agreements.

For additional information, see the Global Enabling Trade Report 2012 at: www.weforum.org/reports/global-enabling-trade-report-2012

Strategic resilience

Supply chains established during more stable times need to be reshaped for operation in an era of increased volatility. Although a number of strategies can be applied to enable this (see figure 13) it is the capacity to adapt, rather than the actual strategy, that will drive resilience.

Accenture's point of view on dynamic operations³² highlights certain organizational capabilities that can make supply chains more resilient to potential disruptions:

- Supply chain operators should be able to synthesize external and internal data and rapidly take action to minimize the impact of a disruption
- Supply chain structures should be adaptable and agile so that they can quickly adjust and respond to the market and economic conditions

In an interconnected economy, embedding these capabilities can also enable better responses to public sector challenges. Therefore, government authorities can adopt private sector approaches for building resilience within their supply chains.

Whilst incorporating these strategies may require a significant structural and cultural shift, both corporate boards and government authorities need to embed these capabilities in their supply chains.

Information technology resilience

The application of IT within supply chains has increased dramatically. Configured correctly, IT can provide significant resilience gains through four main channels: analytics, data and information sharing, scenario modelling, and pre-programmed responses.³³

The cornerstone of IT-based resilience is data and information sharing. Business continuity is enabled through access to real-time data, followed by rapid dissemination of data-driven supply chain fixes. However, information sharing infrastructures depend on a resilient core network, appropriate communication tools, and an element of redundancy.³⁴ This requires IT systems that are scalable, secure and re-routable.

An example of IT-enabled resilience can be seen at aircraft manufacturer Boeing. To address supply chain issues that delayed production of the 787 by three years (resulting in 217 cancelled orders and an estimated US\$ 6 billion in lost profits)³⁵ the company has engaged suppliers such as Alcoa in a collaborative planning, forecasting and replenishment (CPFR) exercise.

In CPFR, IT systems are integrated to allow real-time data exchanges between supplier and manufacturer. Boeing now sends weekly forecasts and inventory counts to Alcoa via enterprise resource planning systems that generate electronic purchase orders for raw materials.³⁶ The improved forecasting accuracy enables Alcoa to adjust its production processes for maximum efficiency, while the enhanced communication ensures this part of Boeing's supply chain is not disrupted.

Figure 13. Example strategies for success in a dynamic risk landscape

Example strategy	Benefits
Diversity of activities, suppliers and markets	<ul style="list-style-type: none"> – Avoidance of over specialization or dependence – Encouragement of internationalization and variety
Transparent organizational structures	<ul style="list-style-type: none"> – Clear corporate structure – Coordinated departments with clear responsibilities
Shared strategic stocks/supply agreements	<ul style="list-style-type: none"> – Prearrangement of access to critical stocks such as emergency fuel, medical supplies, etc.

“

Volatility is the new normal in supply chain and logistics. We need to be more dynamic, more savvy and more informed than ever before to optimize and mitigate risk.

”

Jonathan Wright, Managing Director, APAC Management Consulting-Comms, Media and Technology Sector



