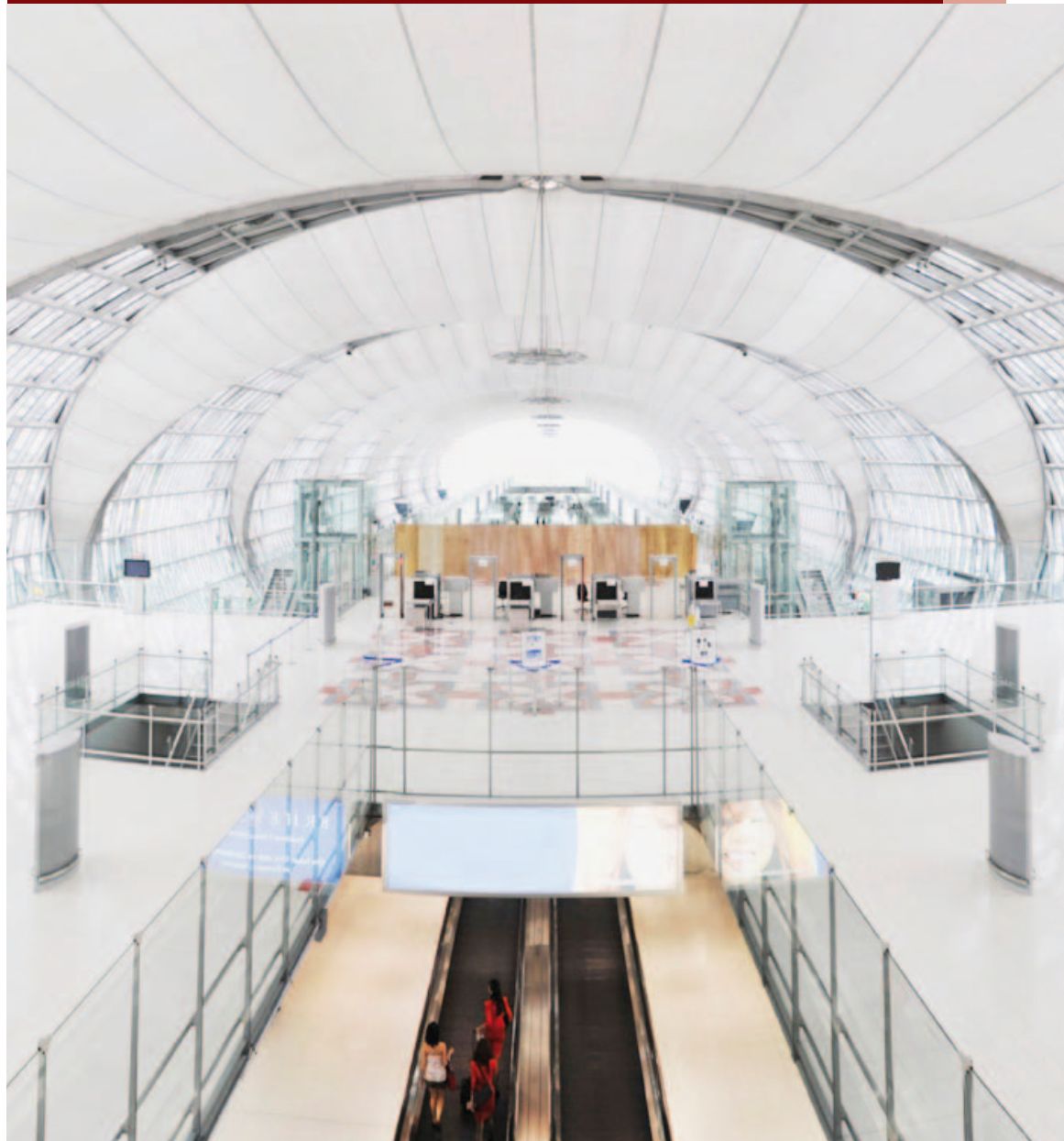


Transportation & Logistics 2030

Volume 4: Securing the supply chain

Strategies to help companies take an active role in improving supply chain security.



Acknowledgements

The editorial board of this issue of our Transportation & Logistics 2030 series consisted of the following individuals:

PwC

Klaus-Dieter Ruske
+49 211 981 2877
klaus-dieter.ruske@de.pwc.com

Dr. Peter Kauschke
+49 211 981 2167
peter.kauschke@de.pwc.com

Gautam Basu
+358 5040 16830
gautam.basu@fi.pwc.com

Julia Reuter
+49 211 981 2095
julia.reuter@de.pwc.com

Dr. Elizabeth Montgomery
+49 89 5790 5159
elizabeth.montgomery@de.pwc.com

EBS Business School Supply Chain Management Institute

Dr. Heiko von der Gracht
+49 611 7102 2100
heiko.vondergracht@ebs.edu

Tobias Gnatzy
+49 611 7102 2100
tobias.gnatzy@ebs.edu

Christoph Markmann
+49 611 7102 2100
christoph.markmann@ebs.edu

Dr. Inga-Lena Darkow
+49 611 7102 2100
inga-lena.darkow@ebs.edu

We would like to thank the panellists who took part in the Delphi survey that underpins this report. For confidentiality reasons their names will not be mentioned. We would also like to thank Thorsten Neumann, chairman of TAPA EMEA, for his support and opening up his network of security experts for this research.

We would like to express our appreciation for the expertise provided by the below listed individuals: Dan Antonio, Jochen Schmidt and Otto Vermeulen.

For more information on the T&L 2030 series or a download of our four T&L 2030 publications, please visit www.pwc.com/tl2030.



Welcome

Supply chains must be secured against any form of man-made and natural disruption. This certainly isn't a new revelation. Some hundred years ago commercial shipping was threatened by pirates and renegades like Anne Bonny, Sir Francis Drake or Klaus Störtebeker, and so transport ships were equipped with cannons and crews ready for a fight. Today piracy as a 'business model' is enjoying a remarkable renaissance. It's but one of many threats facing international logistics.

Freight and passenger transport facilities are frequently the target of attacks, whether the motive be political or purely for profit. Natural disasters like the devastating earthquake and tsunami in Japan show us only too clearly just how vulnerable our transportation and logistics systems are, when, for example, key commercial harbours are taken out of commission; not to mention the far graver human suffering such events can cause. And with electronic data exchange becoming an ever more critical part of interlinked value chains, worries about data security and industrial espionage are becoming more pronounced.

Reason enough to focus the fourth volume of our thought leadership series Transportation & Logistics 2030 (T&L 2030) on the topic of supply chain security. As in previous studies, we've surveyed a global group of experts using the RealTime Delphi method. They told us what elements of supply chain security they believe will be most critical in the future.

Will we see more attacks on supply chains and logistics hubs in the future? Do the experts foresee cyber attacks causing much damage in transportation and logistics? What is the best way to guarantee security – advanced technology or security audits or what else? Will these measures lead to huge extra costs and a slow-down of transport?

These are some of the questions we address in this report. We appreciate that you have 'secured' your copy of T&L 2030 Vol. 4 and hope it will help you secure your supply chain, too.



Klaus-Dieter Ruske
Global Industry Leader
Transportation & Logistics
PwC



Dr. Peter Kauschke
Transportation & Logistics 2030
Programme Director
PwC

Foreword

The world is becoming smaller. Supply chains of today's companies have globalised due to increasing efficiency in transport and logistics. 90 percent of the entire global trade flows through only 39 bottleneck regions. All prognoses indicate that global trade will increase in the future and along these so-called gateway regions. But the world is still a dangerous place: Since our global economy is strongly dependent on certain hubs it is unthinkable what would happen if there was a terrorist attack on just one of them. And exactly that is where the problem lies and what this study addresses:

As long as it remains unimaginable in our minds, it remains dangerous. This study boldly thinks ahead to where, until now, our thoughts have not yet dared to venture.

The study also observes the new face of danger: cyber attacks. Today, entire countries are already exposed to permanent virtual attacks. Every two seconds, the German Internet is attacked. Logistics, as driver of globalisation, will become the focus of offenders in the years to come. A hacker could infiltrate the flight control system, for example, and randomly let airplanes fall from the sky. Or re-set the tracks in rail traffic and let trains crash... What would we do then?

Based on the opinions of leading experts for supply chain security from academia, business practice, technology development and politics, the study proves: It isn't enough to simply react. Supply chain security is not crisis management. Supply chain security is proactive: It hinders attacks before they happen. Supply chain security will have failed if such catastrophes start to occur.

Moreover, the study demonstrates that the future belongs to secure supply chains. However, the one who would like to achieve this security with modern technology builds on sand. The best scanner for explosive agents is useless if the security personnel is not well-trained or if the communication processes within the supply chain do not function.

We are living in an era of increasing menace. However, professional supply chain security guarantees the foundation of modern life: secure supply chains.



Dr. Heiko von der Gracht

Managing Director
Center for Futures Studies and Knowledge Management
Supply Chain Management Institute, EBS Business School

Table of Contents

Executive Summary	6
Findings of Delphi survey	10
Introduction	11
Ensuring secure passage	14
Keeping cyber space safe	22
Investing in a more secure future	25
Wildcards	30
Opportunities	38
Methodology	43
References	49

Executive Summary



As the number of man-made attacks on supply chains increases, how will companies need to react? Where will the critical points on the supply chain be – and how can companies stay flexible if situations heat up? How can companies make sure their people and technology are up to the task of securing the supply chain over the next two decades?

There are no easy answers, but the urgent need to ask these questions is clear. Threats from terrorism and piracy, for example, are on the upswing. That's already starting to have an impact on supply networks.

Total direct costs of piracy in 2010 are estimated to be between US\$ 7 billion and US\$ 12 billion.¹ And when you look at the indirect costs too, the figure is much higher. Piracy damages the tourism industry, causes losses in revenues for canal fees and the costs "loss of use" and "loss of man-hours" while ships and their crew are held hostage are also significant. Many shipping companies are now either hiring special security, working together with UN troops or altering their shipping routes.

Terrorism remains a concern too, particularly since there are a number of locations that are particularly crucial to the smooth flow of supply chains – and therefore potentially most vulnerable to attack. Logistics hubs and gateway regions are one concern. As just one example, a full 14.8% of containerised

and air freight traffic moves through the Hong Kong - Shenzhen freight cluster, so a disabling attack here would have a huge impact. Because logistics hubs drive economic activity, successful attacks could also threaten economic stability.

Chokepoints, geographic features where there's only one narrow way across a strait, valley or bridge, are another potential weak point. Disrupting traffic through the Panama Canal, Suez Canal or the Strait of Malacca, for example, would slow down freight flows significantly.

Ensuring secure passage

We believe that transportation and logistics companies will need to take security concerns into account when choosing transport routes. They'll need to take a close look at how dependent their business is on particular logistics hubs or chokepoints, and then assess how they can reduce the impact of threats to particular locations. Transportation and logistics companies will also need to be prepared to respond quickly if risk levels change.

Man-made attacks on supply chains are increasing. Transportation and logistics companies will need to take security concerns into account when choosing transport routes.

Greater investment to secure ICT systems from cyber attacks will be absolutely mandatory.

Supply chain managers across all industries will need to take into account higher transport costs, longer travel times and potential problems meeting schedules when alternative transport routes are used. Even without disruptions, more security will mean longer transport times. That could have a far-reaching impact. In some cases business models based on time-critical deliveries may be squeezed out of the market.

Keeping cyber space safe

The transportation and logistics industry already relies heavily on Information and Communication Technology (ICT), and as we've shown in previous reports, the trend is upwards. Virtual threats need to be taken just as seriously as physical ones. Indeed, we believe that cyber attacks designed to induce physical damage will be an increasing threat for the transportation and logistics industry. Greater investment to secure technologies from cyber attacks will be absolutely mandatory. Data will be at risk too, and while privacy concerns won't go away, we think the need for greater security will become paramount.

Investing in a more secure future

Does all this emphasis on improving security measures mean profits will decline? Not necessarily. Well-planned security investments provide a payback not only in terms of loss prevention, but also by enhancing supply chain performance.

Planning ahead is critical in other ways, too. When it comes to security, it's especially important to look at future scenarios and manage security proactively. Reacting to crisis situations is not enough. Companies have to find the right combination of preventive and reactive measures to achieve the optimal level of supply chain security.

We believe that companies need to consider the possible, not just the probable. Executives should keep an eye on so-called wildcard events too. That means looking at the possible financial impact, the relative vulnerability of their business model and their company's ability to react to low-probability, high-impact events.

No supply chain will ever be 100 percent secure – but better technology and well-trained people can make a big difference.

Stricter standards and the need to take the lead

And while they won't need to go it completely alone, transportation and logistics companies shouldn't expect government to pick up the slack. We believe that governments won't take a leading role in executing supply chain security, although they will continue to regulate security measures. Transportation and logistics companies will need to work together with governmental institutions to develop new security standards that are not only effective, but also efficient.

We believe that security audits along the entire supply chain will become a requirement to maintain effective levels of security. But even with stricter standards and better technology, no supply chain will ever be 100 percent secure. Technology can help increase security, but people are needed too, to provide human intelligence and good governance.

Supply chain security is challenging, but there are opportunities too. Companies that are able to develop flexible, agile systems that can respond quickly and appropriately to crises – and avoid threats when possible – will have a competitive advantage.

Note on methodology

This study is based on a multifaceted analysis of the importance of supply chain security for the transportation and logistics industry. Our methodology draws upon a rigorous mix of desk research and the results of a Delphi survey among 80 selected subject matter experts from 25 countries around the world, including both emerging and mature economies.

Findings of Delphi survey



Introduction

Supply chains will face more direct attacks.

Terrorist acts, also called man-made attacks, are nothing new. In the 70's, 80's and 90's, the Irish Republican Army (IRA) conducted attacks on British police and army, and Germany's Red Army Faction (RAF) organised bombings and assassinations, to name just two well-known examples. In the past decade, though, media and public attention has gone up dramatically around the world and the focus has shifted from national to international threats. The 9/11 attacks on the World Trade Center in New York and the Pentagon in Washington D.C. in 2001 marked one defining moment. There have been others too. A bomb set off in Madrid in 2004 caused an explosion in a public train which killed more than 190 people. And several explosions in underground trains and busses in London killed and injured more than 200 people in 2005. Both events dominated news headlines around the world.

And the threat isn't letting up. The head of the Federal Service for Supervision of Transport in Russia recently announced that the number of terrorist attacks on Russia's transport systems has more than doubled between 2009 and 2010.² That jump may continue, if the bomb explosion at Moscow's airport Domodedovo in January 2011 is a sign of things to come.³ Recent parcel bombs sent from Yemen via Europe to the US have also received heavy coverage from the international press. It's not

only public transit systems that need to be vigilant – cargo transportation can also be used as a carrier to conduct a terrorist attack and to harm human life. So securing supply chains is vital. Supply chains and transport systems need to incorporate measures to secure human lives and transportation infrastructure into their design. Freight screening, risk profiling of employees and the use of trusted shippers are some of the options that can help.

Attacks on supply chains have a serious human cost when they threaten access to food or medical supplies. They can also place a huge burden on economies by shutting down trade or travel.⁴ When Bangkok airport in Thailand was forced to close in 2008 due to protests, it cost the Thai economy US\$ 8.5 billion. The shutdown impacted not only the tourism and airline business, but also important export businesses, like the orchid industry. Thailand is the world's leading orchid exporter with an 80 percent share of the global market. The closure of the airport cost the sector over US\$ 9 million.⁵ And the eruption of a volcano in Iceland caused a ripple effect around the world. The global airline industry (particularly carriers operating in Europe) lost an estimated US\$ 1.7 billion in revenues when over 100,000 flights were canceled in six days.⁶

One study by Stanford University documents the combined human and economic costs of a terrorist attack through a specific example. The study shows that an attack on the US milk supply chain with only 10g of highly concentrated toxin would be enough to poison almost 500,000 people. The human cost would clearly be catastrophic, and the economic impact would be too. Every 50,000 people who

suffered from the poison would cost the US economy US\$ 8.6 billion.⁷ Just one attack could potentially mean damage in excess of US\$ 80 billion.

Sound far-fetched? We took a look at data on supply chain related attacks between 2004 and 2010 to better understand the risks. A comprehensive, open-source database on the Internet – Worldwide Incidents Tracking System (WITS) – lists information on more than 68,000 incidents worldwide from its creation on 1 January 2004 through 30 April 2010. The database was developed and is permanently updated with open source data by the US National Counterterrorism Center (NCTC), a government body for collecting, integrating and analysing data on terrorism and counter-terrorism.⁸ We analysed NCTC data, focusing on the number of attacks that targeted

- transport infrastructure (including roads, bridges, tunnels, railways and railroad tracks)

Our results show that the total number of supply chain related attacks has increased steadily over the past decade, reaching 3299 attacks in 2010 (see Figure 1a), despite the sharp increase of security measures and control systems put into place after 9/11. Countries and companies are still struggling to come to grips with attacks and supply chain disruptions. Current systems aren't secure enough to protect the flow of global supply chains. We believe that this trend will continue in years to come, which means man-made attacks and supply chain disruptions will increase.

- the aviation sector (includes airlines and airport facilities)
- ships (including any water-borne vehicle or maritime vessel)
- vehicles (including cars, mini buses, trucks, buses)
- train/subway (includes passenger or cargo rail, subway or monorail)

Figure 1a Number of attacks including vehicles

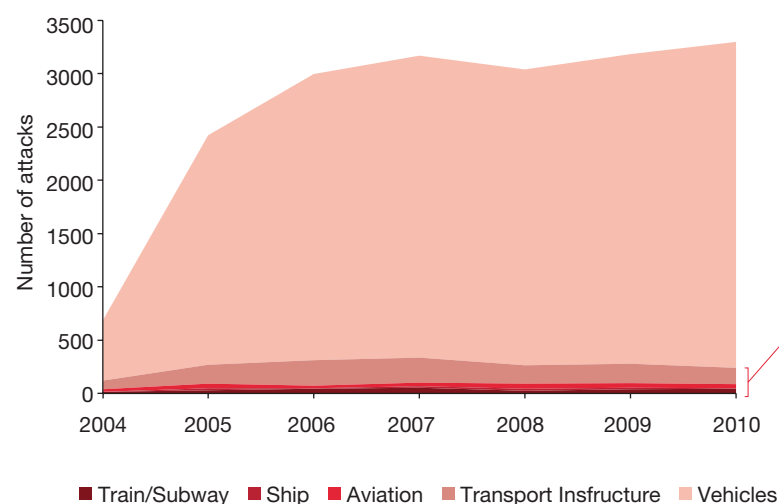
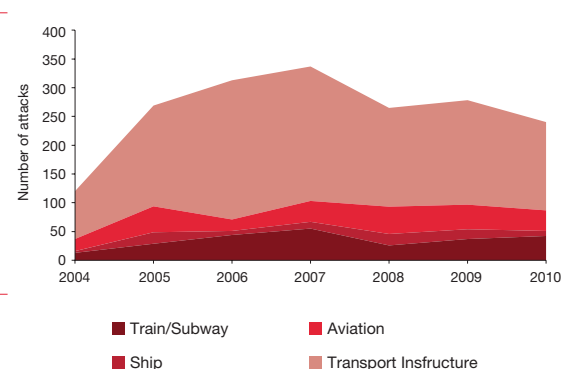


Figure 1b Number of attacks excluding vehicles



Source: NCTC, PwC Analysis

There are far more attacks on vehicles than on other transport modes such as ships, trains/subways or attacks on airlines and airports. The majority of vehicles attacked are cars, although there were also incidents involving buses. Buses and cars are nearby and easy to access; you don't need a lot of planning to successfully attack them. Airlines and airports or harbour regions generally have much higher existing security standards, so you need some level of professional organisation in order to attack them successfully.