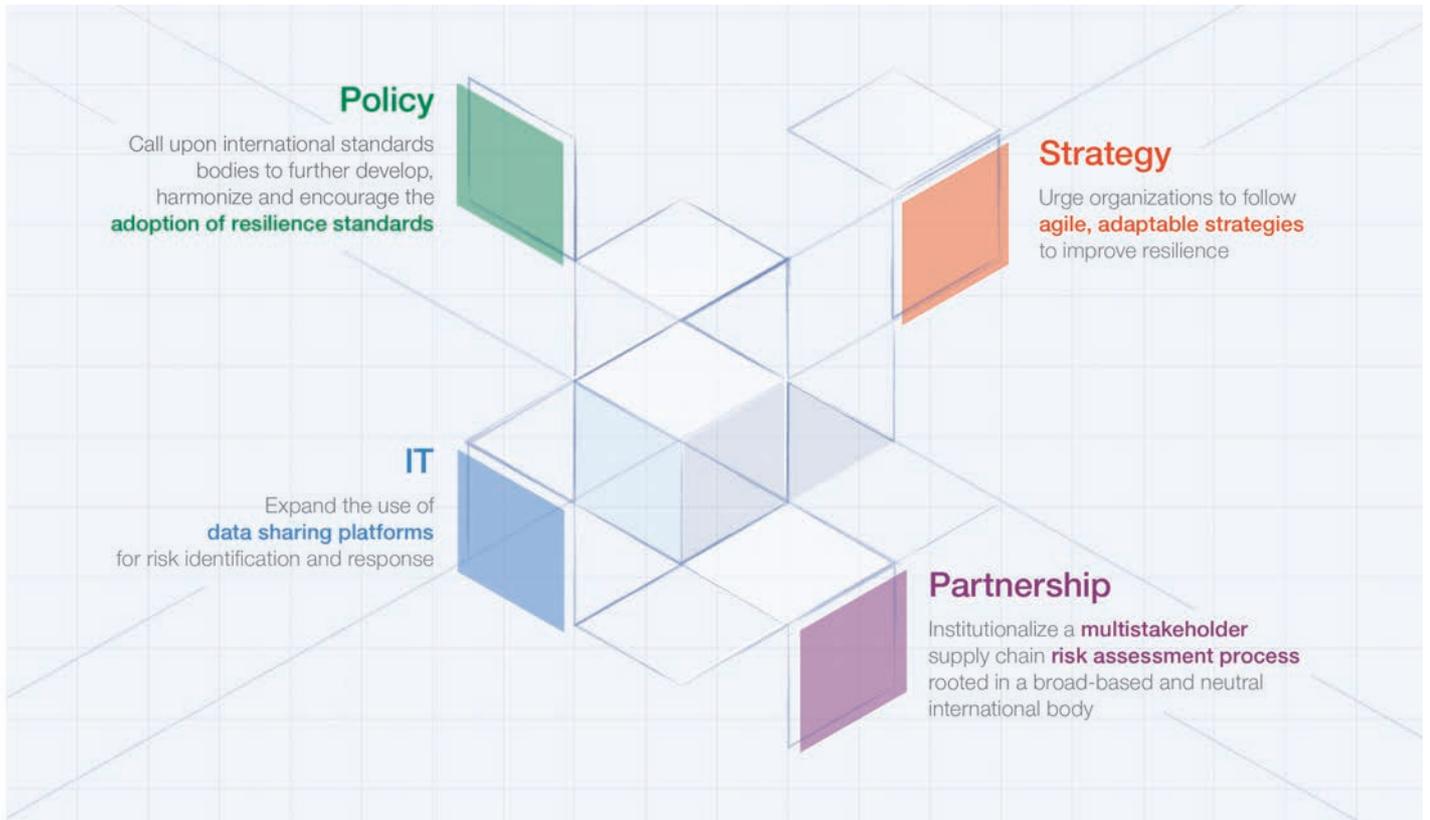
4. Recommendations



This report offers four recommendations that consolidate the project findings into actions for building resilient supply chains. These actions prioritize a range of resilience measures around four core areas; and they recognise the need for a common risk vocabulary, better information flow between parties, and increased supply chain flexibility.

A risk management framework and a blueprint for resilient supply chains work well together when the most important potential risks are first identified, and then mitigation measures are developed for application across a range of global risks.

Collaboration is critical, though primary responsibility for initiation can be assigned to the public or private sector. In either case, strong collective engagement is essential in a network of supply chain actors who share a long-term commitment to protecting and enhancing the backbone of a shared global trading system.



Workshop Participants

World Economic Forum

Karen Campbell, Senior Economist, Risk Response Network, World Economic Forum USA

Matthew A. Miller, Associate Director, Middle East, Global Leadership Fellow, World Economic Forum

Thea Chiesa, Director, Head of Aviation, Travel and Tourism Industries, World Economic Forum

Accenture

Ameer Ali, Senior Manager, Health and Public Services, Supply Chain and Operations, Accenture

Ronald Ash, Senior Executive, Health and Public Services, Accenture

Steven De Bruyn, Senior Manager, Accenture

Agnes Chan, Manager, Communications and Media, Accenture

Olivier Gillerot, Senior Executive, Accenture

Nicholas To, Senior Manager, Accenture Hong Kong

Jonathan Wright, Managing Director, APAC Management Consulting-Comms, Media and Technology Sector, Accenture

Other participants

Stephen Alterman, President, Cargo Airline Association

Jean-François Arvis, Senior Economist, The World Bank

J. Michael Barrett, Principal, Diligent Innovations

Akhmad Bayhaqi, Policy Analyst, APEC Secretariat (Asia-Pacific Economic Cooperation)

Lilian Bertin, Head of Sector, United States and Canada, DG for Taxation and Customs Union, European Commission

David N. Blackorby, Vice-President, Global Sourcing, Asset Protection and Security, Wal-Mart Stores

Alexandra Brintrup, Supply Chain Resilience Expert, University of Cranfield

John P. Brown, President and Chief Executive Officer, Lineage Technologies

Christa Brozowski, Director, Global Supply Chain Security, Office of the President of the United States

Allen Bruford, Deputy Director, Compliance and Facilitation Directorate, World Customs Organization (WCO)

Dylan Brynat, Regional Head, IPZ Sales and Distribution, Asia-Pacific, Zurich Insurance Group

Ralf Busche, Vice-President, Supply Chain, Asia-Pacific, BASF East Asia Regional Headquarters

Greg Carnevale, Deputy Branch Chief, US Department of Homeland Security

Ralph Carter, Managing Director, Trade and International Affairs, Fedex Express

Didier Chenneveau, President, Asia-Pacific, CEVA Logistics Singapore

Chuaa Hui-Hui, Senior Trade Officer, Trade Strategy and Security Branch, Singapore Customs

David Cockroft, General Secretary, International Transport Workers' Federation

Kenneth Dunlap, Director for Security and Travel Facilitation, International Air Transport Association (IATA)

Michael Durst, Chief Executive Officer, ITONICS

Andrew Farrelly, Director, Targeting Programs, US Customs and Border Protection, US Department of Homeland Security

Matthew H. Fleming, Adjunct Professor, Georgetown Public Policy Institute

Matt Fuchs, Deputy Director of Resilience Policy, Office of Policy Development, Infrastructure Design Working Group, US Department of Homeland Security

Monette Galello, Vice-President, Risk Management, C&S Wholesale Grocers

Jos Giele, Director, Corporate Security, Con-way

Mark Goh, Professor, NUS Business School

Glen Goldbach, Director, PwC Advisory Service, Strategy and Operations Supply Chain, PwC

Peter Graham, Associate Partner and Global Leader, Border Security and Immigration, IBM Business Consulting Services

Florian Greif, Chief Operating Officer, ITONICS

Marcus Hallside, Chief Executive Officer, Innovative Compliance Europe

Frank Heijmann, Head, Trade Relations Customs Administration of the Netherlands

David Hesketh, Senior Business Manager, HM Revenue & Customs

David Heyman, Assistant Secretary for Policy, US Department of Homeland Security

Jose Holguin-Veras, Professor and Acting Department Head, Center for Infrastructure, Transportation and the Environment, Rensselaer Polytechnic Institute (RPI)

Julia K. Hughes, President, USA-ITA

Dana W. Hullinger, Director, Supply Chain Strategy and Early Supplier Involvement, Supplier Management, The Boeing Company

Miguel Jaller Martelo, Research Associate, Center for Infrastructure, Transportation and the Environment, Rensselaer Polytechnic Institute (RPI)

Erik Jensen, Vice-President, Corporate Supply Chain Security Manager, Corporate Key Accounts, Panalpina

Mike Kangior, Office of Policy, US Department of Homeland Security

Anders Karlborg, Vice-President, Supply Chain, Huawei Technologies Co.

Henry Kenchington, Deputy Assistant Secretary for Research and Development, US Department of Energy

Tatum King, Attaché, ICE Homeland Security Investigations (HSI)

Lars Kjaer, Senior Vice-President, World Shipping Council

Bob Knetl, Director, Washington Operations, Georgia Tech Research Institute

Roger M. Kubarych, National Intelligence Manager and Officer, ODNI and NIC, National Intelligence Council (NIC)

Michael Kwan, Deputy Head, Office of Supply Chain Security Management, Customs and Excise Department

Brett Laduzinsky, CBP-Office of the Commissioner, US Department of Homeland Security

Debbie Lang, Vice-President, International Supply Chain, Best Buy Co.

Ian Lee, Senior Vice-President, Group Strategy, PSA International

Sylvain Levesque, Vice-President, Corporate Strategy, Bombardier

Karen Lim, Head, Trade Strategy and Security, Singapore Customs

Thomas Lin, Head, Office of Supply Chain Security Management, Hong Kong Special Administrative Region

Geoffrey Lipman, President, International Council of Tourism Partners

Ken Lord, Policy/Plans Specialist, US Department of Transportation

Patrick Low, Chief Economist; Director, Economic Research and Statistics, World Trade Organization (WTO)

Gary S. Lynch, Managing Director and Global Leader, Marsh Risk Consulting, Marsh

Vince McCarthy, Senior Vice-President, Corporate Development and Strategy, Verisk Analytics

Ellen McClain, Deputy Assistant Secretary, Trans-Border Policy, US Department of Homeland Security

Tom McDermott, Research Director, Georgia Tech Research Institute

John McGowan, Senior Vice-President, Border Security, Sandler & Travis Trade Advisory Services

John Manners-Bell, Editor and Chief Executive Officer, Transport Intelligence

Ingo Marowsky, Coordinator, Organising Globally, International Transport Workers' Federation

Jock Menzies, President, Terminal Corporation

Victor Meyer, Managing Director; Global Head, Business Continuity Management, Deutsche Bank

Robert Missen, Head, Unit C-3, Maritime and Land Transport Security, European Commission

Sean K. Moon, Acting Director, Transportation and Cargo Policy Development, US Department of Homeland Security

Alexander N.M. Niejelow, Chief of Staff, U.S. Intellectual Property Enforcement Coordinator, Office of the President of the United States

Kirstjen Nielsen, President, Homeland and National Security Solutions, Civitas Group

Radoslaw Olszewski, Administrator, Counterterrorism, European Commission

Debra van Opstal, Executive Director, US Resilience Project

Philip J. Palin, Coordinator, RCPGP Mid-Atlantic Supply Chain Resilience Project

Martin Palmer, Director, Export Controls, TNT Express

Leslie J. Parish, Chief, Sharing Branch, National Maritime Intelligence-Integration Office

Mariya Polner, Research Analyst, World Customs Organization (WCO)

Nick Rhodes, Director, Cargo, Cathay Pacific Airways

James B. Rice Jr., Deputy Director, MIT - Center for Transportation and Logistics

Martin D. Rojas, Executive Director, American Trucking Associations

Ella-May Seth, Deputy National Intelligence Officer for Economic Issues, National Intelligence Council (NIC)

Yossi Sheffi, Professor of Engineering Systems; Director, Transportation and Logistics, Massachusetts Institute of Technology

Steven Solomon, Associate Director, Global Operations and Policy, US Food and Drug Administration

Maranda Sorrells, Policy Adviser, US Department of Homeland Security

Jagjit Singh Srail, Head, Centre for International Manufacturing, Institute for Manufacturing, University of Cambridge

Bo-Inge Stensson, Senior Vice-President, Group Purchasing, SKF

Seth Stodder, President and Chief Executive Officer, Palindrome Strategies

Julie Szegda, Analyst, National Targeting Center, US Customs and Border Protection

Lotte Taylor, Member of Cabinet, European Commission

Pyers Tucker, Global Head, Strategy, Damco International

Constantine Vassiliadis, Principal Manager, PwC

Alyson C. Warhurst, Chief Executive Officer and Founder, Maplecroft

Andrew S. Weinberg, Chairman, Strategy, Brightstar Corp.