Many terrorist groups are focused on their home territory and often choose targets that are close to their operational basis. When terrorist attacks involve political disputes over territory, they're often carried out in the relevant territory.

Do experts believe that attacks on supply chains will be more common in the future? To find out, we asked our Delphi panel to assess our first projection: "2030 – The number of attacks on supply chains has increased."

The results are surprising. The experts in our panel don't agree about the probability of a significant increase in attacks on the supply chain in the future. Instead, they fall into two distinct camps. One group ('concerned' experts, 60% of the total sample) believes that the number of supply chain attacks will strongly increase in the future. The other group ('relaxed' experts, 40% of the total sample) doesn't foresee a significant increase in attacks on supply chains. For a more detailed analysis of panellists' response behaviour, please see page 47.

But the differences don't stop there. Concerned experts seem to take a more pessimistic position – but they're actually less pessimistic and more willing to take risks to respond to the threats posed to supply chains, as we'll show.

What arguments do concerned experts use to support their view that supply chain attacks will strongly increase? Some note that the number of attacks on supply chains is already increasing. Theft, pilferage, missing cargo and counterfeiting are issues that the supply chain manager has to deal with on a daily basis. Financial damages caused by theft in European supply chains exceed a value of EUR 8.2 billion per year.⁹ They're also worried that rising unemployment and an enlarging gap between rich and poor countries and individuals will drive even greater numbers of attacks on supply chains. What impact will such jumps have? Concerned experts point to supply chains as highly vulnerable and critical to the world economy. Attacks on those economic lifelines would destabilise entire economic systems and cause severe economic downturns. If supply chains come to a halt due to man-made attacks, food and medical supplies might run short. And the cost of fuel could skyrocket, if man-made attacks force a breakdown in international supply chains.

Not all the experts agree. The relaxed group considers an increase in attacks as not very likely. In contrast to the concerned group, they argue that supply chains are already sufficiently secured against attacks, and they believe security levels will get better still. New and innovative technologies will be available to better track the movement of physical goods and spot irregularities in supply chains quicker. That would mean many attacks on supply chains could be avoided.

Whether they're concerned or relaxed about the probability of an increase in the number of attacks on supply chains, it comes as no surprise that the majority of experts see such a jump as highly undesirable. Interestingly, there are some experts who actually see an increase in the number of attacks as a good thing. They argue that attacks mean organisations will make it a priority to find solutions and develop more secure supply chains. Organisations will be more motivated to improve their security measures.

Supply chains will come under increasing attack, and companies need to be aware and prepared. That could mean rethinking their approach to dealing with potential supply chain disruptions.

Ensuring secure passage

Where are global supply chains most at risk? Countries that are less stable, either politically or economically are often hot spots. Gateway regions where there are very large flows of cargo are particularly important for global supply chains, and are therefore also of special interest to those looking to disrupt them. And just like military troops, goods often need to pass through certain chokepoints, geographic features where there's only one narrow way across a strait, valley or bridge.

We've considered all three factors and have developed risk maps which show graphically where supply chains may be most vulnerable, looking first at country risk factors, then gateway regions and lastly geographic chokepoints.

Some geographical regions or individual countries are more attractive targets than others. Figure 2 shows the relative risk of terrorist attack or activities in every country around the world, as well as four major areas of piracy, according to the International Maritime Bureau's. These piracy areas include the Gulf of Aden, near Somalia and the southern entrance to the Red Sea, the Gulf of Guinea, near Nigeria and the Niger River delta; the Malacca Strait between Indonesia and Malaysia; and Malacca Strait between Indonesia and Malaysia; and the coast of Venezuela and Columbia.¹⁰

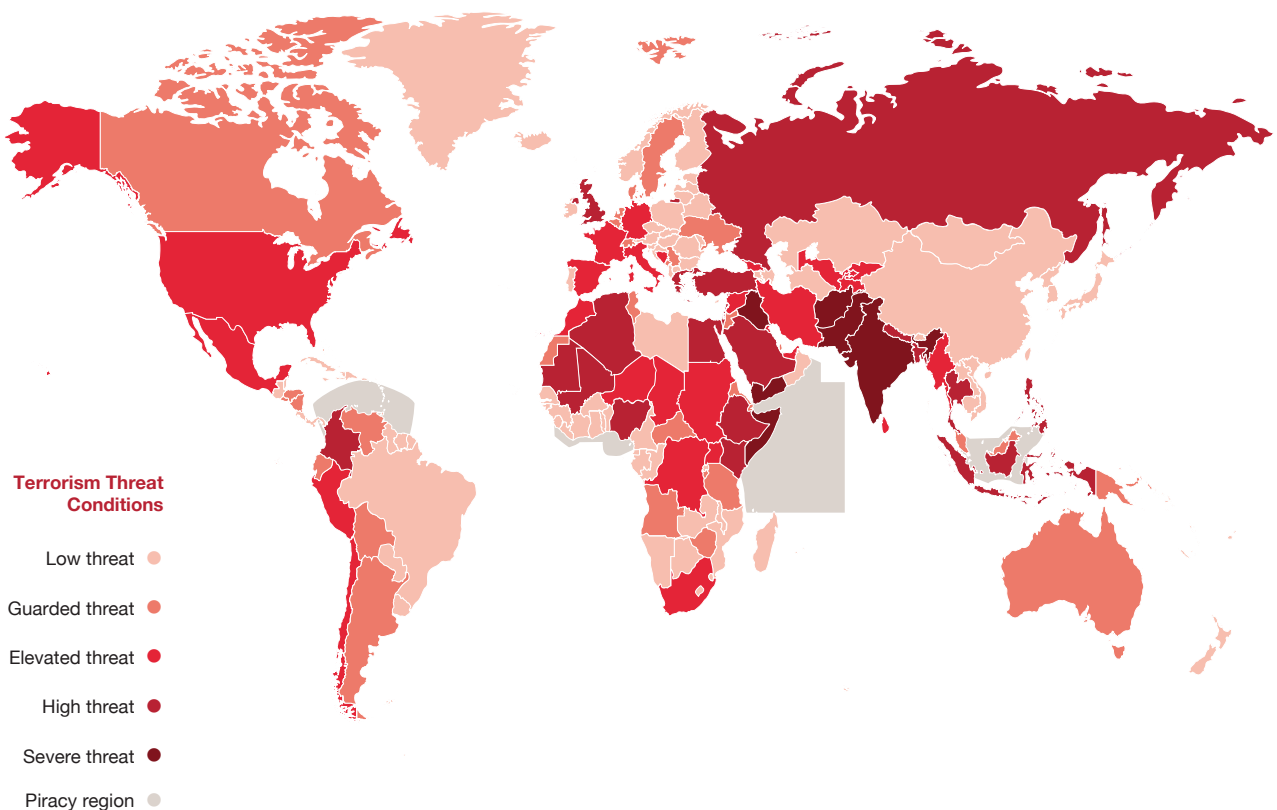
The risk factor calculation takes into account each country's relevance for terrorists, separatists and nationalists, instability due to recently conducted or ongoing revolutions and the number of kidnappings. Countries facing a severe threat include the Horn of Africa with Yemen and Somalia, Afghanistan, Pakistan, India, and Iraq.

Yemen and Somalia's 'severe threat' ranking is largely due to Islamic extremist connections. Somalia was one of the nations where experts believed Islamic extremists might flee after 9/11, and observers still see the country as a possible haven. Yemen is the base for operations by Al Qaida in the Arabian Peninsula (AQAP), including high profile attacks in 2009 that prompted many to urge the Yemeni government to take direct action against AQAP.¹¹

Pakistan is another hot spot, with an increase in unmanned vehicle strikes with extreme violence and extremists groups on the rise in the past years. The recent US mission resulting in the death of Osama Bin Laden may also prompt retaliatory unrest.

Nearby India has a tense relationship with Pakistan, exemplified by the 2008 Mumbai attacks, often referred to in India as 26/11, where more than 10 coordinated shooting and bombing attacks across Mumbai were executed by a Pakistan-based militant organisation. India also struggles with additional threats, from separatists, other religious extremists and individuals or groups pursuing their own interests.