Robert E. White, Attaché, US Customs and Border Protection

Nick Wildgoose, Global Corporate Leader, Supply Chain Product, Zurich Insurance Group

Henry H. Willis, Associate Director, RAND Homeland Security and Defense Center, RAND Corporation

Zhu Gaozhang, Director, Enforcement and Facilitation, World Customs Organization (WCO)

World Economic Forum - Supply Chain Risk Workshops



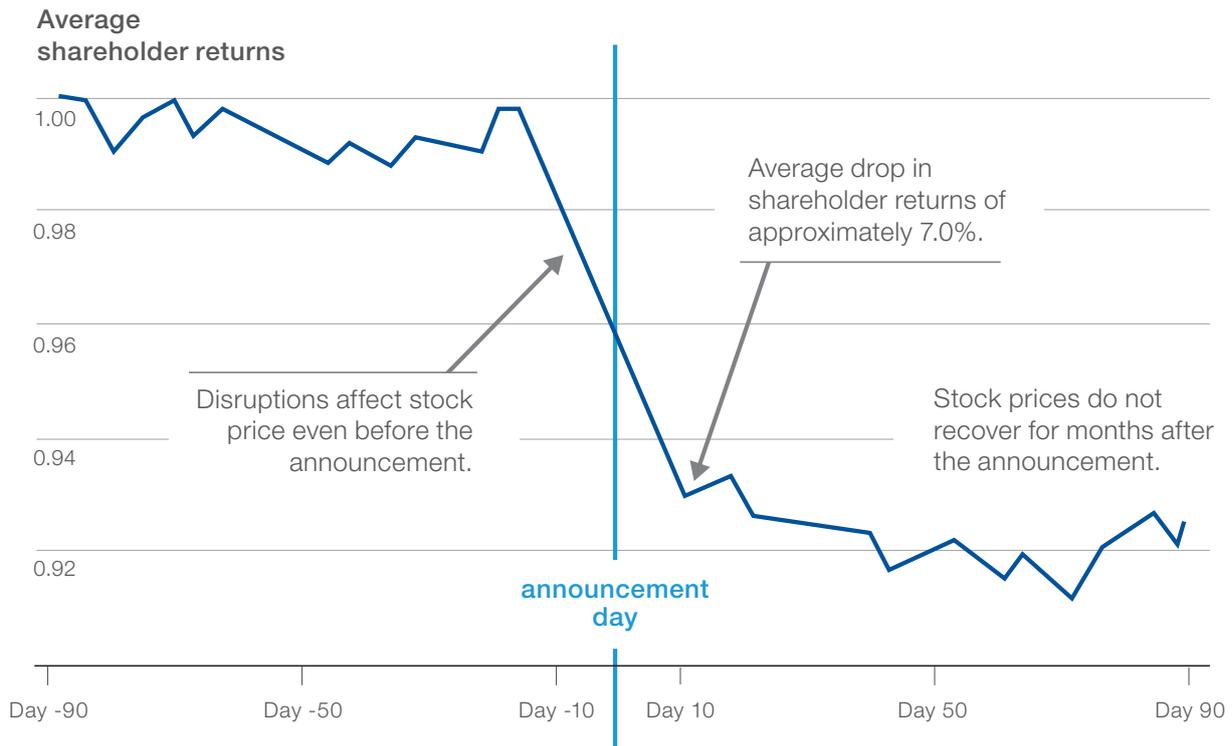


Appendices



1. The Impact of Supply Chain Disruptions on Shareholder Value

Findings



On average, supply chain disruptions can reduce shareholder value by 7%.

Highlights and Methodology

- Using **supply chain disruptions** as an indication of supply chain ineffectiveness, Accenture's research shows that **they destroy about 7% of a firm's shareholder value**
- The shareholder value starts to dip a few days before the actual announcement date as a result of information dissipation, communication and speculations
- The longer it takes to resolve the disruption, the more negative is its impact. Firms need to develop the ability to quickly resolve the problem and prevent escalation and worsening of the situation
- The evidence presented in this study makes an important economic case for embracing 'Dynamic Operations' to mitigate losses and protect shareholder value
- The evidence presented in this study is based on an analysis of 62 supply chain disruptions that were publicly announced during 2005-2011
- These announcements appeared in the financial journals and/or the sources mentioned below and were about publicly traded companies that experienced production issues, shortage of parts, supply chain issues due to natural disasters etc.
- Some of the resources used for the data collection, apart from company websites, include Bloomberg, Business Week, Forbes, Wall Street Journal and Supply Chain Digest
- Examples of such announcements are:
 - 'Japan Earthquake May Cause Prius Shortage'
 - 'Nissan to Suspend Domestic Lines because of a delay by supplier Hitachi Ltd. in delivering auto-engine components.'
 - 'Vestas Shares Fall 20 Percent Following Production Delay Warning'

2. Top Five Vulnerabilities Identified in Phase I

The figure below shows the top five vulnerabilities identified in expert surveys during Phase I of the Supply Chain Risk Initiative. Phase II has focused on building resilient supply chains to address these and other vulnerabilities.



3. Measures of Resilience

The table below captures 11 measures of resilience identified by the World Economic Forum. Participants in workshops were asked to rank the importance of each of these based on circumstances within their specific sector and region.

Measures of resilience
Harmonized legislative and regulatory standards
Improved information sharing between governments and businesses
Crisis communications integrated across supply lines
Building a culture of risk management across suppliers
Redundancy across critical functions and supply lines
Improved alert/warning systems
Common risk assessment frameworks
Trade resumption plans, protocols and lines of authority for redress of major concerns
Use of exercises to “stress test” assumptions and plans
Identification and elimination of supply chain bottlenecks and other nodes in the aftermath of an adverse event
Tiered classification of firms and their relevant procedures to allow for possible preferential treatment following an adverse event

4. Joint Resilience Measures

This appendix provides a context, description and example for the top five joint resilience measures. For analysis of the measures specific to the public and private sector, see appendices 6 through 9.