Figure 2: Supply chain risk map – Terror threat conditions



Source: Aon's 2010 Terrorism Threat Map³⁹

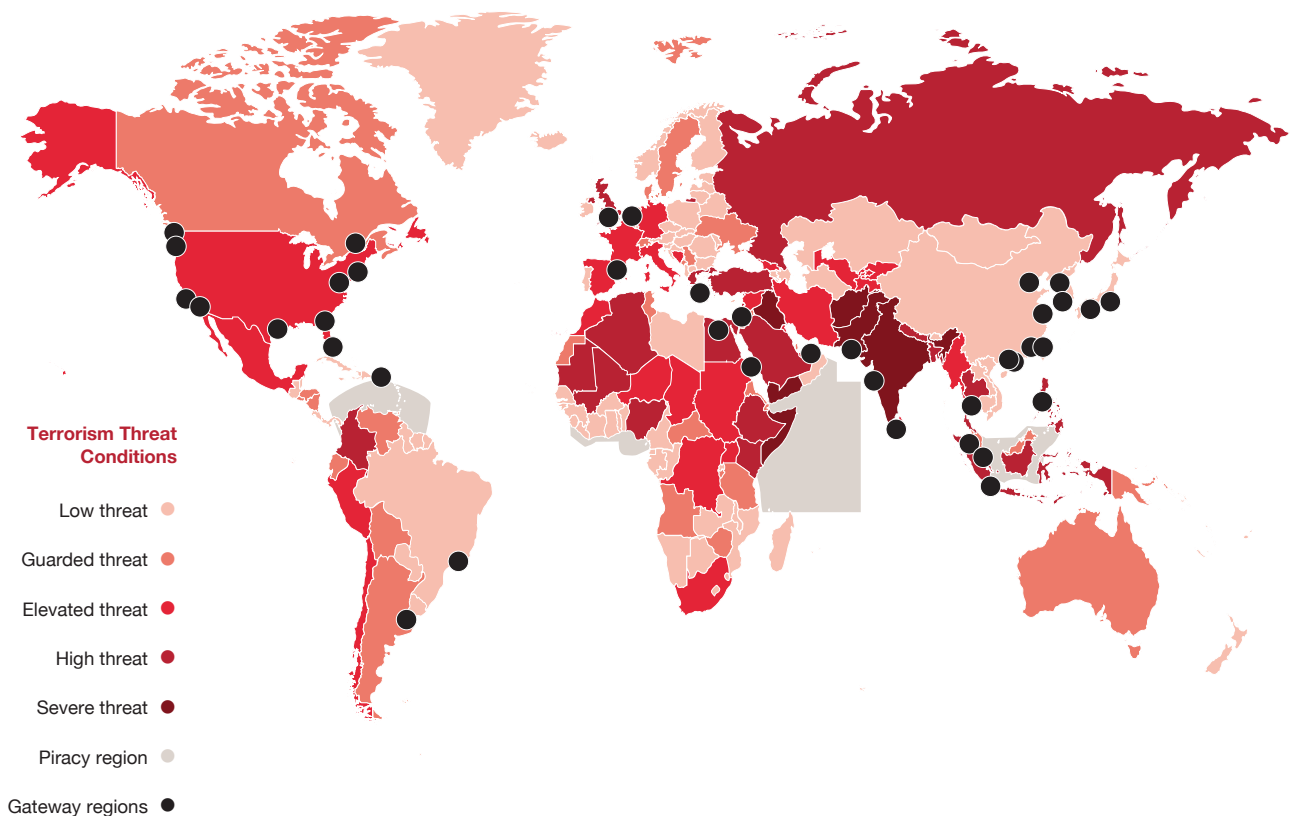
Logistics hubs and chokepoints will be favoured targets. Successful attacks could threaten economic stability.

Attacks on supply chains are often looking for a big return on a small investment.¹² Because they're so vital to trade flow, logistics hubs like airports or ports offer the ideal target. The possible consequences of disrupting a logistics hub, for example, can be seen by taking a look at the port strike in 2002, where 29 ports on the US West Coast were locked out due to a labour strike of 10,500 dockworkers. The strike had a massive impact on the US economy. Approximately US\$ 1 billion was lost per day and it took more than 6 months to recover. At this time, 60 per cent of USA's cargo – with a value of more than US\$ 300 billion – passed through

west coast ports annually. As the US accounts for around 20 percent of global maritime trade, the consequences of the port strikes were not just limited to the US but affected economic activities around the globe.^{13,14}

If seaports and airports that serve as global gateways were attacked, the consequences for international trade flows could be a lot more severe. Figure 3 shows 39 major gateway regions, which account for 90 per cent of world trade. These include many ports, airports and train stations in metropolitan regions.¹⁵ Gateway regions are centres of cargo handling and thereby determine areas of high relevance for global supply chains. One example is the Tokyo - Singapore corridor in Pacific Asia, where there's a major concentration of freight activity. The world's largest gateway region is the Hong Kong - Shenzhen freight cluster. A full 14.8% of containerised and air freight traffic moves through this region.

Figure 3: Supply chain security map – Global gateway regions



Source: Aon's 2010 Terrorism Threat Map, The Geography of transport systems^{15,39}

If you include China's Pearl River Delta (with Guangzhou), then the region's share of world trade reaches 16.7%. Europe's Rhine/Scheldt delta (from Amsterdam to Brussels) accounts for 7.5% of global containerised and air freight volume. The most important North American gateway system is Los Angeles/ Long Beach system.¹⁶

According to a report of the Congressional Research Service (CRS) for the US Congress, the detonation of a nuclear bomb, comparable with the one from Hiroshima, in one of the world's major gateway regions or harbours would kill and injure a catastrophically high number of people. In addition to the human cost, the economic impact would be huge. This type of event could cause US\$ 50 to 500 billion in direct property damage, US\$ 100 to 200 billion losses due to trade disruptions and additional US\$ 300 billion to US\$ 1.2 trillion of indirect costs¹⁷. Likewise, the costs associated with the closing of US ports because of a bomb detonation in a harbour could amount to US\$ 1 trillion.^{18,19}

But could it happen? It's certainly possible. There have been news reports that plutonium from former military inventory 'leaks' on to black market, and that there's also a trade in nuclear bomb blueprints.^{20,21} With nearly 9 million containers entering the United States annually by ship, it's not hard to imagine someone successfully hiding a nuclear bomb in one of them.²²

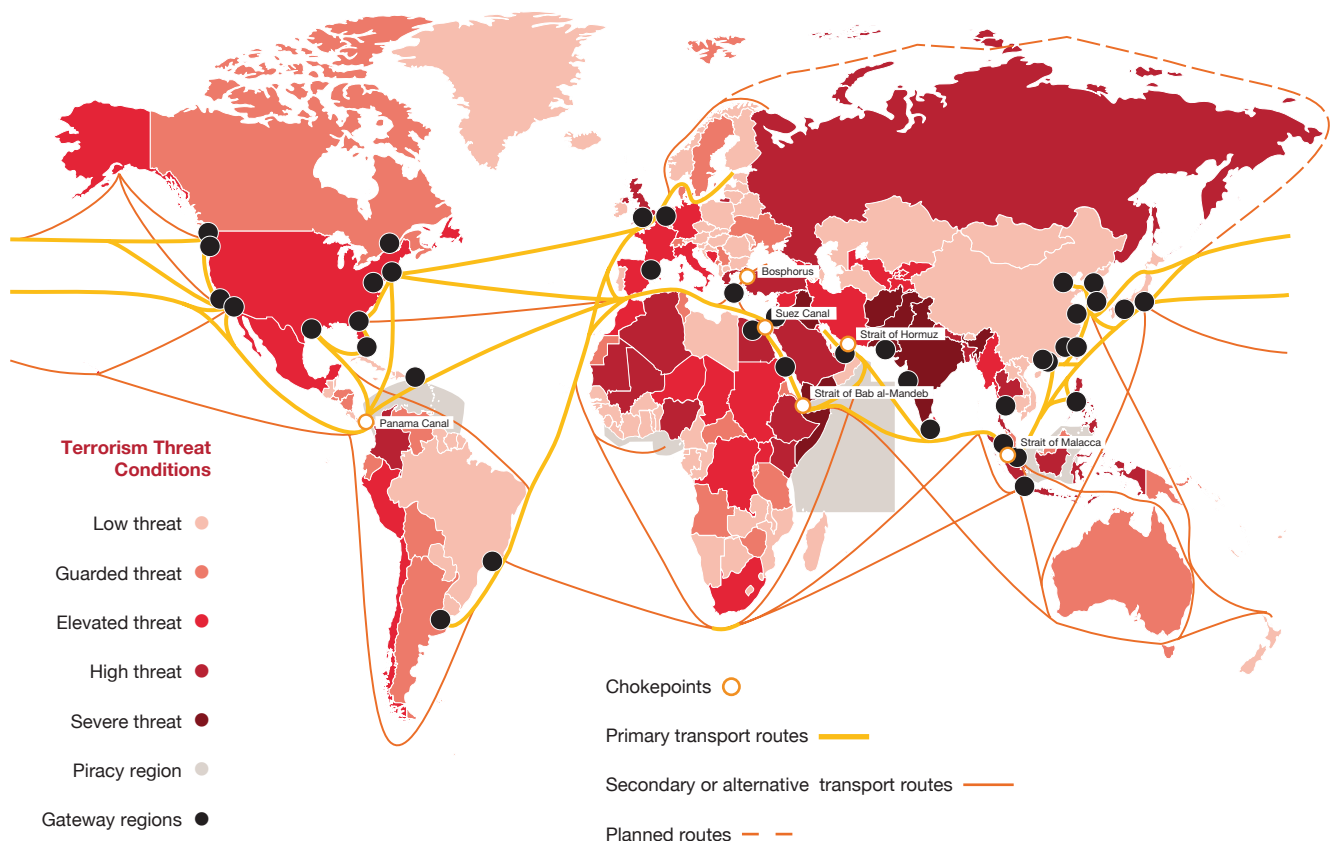
And the dangers aren't confined to sea freight. Last year, parcel bombs were sent from Yemen and transhipped via Europe to the USA. That drew attention to air cargo traffic and prompted US Homeland Security Secretary Janet Napolitano to demand a closer cooperation between the EU and the US to protect critical air, land and sea transportation hubs. She pointed out that "regardless of where a potential event might occur, the ripple effect of a significant disruption of this global system could potentially impact the entire international community."²³ Napolitano also said it is imperative that governments work together to ensure that the global supply chain is able to

rebound quickly from any future attack as consequences for the global economy could be catastrophic.²⁴

Logistics hubs are determined by trade flows, but chokepoints such as channels, narrows and bridges are critical spots for global supply chains, and they're an unavoidable part of the landscape. International shipping lanes pass through around 200 passages, capes and straits. A handful of these are of strategic importance. Take the Panama Canal. Bypassing this man-made channel would mean a vessel on its way from Los Angeles to Barcelona would need to travel around Cape Horn, or through the Indian Sea – options which would lengthen the overall travel time 9-11 days.

Figure 4 shows primary and secondary sea routes that connect the major gateway regions. Many of the most important sea routes pass certain chokepoints. Some of them, such as the Suez Canal or the Strait of Malacca, are also marked on the supply chain risk map.