Improved data and information sharing

Accessing and contributing to available data streams can advance supply chain resilience profoundly. Government and businesses must access and apply data wisely, and also consider making data available for overall systemic benefit. This measure is receiving growing support, with officials such as the US Chief Technology Officer pursuing initiatives that “liberate” government data and voluntarily contributed corporate data to create business value.³⁷

Organizations committed to improving data and information sharing for supply chain resilience can find guidance in approaches such as the National Oceanic and Atmospheric Association’s (NOAA) weather products and the Carbon Disclosure Project (CDP).

Example: Accessing data NOAA weather products

What is it?	What are the benefits?
NOAA works with various groups as a data provider and research partner to examine the effects of weather on supply chains. Products such as the Severe Weather Data Inventory provide invaluable data to risk modellers. ³⁸	<ul style="list-style-type: none"> – Access to pertinent climate and weather data – Advanced understanding of local to regional weather risk exposure – Enhanced decision-making capabilities

Example: Contributing data – CDP supply chain

What is it?	What are the benefits?
The CDP collates data submitted by corporate entities to understand an organization’s carbon footprint and the climate change risks and opportunities across its supply chains. The information gathered is used to drive action in over 50 of the largest organizations worldwide, such as Dell. ³⁹	<ul style="list-style-type: none"> – Informing robust climate change strategies – Improving long-term risk and opportunity management – Gaining access to CDP support and tools – Collaborating with peers and a global independent non-governmental organization to share best practice and reduce supplier fatigue

A key benefit of improved data and information sharing is combining the specificity of business data with the public sector capability to scale its application for systemic benefit. The effectiveness of public-private data sharing can be demonstrated with examples such as the CASSANDRA (common assessment and analysis of risk in global supply chains) project in the European Union. CASSANDRA aims to make container security more efficient and effective by consolidating disparate corporate data capture systems into one pragmatic risk data base. This improves supply chain visibility, increases the speed of cross-border transactions in the EU, and provides a collective opportunity to enhance resilience.

Harmonized legislation and regulatory frameworks

Multilateral approaches to global challenges have succeeded in kick-starting collective action at scale in the past. For example, the Montreal Protocol led to a 96% reduction in CFC emissions within 20 years.⁴⁰ Uniform legislation could be equally effective within a supply chain context; voluntary cooperation programmes, such as the World Customs Organization’s (WCO) Program Global Shield, are already leading the way.

Example: Global Shield Programme

What is it?	What are the benefits?
Launched in 2011, Global Shield is an unprecedented international effort to counter the smuggling of chemical precursors that could be used by terrorists to manufacture explosive devices. More than 70 countries participate. ⁴¹	<ul style="list-style-type: none"> – 22 seizures of explosive precursors – Over 33,000 kilogrammes of chemicals seized – 18 arrests reported by participating countries

Under circumstances where legislation and regulation are not in place or lack enforcement, public and private sector entities can collaborate to drive new system-wide standards. This approach is common for supply chain sustainability, where cross-sector roundtables certify supply chains on compliance with agreed standards. It is also gaining traction within supply chain security. For example, the WCO SAFE Framework of Standards to Secure and Facilitate Global Trade⁴² is a non-binding set of standards serving as a common framework. Many countries have used it to develop authorized economic operator (AEO) programmes. Some AEO programmes (e.g. in the EU, Japan and Mexico) are embedded in national legislation and are part of the national regulatory framework.⁴³

Example: EU AEO Programme

What is it?

EU AEO is a partnership programme with the private sector that enables the sharing of customs security responsibilities in return for a number of mutual benefits.

EU AEO is a single and uniform import/export programme covering all supply chain operators in the 27 EU member states. Any economic operator can apply to join the programme; if the criteria are met, the operator will receive AEO status.

What are the benefits?

- Lower risk that goods flowing into and out of the EU will be stopped for examination
- Reduced data required in summary declarations
- Easier access to authorizations and permits for customs simplifications
- A specially appointed customs support officer
- Priority treatment
- Improved security and communication between supply chain partners

Building a culture of risk management

Executives recognize the need for resilience, but awareness is not filtering down to supply chain managers. This disconnect is partly due to performance-based incentive approaches which increase risk appetites. To remedy this, actions must be taken to embed risk management values across supply chain personnel, such as:

- **Define appropriate metrics**, communicate them and integrate them with employee objectives
- **Tie expectations to compensation**, to ensure proper focus on risk issues
- Creating a risk management culture – through realigned incentives, employee empowerment and demonstration of core resilience values – will support overall resilience efforts.⁴⁴

Common risk assessment frameworks

Over time, supply chain risk frameworks have come to rely on a combination of methodologies which have limited integration. They provide incompatible data and often require manual bridging.⁴⁵ The effects are limited visibility, delayed decision-making and reduced flexibility and scalability.

Supply chain experts engaged by the World Economic Forum agree that, as supply chains continue to evolve into tiered integrated networks, disparate risk frameworks must converge on common risk parameters and assessments. Examples of scalable risk assessment frameworks include the US Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

Example: Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

What is it?

HITRAC is the US Department of Homeland Security's risk intelligence centre. It employs analysts from various risk departments to "create actionable risk-informed analysis for federal, state, local, tribal, territorial, private sector, and international partners."⁴⁶

It is mainly focused on providing a common understating of regional, critical infrastructure, cyber and explosives threats. It conveys its findings through reports, conferences, teleconferences and special briefings.

It also provides an annual report for critical infrastructure and key resource sectors. The report identifies the highest relative risks including man-made and natural hazards, and the sectors most exposed to them.