Figure 4: Supply chain risk map – Maritime sea routes and crucial chokepoints



Source: Aon's 2010 Terrorism Threat Map, The Geography of transport systems, National Center for Ecological Analysis and Synthesis^{15,27,33}

Many chokepoints are close to regions with an elevated risk, which increases navigation risks and potentially compromises access and use. A large number of chokepoints cannot be easily bypassed, if at all. For many, the alternative would mean a detour major enough to mean significant financial costs and delays. Due to natural conditions, these chokepoints also have natural capacity constraints. Only a certain number of ships can pass through, or bypass them, per day (see Figure 5).

Figure 5: Chokepoints in global shipping

Chokepoint	Vessels per year (2009)	Capacity	Limitation threat
Strait of Hormuz	50,000	Narrow Corridors	Iran/Terrorism
Suez Canal	17,228	200 000dwt and convoy size	Terrorism
Bosporus	50,000	Ship size and length; 200 000dwt	Restrictions by Turkey; navigation accidents
Strait of Malacca	60,000	300 000dwt	Terrorism/ Piracy
Panama Canal	14,323	65 000dwt After expansion: 116 000dwt	Not significant
Strait Bab el-Mandeb	22,000	2-mile-wide channels for shipments	Terrorism/Piracy

These chokepoints represent the geographical Achilles heels of the global transportation industry. But how likely is an attack on the security of one of these hubs and nodes? Our expert panel was asked to discuss whether logistics hubs and infrastructural nodes will become preferred targets of terrorist attacks in the future.

The experts don't all agree. Concerned experts argue that the number of attacks on these targets will strongly increase. Logistics hubs and infrastructural nodes are the weakest links of global supply chains and their importance for global trade will continue to rise. So they'll be more attractive targets for terrorist attacks, too. Since the connection of today's public and freight transport network is tight, ports, airports and train stations are not only economically important logistics hubs, but also often located in densely populated areas. A targeted attack will cause a maximum of destruction, disruption, media visibility and political pressure.

Relaxed experts have a more optimistic outlook regarding the possibility of more attacks. They're counting on

new security technologies to have an impact. They also think that regulations and governmental cooperation will be successful and help to resolve security issues around such targets. That's partly because relaxed experts expect a shift of attacks towards the most densely travelled global transport routes. That could pose its own issues, since as they point out, it will become almost impossible to prevent such attacks if they could take place everywhere within the global supply chains.

Do attacks on supply chains or hubs have the potential to destabilise the economies of entire regions? Here too, experts held very different views. Some see the direct and indirect damages of the paralysis of logistics chokepoints as harmful for the global economy, as in the West Coast harbour strike example. However, they still view the consequences for the local and global economy as only temporary. That's because they have faith in common international efforts to establish the steady flow of goods.

The panel also identified a number of factors that can influence the economic consequences of an attack:

- the size of the attacked region,
- its importance for global trade,
- its ability to absorb the attack and
- the level of support from other nations received during the recovery process.

And while there may be significant disruptions at the regional level, the global impact can be mitigated by efforts to make supply chains more resilient to disruptions. Recent pipeline projects provide some good examples where systems are designed to offset the impact of possible disruptions to a critical chokepoint. The Habshan-Fujairah pipeline, from the Habshan onshore field in Abu Dhabi to Fujairah (United Arab Emirates), is planned to back up gas and oil transport in the case of any disruption in the Strait of Hormuz. The Sino-Burma pipeline aims to reduce tanker traffic through the Strait of Malacca by providing an alternative transport route for oil and gas to China.²⁵ Although these projects can be seen as targets as well, they contribute to an improved resilience of critical transport infrastructure, by creating more diverse routing options for critical natural resources.

The danger of significant disruption may be greater in smaller regions which are dependent on single hubs or only a few critical infrastructural nodes. For example, Singapore is proud to operate one of the world's busiest and most important intermediate hubs. 85

percent of the total cargo traffic going through Singapore continues on to other regions, underlying its immense importance as a gateway region.^{26,27} An attack on Singapore's harbour could have drastic consequences for the country's economic prosperity – and also for the other regional economies which use the harbour as a transshipment hub. Likewise, a piracy induced long-ranged rerouting of ships around the Strait of Malacca directly to ports in China, Indonesia and Japan would be significant for the local economy of this region.

Temporary economic losses will certainly hurt, but the impact of attacks on logistics infrastructure or vessels might also be much far-reaching, if trade routes change permanently in response. The EU and China are already investigating transport routes along the Northern Russian Coast. As a result of the melting Arctic sea ice, such a route might become a valuable alternative to the traditional sea ways (see Figure 4), which are increasingly disturbed by acts of piracy.²⁸ The route along the Russian coast would shorten the shipping route between Hamburg and Shanghai for example by about 5,000 miles, i.e. at least 7 days of travel (see Figure 6). So this route could save time as well as being more secure. Japan is also planning to cooperate with Russia to transport uranium ore via the Trans-Siberian Railway in order to avoid incidents in the Strait of Hormuz, according to Asia News Networks.²⁹

Companies need to take a close look at how dependent their business is on particular logistics hubs or chokepoints, and then assess how they can reduce the impact of threats to particular locations.

Transportation and logistics companies will need to take security concerns into account when choosing transport routes. They'll also need to be prepared to respond quickly if risk levels change.

Piracy and hijackings of ships causes severe problems for the maritime shipping industry. Total direct costs of piracy in 2010 are estimated to be between US\$ 7 billion and US\$ 12 billion.³⁰ And when you look at the indirect costs too, the figure is much higher. Piracy damages the tourism industry, causes losses in revenues for canal fees and the costs "loss of use" and "loss of man-hours" while ships and their crew are held hostage are also significant.

The Gulf of Aden is currently the world's hot spot in terms of pirate attacks. The politically instable states of Somalia and Yemen are located on either side of the Gulf. To make matters worse, the entry point to the Gulf, the Strait of Bab el-Mandeb, is a chokepoint along the heavily used Asia-Europe sea route.

Some shipping companies have responded to the threat of piracy by hiring special security troops or taking advantage of protection offered by UN troops. Others have already shifted their shipping routes, including A.P. Møller-Maersk, CMA CGM and dozens of other carriers which have chosen to avoid the Gulf of Aden and Suez.³¹ Egypt is losing more than US\$ 642 million a year due to lost revenues from Suez Canal fees, as ships are re-routed to avoid the Gulf.³²

Commercial piracy isn't the only risk factor. For example, as previously noted, on our supply chain risk map (cf. Figure 2) Yemen and Somalia are considered to have 'severe threat' conditions, because of Islamic extremist connections which increase the risk of possible terrorist acts.

Just how big are the impacts of changed routings on shippers? We calculated the effects of re-routing vessels on this route and three others (see Figure 6). If ships choose not to pass through the Gulf on their way to the Suez Canal they face at least 4,000 extra miles, or 6 more transport days (minimum).

Figure 6: Distances and travel times for direct and alternative sea routes

Departure	Destination	Route: Direct (D) / Alternative (A)	Distance	Travel time
Los Angeles	Barcelona	D: Panama Canal	7821 nm	13 days
		A: Cape Horn	12967 nm	22 days
		A: via Indian Sea	14320 nm	24 days
Rotterdam	Singapore	D: Suez Canal	8302 nm	14 days
		A: Cape of Good Hope	11759 nm	20 days
Abadan (Iran)	Hong Kong	D: Strait of Malacca	5274 nm	9 days
		A: Sunda Strait (along Jakarta)	5843 nm	10 days
Hamburg	Shanghai	D: Suez Canal	10734 nm	18 days
		A: Northern Route	6440 nm	11 days

Cruising speed of 25 knots (~29 mph), nautical mile (nm)=1.852 kilometers

Another route plagued by piracy is the Strait of Malacca. It's the shortest sea route between the Persian Gulf and the Asian market. 60,000 vessels use it each year, making it Asia's most relevant chokepoint. If this strait were blocked, almost half of the world's merchant fleet would be forced to take the longer route around Indonesia's archipelago³⁴, adding one more day to the total travel time.

When piracy drives shippers to change routes, it places a huge strain on business, with longer delivery times. It also drives up costs, as shippers need to spend more on gasoline, labour etc. That means in some cases only very large shipping lines can afford to send ships the long way round.³⁵

The supply chain experts who participated in our Delphi study generally agree with the thesis '2030: Regional threats to security have caused shifts to transport routes. 'Some point

out that transport routes are already shifting e.g. changes to shipping routes as a result of piracy in Somalia or concerns around political unrest in Egypt and Tunisia. The Delphi panel also sees future levels of international cooperation as likely to increase as the US and other major developed nations are less able to effect change. And they think that some major emerging economic powers, e.g. China will 'buy' protection by supporting rogue regimes.

Transportation and logistics companies will have to be much more flexible in their transportation routing in order to avoid 'hot spots' that pose problems for security in transit. And supply chain managers will need to take into account higher transport costs, longer travel times and potential problems meeting schedules when alternative transport routes are used.

Additional security measures will result in increased transport times. Business models based on time-critical deliveries may be squeezed out of the market.

The need to re-design global supply chains due to security issues has a profound effect on transport times. It doesn't matter what the reason is – piracy, terrorism or other concerns – the outcome remains the same: a slowdown in global supply.