What are the benefits?

- Three key benefits:
 1. Informs constituents of physical and cyber threats against the nation's critical infrastructure and all levels of government and critical infrastructure sectors
 2. Supports constituents' threat-mitigation strategies and investment decisions
 3. Educates constituents on adversary tactics and use of weapons and explosives⁴⁷
- Also releases an annual risk mitigation plan that "provides a baseline framework that informs the flexible and tailored development, implementation, and updating of sector specific plans"⁴⁸

Improved alert and warning systems

Supply chain risks manifest themselves at the systems level, but their triggers tend to have detectable epicentres at the operational scale, e.g. a significant drop in supplier production quality. The abundant and accessible operational data can be better analysed to not only detect distress signals but also envisage the wider implications of disruption, enabling supply chain managers to coordinate a pre-emptive response. The tools required are already available, e.g. SAPInfonet.

Example: SAPInfonet

What is it?	What are the benefits?
<p>SAPInfonet is a system that crowd-sources supplier information from over 13,000 sources to:⁴⁹</p> <ul style="list-style-type: none"> – Trigger alerts based on user-defined risk thresholds – Understand the impact of negative events affecting n-tier suppliers – Predict future performance and proactively manage alternative supply continuity 	<ul style="list-style-type: none"> – Access to trusted global content – Exploring risks in multi-tier supply chains – Anticipating the future behaviour of suppliers: <ul style="list-style-type: none"> – E.g. “A 75% likelihood of an increased supplier lead time (from 21 to 45 days) within the next 3 months”⁵⁰

Government supply chains were criticized recently for allowing a “hunger gap” to open during the East African Food Crisis⁵¹ – despite a call to action from the Famine Early Warning System Network one year in advance. This highlights the need not only for improved alert systems, but also their acknowledgement and incorporation into system-wide responses.

Supply chains can apply existing successful approaches to address this need. An existing example is the US Department of Food and Drug Administration’s Drug Shortages Index, which calls upon government authority to provide notification of potential shortages from drug manufacturers.

Example: Drug shortages index

What is it?	What are the benefits?
<p>On its website, the US Food and Drug Administration publishes information provided voluntarily by manufacturers about drug shortages caused by manufacturing and quality problems, delays or discontinuations. It also works with firms that manufacture the same drug, and can request increased production in order to prevent or reduce the impact of a shortage.⁵²</p>	<ul style="list-style-type: none"> – Advance warning of drug shortages – Ability to source alternative supplies – Public awareness and self-enabled resilience

5. Top Five Joint Resilience Measures – Regional View

The table below shows the regional prioritization of resilience measures. While there is significant variation by region, the top three priorities are the same across all regions.

Priority	North America	Europe	Asia
1	Harmonized legislative and regulatory standards	Harmonized legislative and regulatory standards	Improved information sharing between governments and businesses
2	Improved information sharing between governments and businesses	Improved information sharing between governments and businesses	Building a culture of risk management across suppliers
3	Building a culture of risk management across suppliers	Building a culture of risk management across suppliers	Harmonized legislative and regulatory standards
4	Trade resumption plans, protocols and lines of authority	Use of exercises to “stress test” assumptions and plans	Improved alert / warning systems
5	Common risk assessment frameworks	Common risk assessment frameworks	Common risk assessment frameworks

6. Top Five Public Sector Resilience Measures – Aggregated View

Priority	Resilience measure
1	Harmonized legislative and regulatory standards
2	Trade resumption plans, protocols and lines of authority for redress of major concerns
3	Tiered classification of firms and their relevant procedures to allow for possible preferential treatment following an adverse event
4	Building a culture of risk management across suppliers
5	Improved information sharing between governments and businesses

Text = variance from joint measures

7. Public Sector Specific Resilience Measures

Trade resumption plans

While day-to-day operation of the public sector supply chain can be delegated, responsibility for its failure cannot.⁵³ In the aftermath of a disruption it is often the public sector that must provide health and emergency supplies, or control transportation systems. Failure to supply these basic necessities can cause formidable human cost.⁵⁴ It is therefore imperative that the public sector embed rapidly deployable and scalable trade resumption plans. An example of a proactive public sector approach can be seen in the UK Civil Contingencies Secretariat’s Business Continuity Management Toolkit, which helps organizations “identify those parts of your organization that you can’t afford to lose – such as information, stock, premises, staff – and plan how to maintain these, if an incident occurs”.⁵⁵

Tiered classification of firms

A more diligent, classification-based approach to commissioning supply chain partners and providers can enhance resilience within public sector supply chains.⁵⁶ Two fundamental steps in supply chain classification are: ensuring candidates are compliant with standards such as ISO 31000 (a set of sector, function and risk agnostic guidelines and principles for implementing risk management across industries and regions⁵⁷); and accessing consistent feedback on supplier criteria such as service quality, financial health and legal incidents through sources such as the Business Identification Number Cross-Reference System (BINCS).

Example: Business Identification Number Cross-Reference System

What is it?

BINCS is a search engine for businesses and suppliers supporting the US federal supply chain. When combined with other information gathered pre-solicitation, BINCS data can indicate a type and likelihood of risk (such as subversive foreign interests) prevalent within certain supply chain entities.⁵⁸

What are the benefits?