We've already discussed how political turmoil in Egypt has brought up concerns about a potential blockage of the Suez Canal, and the consequences that this could have for shipping.^{36,37} Other transport modes are facing slowdowns, too. One major example is the additional security measures imposed on the airline industry, which are resulting in increased transport times. According to a recent PwC survey, German executives responsible for air freight shipments are strongly in favour of more screening, but many believe there will be enormous costs as a result. One third estimate that the airline industry in Germany will face US\$ 284 million in additional costs due to higher security standards.³⁸ And another source estimates that new security measures which mean an additional half-hour per traveler in airports cost the American economy US\$ 15 billion per year.³⁹

The European Commission took a look at the correlation between increased travel times and greater costs due to new screening methods. Their calculation focuses on the indirect costs which occur when cargo consignment is delayed due to screening. The EC estimates that extended transit time would result in an increase in inventory costs and delays in delivery which together would amount to more than US\$ 9.34 million per annum in additional costs for the shipping company. And a two day delay could have severe consequences in the case of a just-in-time consignment which fails to meet the deadline.⁴⁰

The impact increases if you consider transatlantic shipments. There could be additional delays from longer dwell times when ships are waiting in port, increased turn-around time of feeder vessels or delays in inland transport modes delivering to different state boundaries. And that doesn't take into account potential shifts between transport modes.⁴¹ If additional security measures slow down global transport flows, business models might change too, as companies may struggle to adhere to just-in-time or time-definite delivery schedules. Transportation and logistics companies may find it difficult to predict when goods will arrive, especially in transatlantic shipments.

The majority of our Delphi panel expects there will be an increase in transport times. The experts of the concerned group are truly convinced that in '2030: Additional security measures have resulted in increased

transport times.' They see time as a more critical parameter for efficient logistics than cost. Increased security means additional time for verification, searches, audit and the like. The experts argue for the development of new performance criteria too. Once shipping times increase, logistics service providers may look to shift the focus from delivery times to other aspects of customer service. For example, they may develop new service offerings around 'secure' delivery. And delivery to countries facing a severe threat may become a specialised service that only some carriers are willing to offer. Nonetheless, time will still be a critical parameter for efficient logistics, so any security measures that companies implement will need to be as quick to execute as possible.

The relaxed group of Delphi panellists sees advances in technology and security techniques as counter-techniques to prevent a slowdown in global trade. They expect advanced technology developments to lead to simpler procedures like quicker security checks, or even safe lane procedures without additional interruptions. As global transport flows shift eastwards, though, not all countries worldwide may be able to adapt the necessary 'intelligent' solutions for security procedures quickly enough.

It will be essential for companies to handle security procedures effectively and efficiently. New kinds of customer services will develop which shift the focus away from the time factor.

Keeping cyber space safe

Cyber attacks inducing physical damage are an increasing threat for the transportation and logistics industry.

NATO believes that cyber attacks are the “battlefield of the 21st century”.⁴² IT systems are becoming more interdependent, as companies connect across their supply chains. While this increases information flow and efficiency, it also means that one successful cyber attack could have disruptive, unpredictable, devastating effects on other systems and companies and cause long-lasting consequences to economies.⁴³ Large economies such as the US and Germany have already established national cyber security divisions which are designed to counteract cyber attacks.⁴⁴

What can happen when one IT system breaks down? In 2004, a minor short-circuit hit British Telecom – with major consequences. Within minutes, 130,000 users’ telephone, fax and Internet systems broke down. 31 bank branches had to close since their connection to their data centre stalled, automated teller machines collapsed, and even emergency hotlines were inaccessible. The damage of this minor short-circuit was estimated at more than US\$ 7 million per day⁴⁵. What if this short-circuit had been induced by a cyber attack?

Since also large technology-leading companies, as Sony or Lockheed Martin, become victims of cyber attacks, how can logistics services providers protect themselves?

The damage which can be caused by cyber attacks isn’t only virtual. Cyber attacks can also cause physical destruction. That’s because information systems also control vital functions like air traffic control, so if commands cause

deliberate malfunctions major damage could be the result.⁴⁶

In 2002, a passenger plane of the Russian airline Bashkirian Airlines collided with a cargo aircraft operated by logistics service provider DHL close to Lake Constance. 71 people were killed in the crash. Investigations have revealed that the tragedy was caused by a problem in the telephone and computer system of Switzerland’s air traffic control.⁴⁷ Air traffic control was unable to recognise the impending collision. Claims for damage exceeded EUR 20 million.⁴⁸ What if hackers could manipulate air traffic control systems and cause similar events?⁴⁹ And it’s not only air traffic that is at risk. A collision of two cargo trains in 2010 caused economic damages of several million euros.⁵⁰ If criminals or terrorists gained control over the command systems of a major rail infrastructure operator, the consequences could be disastrous. And if cyber attacks stopped GPS systems from working, the negative impact on the transport and logistics industry could be immense.

Is the danger even greater than that posed by physical attacks? We asked the Delphi panellists for their views, and once again, opinions were sharply divided. Concerned experts believe that by 2030 cyber attacks may cause more damage than physical ones. In our 2011 *Global Information Security Survey*, PwC found that 20% of respondents had experienced financial losses from security events, 15% reported theft of intellectual property and 14% experienced compromises to brands or reputations.⁵¹ Relaxed experts consider it unlikely that damage from cyber attacks will exceed that from physical attacks. They argue that an increasing number of cyber attacks on supply chains would motivate the development of effective measures to minimise the potential for future cyber attacks and their negative consequences. While the number of cyber attacks is increasing, global spending on IT security is going up too. It's estimated to rise to US\$ 60 billion in 2014.⁵² By 2030 there may be adequate counter attack mechanisms in place to ward off cyber attacks.

Supply chains are increasingly dependent on ICT. In *Transportation & Logistics 2030, Volume 2: Transport infrastructure – Engine or hand brake for global supply chains?* we found that a variety of innovations in ICT are likely to maximise the capacity and effective use of transport infrastructure. As systems like flow control for highways and public transport are implemented, the potential damage that can be caused by cyber attacks rises dramatically, too. More frequent use of tracking and tracing systems and real-time control applications with web interfaces also provide new and growing weak points to be attacked by cyber criminals.

The increasing threat of cyber attacks for supply chains has motivated many high-tech suppliers to team up and to develop measures to fight cyber crime. Boeing, Cisco, IBM, Microsoft, NASA and the US Department of Defence are working to develop an internationally-accepted framework to secure supply chains from cyber attacks. The new standard should help prevent cyber criminals from introducing security vulnerabilities into IT equipment as it passes through the supply chain.⁵³

Companies will need to increase investments in security programmes and IT personnel to secure their technologies from cyber attacks and to minimise the risk of major incidents.

Sabotage and industrial espionage will affect supply chains, but competitors won't be the primary source of attacks.

A large number of attacks on supply chains, including thefts by employees or criminals outside of the organisation, are conducted for individual profit. But sabotage, industrial espionage and manipulation, carried out by competitors, represent another growing area in economic crime.

A recent study revealed that the number of attacks by competitors is underrated. Only 18.9 percent of almost 7,500 surveyed companies stated that they had at least one incident of industrial espionage within the last year. But more than four times as many – 80 percent – of the surveyed companies assume that there is a much higher level of espionage, just “not in my company”.⁵⁴

Logistics operations increasingly depend on ICT and attackers are increasingly using the Internet for this kind of crime. But our expert panel does not believe that the number of attacks on supply chains by competitors, for example in the form of sabotage, industrial espionage or manipulation, will increase until 2030. Instead respondents argue that the main trend in industry development is collaboration. According to the experts, competition is seen as healthy and as an important way to increase efficiency in the sector. As long as there are no significant changes in the global economy and its structure, the risk of being “named and shamed” will prevent companies from turning to crimes against competitors. One expert believes that there could eventually be a backlash, if a guilty company that isn't brought to justice causes a wave of revenge attacks.

While the experts do assume there will be an increasing number of attacks on

supply chains in the future, they argue that there's no evidence of such a trend for attacks induced by competitors. In PwC's *Global Economic Crime Survey*, the transportation and logistics industry reported the fifth highest number of fraud incidents out of more than 15 industries we investigated.⁵⁵ Most of these crimes fall under the categories of asset misappropriation, accounting fraud and bribery and are perpetrated by staff members, though. Sabotage and espionage aren't reported to be playing a prominent role for the transportation and logistics sector.

We should also note that cyber attacks are on the increase, and they often can't be traced back to their perpetrators. Today's sabotage, espionage and manipulation attacks may in many cases be classified as ‘cyber attacks’, rather than being counted as attacks made by competitors. Indeed, one expert notes that it may become increasingly difficult in the future to differentiate between an offense by a competitor and any other type of attack. Nevertheless, most experts expect competitors to focus their efforts on competing rather than resorting to such tactics. They assume more potential attacks will have other motivations.

Does this mean sabotage and industrial espionage are not an issue in the transportation and logistics industry? Typical victims of industry espionage are companies in industries where innovation and research and development are even more critical success factors than price or efficiency. Technological leaders in e.g. the automotive or pharmaceutical industry need to protect their product and production technologies, formulations and other kinds of know-how and innovation from competitors' attacks. Such incidents are still rare in transportation and logistics. But that may change as logistics operators continue to invest in innovation. Many are now developing and incorporating new technologies into their service offerings as a way to differentiate from the competition.

Sabotage and industrial espionage among competitors aren't key concerns for transport and logistics companies, although that could change as the sector becomes more innovative.

Concerns around data privacy are increasingly ignored in favour of greater security.

To keep global supply chains running smoothly, data containing information about individuals, companies, financials and goods needs to flow around the clock. Often data are shared and stored through web-based applications. Great technological progress has been made in logistics operations, with tracking and tracing systems using barcodes or RFID tags as well as GPS systems now being commonplace. These mean transportation and logistics companies and their customers can now retrieve background information of a shipment at every step in the supply chain and identify its location. But the same data that provides transparency for legitimate users can also attract cargo thieves, who are now using the Internet to track shipments, book transportation with legitimate motor carriers, or, conversely, to set up bogus trucking operations that arrange cargo pick-ups for legitimate shippers and forwarders.⁵⁶ Transportation and logistics companies need to step up efforts to thwart such schemes; as we've already noted, cyber attacks are one of the fastest growing areas in crime.⁵⁷

Modern screening and surveillance systems are fast, convenient and anonymous – and those same qualities also make them likely candidates for a cyber attack. In passenger transportation, travelers are used to x-ray screening, camera observation or permitting detailed access to their personal data. If these systems were hacked, the damage could be severe. The global market for surveillance and security equipment is already estimated at US\$ 80 billion (2010), and is growing at a compound annual growth rate of 11.7%.⁵⁸ London already uses more than 10,000 crime-fighting CCTV cameras and Paris aims to establish more than 13,000 cameras by the end of 2011 in order to improve video surveillance and to reduce crime rates.⁵⁹

Such security measures walk a fine line between protecting the public and invading individual privacy. The question is to what extent will people and corporations be willing to sacrifice their rights of privacy and liberty in exchange for potentially safer and more secure travel? What's the trade-off between privacy and security for individuals?