- Indicates likelihood that a particular risk is prevalent in a specific industry
- Precludes high-risk suppliers from tendering process

8. Top Five Private Sector Resilience Measures – Aggregated View

Priority	Resilience measure
1	Improved information sharing between governments and businesses
2	Common risk assessment frameworks
3	Use of exercises to “stress test” assumptions and plans
4	Harmonized legislative and regulatory standards
5	Trade resumption plans, protocols and lines of authority for redress of major concerns

Text = variance from joint measures

9. Private Sector Specific Resilience Measures

Use of exercises to stress test assumptions and plans

Given the diversity of supply chain configurations available to businesses, and the criticality of selecting the correct one for their bottom line, the vulnerabilities of viable options must be understood prior to selection. Modelling the behaviour of supply chains under stress can provide this understanding. Accenture's latest thinking on scenario-based enterprise performance management recommends seven steps for completing the modelling process (see figure 14).

Figure 14: Scenario-based enterprise performance management

Adapted from: *Managing the Unthinkable: Scenario-Based Enterprise Performance Management*. Accenture, 2012.

Step	Action
1	Identify key factors that can have a material impact on the organization; e.g. for airlines oil prices; for global manufacturing companies exchange rates and freight costs
2	Define relevant scenarios that describe a range of future operating environments; e.g. What if oil prices average US\$ 75 a barrel, US\$ 110 a barrel or US\$ 140 a barrel?
3	Agree on a baseline scenario that will be used to develop/review strategy, set targets and develop operational plans and budgets
4	Develop strategic plans, targets, action plans and budgets using the baseline scenario
5	Develop alternative views of targets, plans and budgets under each scenario. Identify the major impacts and changes under each scenario, e.g. What will be the positive/negative impact on key financial metrics under each scenario?
6	Identify relevant triggers and corresponding tolerance ranges for each scenario that should be monitored on an ongoing basis in order to provide management with advance warning of material changes in the operating environment
7	Whenever established triggers/tolerances are exceeded, adjust tactics using previously developed plans and generate a new forecast reflecting the change in scenario and the changes in tactics

Trade resumption plans

Disruptions are inevitable. Therefore supply chain managers must have a selection of coordinated strategies to resume operations.

The need for trade resumption plans and the resilience they can provide has been underscored by the recent impacts of Hurricane Sandy. Power outages forced the first double-day closure of the New York Stock Exchange in 127 years. The dominant trading house, NYSE Euronext, unveiled (but did not apply) a precautionary plan to shift processes to the Arca platform and resume trading.

Arca is an all-electronic system capable of handling the opening and closing auctions, should the default system be inoperable for an extended period. The Arca system was tested on 31 March 2012. Despite Hurricane Sandy, it has yet to be used.

Sources

1. New Models for Addressing Supply Chain and Transport Risk. World Economic Forum, 2012. www3.weforum.org/docs/WEF_SCT_RRN_NewModelsAddressingSupplyChainTransportRisk_IndustryAgenda_2012.pdf. Last accessed: 07/12/2012.
2. Transportation & Logistics 2030. Volume 4: Securing the supply chain. PwC, 2011.
3. The Jones Act is the Merchant Marine Act of 1920.
4. "White House expected to seek billions in Sandy disaster aid again". Reuters, 2012.
5. Thailand's 2011 flooding: Its impact on direct exports, and disruption of global supply chains. Chongvilaivan, A., 2012. ARTNeT Working Paper No. 113, May, Bangkok, ESCAP. Available from www.artnetontrade.org.
6. "Thailand's flood defenses under strain again". Reuters, 2012.
7. Barge traffic moves after another Mississippi River snarl. Reuters, 2012.
8. A Dangerous Delay, The cost of late response to early warnings in the 2011 drought of the Horn of Africa. Oxfam & Save the Children, 2012.
9. "Fed's Lockhart warns of unusual threats to financial systems". Reuters, November 2012.
10. A global regulatory standard on bank capital adequacy, stress testing and market liquidity risk drawn up by the Basel Committee on Banking Supervision.
11. The state of food insecurity in the world - Policy options to address price volatility and high prices. Food and Agriculture Organization, 2011. www.fao.org/docrep/014/i2330e/i2330e05.pdf. Last accessed: 07/12/2012.
12. "Thai floods, hard drive shortage threaten PC sales". Reuters, October 2011.
13. Accenture research on the concept of dynamic operations, available at www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Designing-Dynamic-Operations.pdf#zoom=50.
14. Policy Options for Reducing Losses from Natural Disasters: Allocating \$75 billion. Kunreuther, Howard and Michel-Kerjan, E., Center for Risk Management and Decision Processes, 2012.
15. The US housing bubbles and bust: impacts on employment. Buyn, Kathryn J., US Bureau of Labor Statistics, 2010.
16. Deutsches Cyber-Abwehrzentrum nimmt Arbeit auf. Heise online, 2011. www.heise.de/security/meldung/Deutsches-Cyber-Abwehrzentrum-nimmt-Arbeit-auf-1220106.html. Last accessed: 14/12/2012.
17. Risk and Responsibility in a Hyperconnected World: Pathway to Global Cyber Resilience. World Economic Forum, 2012.
18. Transportation & Logistics 2030, Volume 4: Securing the supply chain, PwC, 2011.
19. "The Changing Face of the Supply Chain". Industry Week, 2010. www.industryweek.com/companies-amp-executives/changing-face-supply-chain. Last accessed: 11/10/2012.
20. Global Electronic Health Record Systems Market 2011-2015. TechNavio, 2011.
21. Global Risks report. World Economic Forum, 2011.
22. Creating Resilient Supply Chains: A Practical Guide. Cranfield School of Management, 2003.
23. Resilience – What is it and how to achieve it. Sheffi, Yossi, 2008. http://web.mit.edu/scresponse/repository/Sheffi_Congressional_Testimony.pdf. Last accessed: 20/12/2012.
24. "Building a Resilient Supply Chain". Harvard Business Review. Supply Chain Strategy. Sheffi, Yossi, 2005.
25. Structural policies and economic resilience to shocks. Organisation for Economic Co-operation and Development, 2007.
26. Food for Thought: Exploring Food Security in the Pacific. Pacific Institute of Public Policy, 2011.
27. Cannes B20 Business Summit: Final Report, with appendices. Cannes B20 Business Summit, 2011. www.b20businesssummit.com/uploads/presse/Final-Report-with-with-appendices-B20-2011.pdf. Last accessed: 10/12/2012
28. C-TPAT, 2012. www.c-tpat.com/. Last accessed: 05/10/2012.
29. Benefits. TradeXchange, 2012. <https://www.tradexchange.gov.sg/tradexchange/ShowBinary/BEA%20Repository/txwp/document/tx-brochure.pdf>. Last accessed: 21/11/2012.
30. Activity contents. Kyohokai, 2012. www.kyohokai.gr.jp/english/outline/activity.html. Last accessed: 21/11/2012.
31. Logistics Performance Index. World Bank, 2012.
32. Designing Dynamic Operations: How Companies Can Turn Permanent Volatility into a Permanent Competitive Advantage. Accenture, 2012.
33. Improving Supply Chain Effectiveness. SAP, 2011.
34. Is your supply chain disruption proof? A guide to building resilient supply chains. SingTel, 2007.
35. "Boeing 787 Profit Plan Strained by Order Cut". Wall Street Journal, 2012. online.wsj.com/article/SB10000872396390444082904577607763462282088.html. Last accessed: 28/09/2012.