Other recent studies have also shown that many individuals are willing to pay for security improvements, even though they imply a loss of data privacy. This suggests that many people prefer higher security standards to keeping personal data private.⁶⁰ And the next generation of business leaders will bring with them different expectations about data privacy after having grown up with web-based social networks, such as facebook, myspace or twitter.

The Delphi panel foresees that definitions of 'privacy' will become looser in favour of better protection, particularly where individuals are concerned. While many would prefer to maintain data privacy, they are ready to sacrifice it when there's a documented need, such as preventing terrorist attacks. For individuals, data privacy is a personal issue. But in supply chain management, the issue is more about the relationship between commercial entities, rather than data on individuals. Some experts raise concerns that the public won't raise issues around data privacy until they begin to be confronted with negative aspects of security measures, such as permanent surveillance. They see the need for new technological systems and enhancements which ensure the confidentiality of data while at the same time not jeopardising security and trade.

Organisations need to learn how to handle private data more respectfully. However, individuals will be willing to share private data if it serves security improvements.

Investing in a more secure future

Increasing security means cranking up investment, but the returns are many.

Enhanced security measures mean higher costs. The direct economic losses caused by the 9/11 terrorist attacks amounted to tens of billions of dollars, but the costs of the enhanced security measures which followed were far higher.⁶¹ The budget for the US Department of Homeland Security is approaching US\$ 50 billion per year, and state and local governments are spending billions on security as well. The direct costs are just the beginning. A private-sector analysis conducted by the International Monetary Fund (IMF) found that businesses spent US\$ 1.6 billion per year on higher security costs. The extra financing burden of carrying 10% higher inventories had an even steeper price tag, at US\$ 7.5 billion per year.⁶² And additional safety measures also create a range of opportunity costs that might not always be immediately apparent for transportation and logistics companies, i.e. costs incurred through longer transport times, longer dwell times and increased turnaround times.

Many companies have not yet invested in improving security beyond the minimum level due to difficulty in justifying security investments.⁶³ Companies may not yet see the benefits of enhanced security or may be unable to make an adequate business case for security implementation. That's because penalties for non-compliance with new security standards are minimal or non-existent – and the benefits are hard to measure.⁶⁴

However, supply chain security management is not a black hole. We believe that secure supply chains do provide a return on investment for transportation and logistics companies. Research has quantified the tangible

business benefits of investing in supply chain security efforts. Areas positively influenced by security efforts include supply chain visibility (50% increase in access to supply chain data, 30% increase in timeliness of shipping information), improvements in inventory management (14% reduction in excess inventory, 12% increase in reported on-time delivery), more efficient customs clearance processes (49% reduction in cargo delays, 48% reduction in cargo inspections/examinations) and in the long-term benefiting the customer relationship (20% increase in new customers and 26% reduction in customer attrition).⁶⁵

When evaluating the thesis ‘2030: Security has become one of the most important cost drivers for logistics’ the Delphi panel was split up again. One group of experts regards security spending as purely a cost factor. They take a fairly narrow view, where higher levels of security simply mean increased costs. The other group considers security spending more broadly, seeing it as an investment in business operations. They argue that investments in additional security will have a return, since they reduce costs associated with theft and smuggling. They also enhance delivery reliability, which leads to better customer relationships, another important form of return on the original investment. So security strategies should be seen as proactive loss prevention incorporating a positive return on investment.

Well-planned security investments provide a payback not only in terms of loss prevention, but also by enhancing supply chain performance.

It’s not enough to just react to crisis situations. Organisations need to take preventive action to mitigate security risks.

Extreme supply chain disruptions or emergencies, like the catastrophe in Japan, the Deepwater Horizon oil rig explosion in the Gulf of Mexico or the 2010 Haiti earthquake, where entire supply networks throughout a region collapsed, get the most attention. But supply chain disruptions happen on a day-to-day basis, too, and these more common-place incidents also affect logistics systems and economies. The average loss per cargo theft has been calculated to be around US\$ 4 million.⁶⁶ And pirate attacks alone cost the global economy between US\$ 7 billion and US\$ 12 billion per year.⁶⁷

The financial cost of such disruptions is only the tip of the iceberg. Supply chain failures and disruptions can also cause a host of other negative consequences. If consumers lose confidence in a company’s brand, the ramifications can be far-reaching. That’s why consumer concerns are driving enhanced security initiatives. Logistics services providers which guarantee on-time delivery may also be especially vulnerable to the negative effects of disruptions, but all transportation and logistics companies need to establish crisis management procedures. That means having appropriate response plans for various service level disruptions that go into effect immediately in the case of a crisis. It’s important to cover all the bases, including putting plans and checklists in place and training response teams which are available when needed.

We asked our Delphi panel if in ‘2030: Strategies to cope with emergencies are a more effective means of dealing with supply chain disruptions than preventive measures.’ Their answer? – A resounding no. Reactive solutions are no longer seen as adequate to the challenges of keeping global supply chains running smoothly. Several experts point out the costs of supply chain disruptions are too high and unpredictable and that consequences can be far reaching, e.g. the record billions required for clean-up and compensation efforts following the Deepwater Horizon incident. They believe prevention efforts need to be in place which also includes mitigation plans for potential emergencies. A proactive approach leads to better decision-making and service provision. And investments in proactive measures can also help companies negotiate reduced rates on insurance.

Many experts note that reactive and preventive solutions cannot be analysed apart from each other. Security strategies generally combine preventative and responsive measures. Supply chains are complex, and some transportation and logistics players operate across the world and in multiple segments, making a purely preventive approach costly to implement. The combination of both measures is key.

Companies have to find the right combination of preventive and reactive measures to achieve the optimal level of supply chain security.

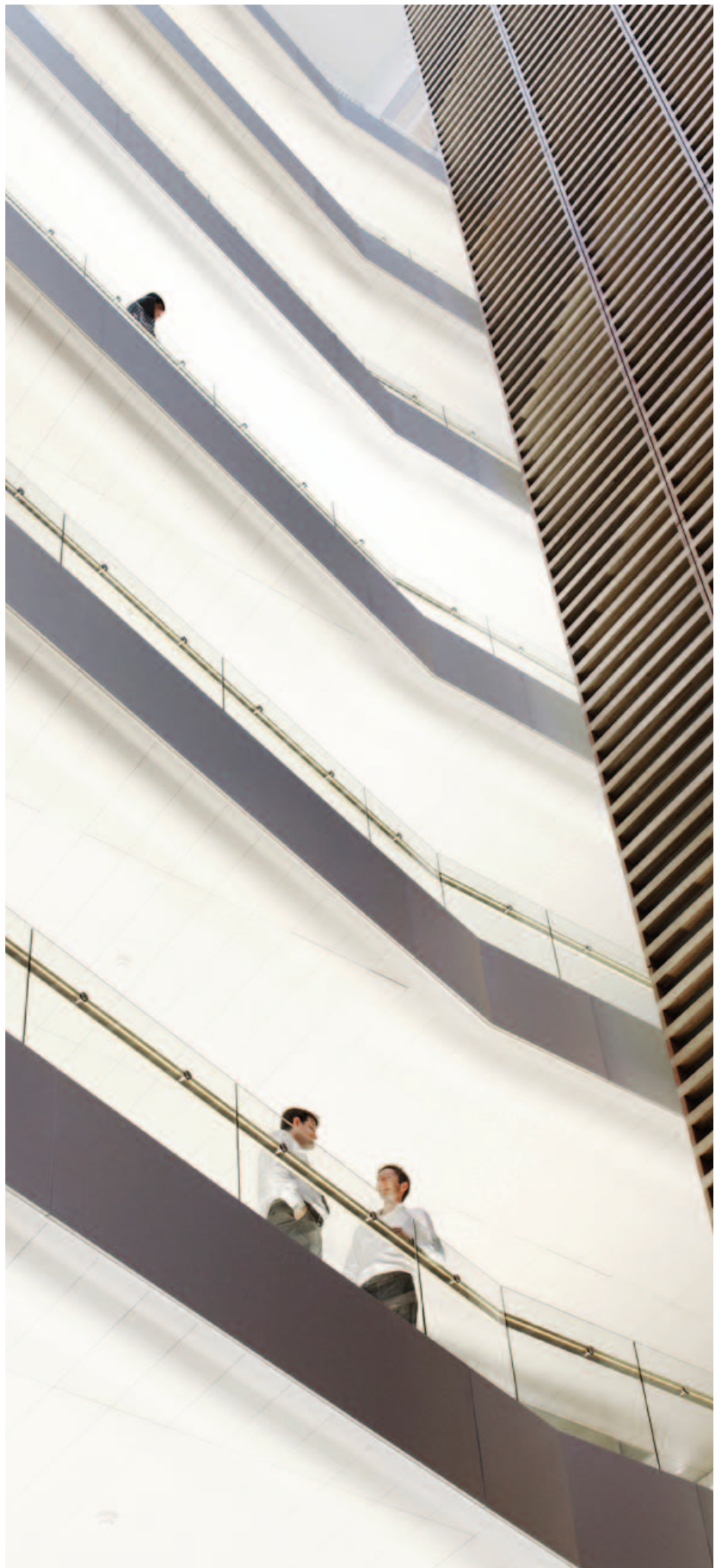
Governments reduce their executive power and focus on their legislative roles. Transportation and logistics companies embrace the opportunity to improve their own security measures on their own terms.