36. Supply Chain Risk Management: Tools for Analysis. Olson, D. Business Expert Press, 2012.
37. Technology. White House, 2012. www.whitehouse.gov/issues/technology. Last accessed: 05/10/2012.
38. NOAA's National Climatic Data Center Sectoral Engagement Fact Sheet. Transport. NOAA, 2010.
39. CDP Supply Chain. Carbon Disclosure Project, 2012. <https://www.cdproject.net/en-us/programmes/pages/cdp-supply-chain.aspx>. Last accessed: 24/10/2012.
40. Key Environmental Indicators. United Nations Environment Programme, 2011.
41. Global customs and police operation nets large seizures of bomb-making material. World Customs Organization, 2011.
42. WCO SAFE Framework of Standards (2012). World Customs Organization, 2012. www.wcoomd.org/~media/WCO/Public/Global/PDF/Topics/Facilitation/Instruments%20and%20Tools/Tools/Safe%20Package/SAFE_Framework_2012_en.ashx?db=web. Last accessed: 22/11/2012.
43. For more detailed information on AEO programmes, see Polner, M., AEO Compendium – 2012 edition. WCO Research Paper Series No.25, <http://www.wcoomd.org/en/topics/research/activities-and-programmes/~media/930340C77B3740D6B3894F747AF6A7FF.ashx>. Last accessed: 14/12/2012.
44. Avoiding low probability, high impact events. PwC, 2008.
45. New Strategies for Supply Chain Leaders. Roy, Stuart. Oracle, 2010. www.oracle.com/us/corporate/profit/opinion/080410-roy-167041.html. Last accessed: 26/10/2012.
46. About the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). HITRAC, 2012. www.dhs.gov/about-hitrac. Last accessed: 01/11/2012.
47. Ibid.
48. National Infrastructure Protection Plan: Partnering to enhance protection and resiliency. US Department of Homeland Security, 2009.
49. Minimize supply chain disruption and reduce risk. SAP, 2012. www.sap.com/solutions/technology/cloud/supplier-infonet/index.epx#features. Last accessed: 05/10/2012.
50. "Supplier InfoNet Takes Supply Chain Risk Management to the Next Level". Procurement Transformation Blog. Capgemini, 2011. www.capgemini.com/procurement-blog/2011/12/23/supplier-infonet-takes-supply-chain-risk-management-level/. Last accessed: 05/10/2012.
51. Scientific Advice and Evidence in Emergencies. Third Report of Session 2010–11, Volume I: Report, together with formal minutes, oral and written evidence. House of Commons, Science and Technology Committee, 2011.
52. Current Drug Shortage Index. US Food and Drug Administration, 2012. www.fda.gov/Drugs/DrugSafety/DrugShortages/ucm050792.htm. Last accessed: 24/10/2012.
53. Public sector supply chain: risks, myths and opportunities. A New World of Risk. Zurich Municipal, 2009.
54. "On the Unique Features of Humanitarian Logistics". Journal of Operations Management (JOM). Holguín-Veras, J., Jaller, M., Perez, N., Van Wassenhove, L., and Wachtendorf, T. (2012) DOI: 10.1016/j.jom.2012.08.003, 30(7-8):494-506.
55. How prepared are you? Business Continuity Management Toolkit. HM Government, 2012. businessassurance.com/downloads/2009/01/bcm_toolkit_active11.pdf. Last accessed: 09/11/2012.
56. Commissioning for Success: How to avoid the pitfalls of open public services. Institute for Government, 2011.
57. ISO31000. Risk management - Principles and guidelines. International Standards Organization, 2009.
58. Piloting Supply Chain Risk Management Practices for Federal Information Systems. National Institute of Standards and Technology. US Department of Commerce, 2010.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is tied to no political, partisan or national interests.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org