Most companies and governments recognise the need to implement comprehensive and integrated end-to-end security that extends beyond asset protection. This has led to the implementation of diverse security initiatives, including required statutory standards and voluntary industry efforts, in order to minimise the weaknesses of supply chains and to raise general security levels.

Some of the initiatives taken by the US government to assess and minimise the risk involved in international transportation of goods, include, amongst others, the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), the Advanced Manifest Rule (AMR)/ Advanced Cargo Information (ACI) and the Free and Secure Trade initiative (FAST).⁶⁸

Multiple security initiatives are also taking place outside the US as well. These include the development of the Framework of Standards to Secure and Facilitate Global Trade by members of the World Customs Organization (WCO). This series of measures were presented by the European Commission to accelerate implementation of the WCO Framework, including the Authorized Economic Operator (AEO) programme, as well as various initiatives that were taken by the World Trade Organization (WTO) to better facilitate trade.⁶⁹

In addition to these government initiatives, businesses have also been proactively seeking ways to mitigate supply chains risks. The Transported Asset Protection Association (TAPA) has established an objective of reducing losses from international supply chains. TAPA is looking to establish consistent freight security requirements for transportation and logistics companies.⁷⁰ The International Standards Organization (ISO) has also issued the standard ISO/PAS 28000, outlining the requirement to implement a security management system in an organisation, including those aspects critical to security assurance in the supply chain.⁷¹



One necessary element is a comprehensive risk analysis which analyses high risk goods and processes and is able to answer the question: 'Who and what should be protected against whom or what and through which means?' That means understanding the respective roles of government bodies and transportation and logistics companies. While governments are the ones developing and setting regulatory frameworks, transportation and logistics companies are the ones executing them. Security requirements need to be aligned with the business operations of transportation and logistics companies, e.g. take into account and try to minimise potential efficiency losses due to additional costs for congestion, intermediate warehousing or delivery delays. One positive example is the US Container Security Initiative (SCI) and the 'SAFE' framework of the World Customs Organization (WCO) since they identify and control high risk goods and initiate preliminary notice without impeding the flow of goods.

Who will take the lead in ensuring supply chain security in 2030? According to our Delphi panel, probably not the government, although they'll define processes regulate standards and are responsible for setting up legal frameworks. Execution will remain the responsibility of the private sector, since financial constraints limit governments' abilities to take over this function. Some experts also note that the sheer size of cargo volumes in some countries will be too large to be controlled by one institution. The experts also point out that it may be easier for transportation and logistics companies to manage security costs since they can factor them into the final product price. If the government were to take over the execution of supply chain security, special charges might need to be introduced, adding an additional layer of bureaucracy. The Delphi experts see such a shift as unlikely. Some also believe that security management offers lucrative opportunities to drive revenues in a high-margin business. Private companies will try to keep it in their responsibility and more private players may look to enter the market in the future.

Companies which have to execute security standards should work together with governmental institutions to represent their own interests. That will help security standards become not only effective, but efficient.

No supply chain will ever be 100 percent secure. Technology can help increase security, but people are the critical link.

Enhancing security levels is a major priority for governments and companies and the reliance on technology is continuously growing. After the recent parcel bomb discoveries, the US Department of Homeland Security initiated the design and application of active interrogation, a non-intrusive inspection system for air cargo that costs around US\$ 14 million.⁷² New systems allow threatening materials, weapons, drugs and currency to be detected and identified automatically, even in concealed shipments. Another promising development is 'voiceprint' technology. A technique similar to fingerprints should allow law enforcement agencies to electronically match a voice to its owner.⁷³

The defence industry may have some lessons to share with transportation and logistics companies more broadly too. NATO has conducted research to increase the protection of harbours and ships, including the development of a range of technical equipment including sensor nets, electro-optical detectors, rapid reaction capabilities and unmanned underwater vehicles.⁷⁴ These technologies have clear applicability for non-military use as well. Other key research areas include the development of an airborne early warning system and control mechanisms that use infrared transmitters to initiate necessary counter measures when aircrafts are under attack.⁷⁵

The global security market is growing fast. Between 2005 and 2009 the global value of security technology has more than doubled, reaching US\$ 946 million in 2009.⁷⁶ In the US, the Department of Homeland Security will administer a budget of US\$ 42.3 billion in 2012 and some legislators proposed raising it still further. The US Transportation Security Administration received a budget increase of US\$ 8.2 billion in 2011, mostly to fund a range of technology devices like explosive detection systems, portable explosives trace detection devices and whole body scanners.

This broad implementation of security technology is not without its critics. Some observers question the return on investment of technology and its real contribution to higher security levels. Technological improvements still can't prevent all supply chain disruptions or interruptions. As security technologist Bruce Schneier puts it: "Stop trying to guess. You take away guns and bombs, the terrorists use box cutters. You take away box cutters, they put explosives in their shoes. You screen shoes, they use liquids. You take away liquids, they strap explosives to their body. You use full-body scanners, they're going to do something else."⁷⁷

Can we rely on the 'magic' of technology to create 100% security against supply chain sabotage? Are there other options – and what might they be? Measures based on trust or expert knowledge of human behaviour? The airport of Tel Aviv, reported to be one of the most secure airports worldwide, seems to have found an effective strategy which relies on both human intervention and technology. The security personnel concentrate most of its efforts on personal contact and try to engage at least once with each passenger. Decisions as to whether a passenger is allowed to continue to check-in or needs to be interviewed in depth are based on analysis of behaviour.⁷⁸ In addition to this, the airport implements the newest technology available.

Will technology be the best way to guarantee security by 2030? Our Delphi panel has mixed views once again, with concerned and relaxed experts again showing markedly different responses. For the concerned, technology is the best solution and the way to move forward in supply chain security management. Some even prefer to replace personnel-intensive solutions with electronic monitoring devices, 'hack-proof' systems and other technologies allowing a broader coverage. This group sees the human factor as being the weakest link in the chain historically and remaining so in the future. Their solution is to substitute technological equipment wherever possible.

The relaxed experts attribute a much lower probability to technology as the only reliable lever to guarantee security. They see the future in a combination of technology, trained personnel and policies. This group argues that even the most state-of-the-art technology currently in place doesn't prevent successful attacks on supply chains from happening.

Technology alone can't secure the supply chain. People are needed too, to provide human intelligence and good governance.

Security audits along the entire supply chain are a requirement to maintain effective levels of security.

Global trade is no longer just about moving goods quickly and efficiently, it is also about moving goods securely. As many as 25 different parties are involved in the global movement of just one container⁷⁹. The chain encompasses different representatives of buyers, sellers, inland freighters, shipping companies, intermediaries, financiers, governments, and the list goes on. With so many different supply chain operators involved, the risk of supply chain disruptions and vulnerability to external intervention increases.

A supply chain is only as strong as its weakest link. One supply chain partner may have excellent internal security efforts, but if others in the supply chain are lacking adequate security efforts, or if there isn't sufficient coordination between supply chain partners, those efforts may be for naught.⁸⁰ Supply chain security management needs to be all-encompassing and supported by all players in the supply chain. Long-term cooperation with supply chain partners is a necessary first step, but securing the supply chain will require an even greater commitment. We believe that a supply chain security strategy which is cross-institutional and international, including all players of the supply chain is absolutely critical.

How can you control and verify that supply chain partners are keeping their end of the bargain? Security audits are one valid option. Several companies already offer such a service to their customers, based on C-TPAT requirements or individually developed checklists addressing both physical and personnel security.^{81,82} Companies will need to tailor systems to their individual needs, though. Those who only complete the minimum obligatory requirements are unlikely to have effectively secured transport services and logistics from disruption. Transportation and logistics companies also need to include crisis management and contingency planning for man-made catastrophes, as well as natural ones.

What will the regulatory situation in 2030 look like? Will security audits be compulsory along the whole supply chain, from raw material delivery up to point of sale? This time the answer from our Delphi panel is an emphatic yes – and the experts see that as a good thing. They rated this thesis with both highest probability and the highest desirability scores.

The experts note that a move towards security audits has already begun, as reflected by trusted shipper elements in supply chain security. Those shippers almost certainly require some type of auditing. The question some pose is not whether audits will happen, but rather whether the trusted shipper concept will reach back as far as the raw material stage. The trend towards government-mandated security programmes is another sign that audits will be one of the main measures to provide international and national security. Though the Delphi panel believes that security audits will be implemented, they argue for individual customisation. That means analysing the specific nature of the threat involved, which differs among industries. The Delphi panel argues that security audits might become obligatory only for certain commodities, and for certain shipping methods, e.g. aviation. But protection of the vast majority of commodities will remain to be seen. It's important to remember that a very high audit check could hamper trade and have a significant financial impact. That means developing a system where the weakest links in the supply chain get the most attention makes good sense.

Companies should work together with standard setters to develop generally accepted security principles.

Wildcards



Expect the unexpected

In the previous chapters of this study we've taken a systematic look at the future and have identified a number of trends that look likely to continue. Surveying a group of experts by using the Delphi method helps identify the probable outlook for the transportation and logistics industry. These views can help decision makers to make appropriate decisions and to prepare their organisations for future developments.

We believe that any 'look into the future' should not be limited to the most probable scenarios though. Unlikely events do sometimes happen – and can have a huge impact on both society and the economy. Such low-probability, high-impact events can be termed 'wildcards'. Sudden and unique events may represent the turning point of long-term trends, or even of an entire social system – as in the fall of the Berlin Wall in 1989. Their occurrences may happen at any time and are difficult to predict, and the potential impact may be enormous.

And while it's impossible to consider all possible wildcards – their number is literally endless – it is possible to identify some of the areas where wildcards could occur. Take the eruption of the Eyjafjallajökull volcano in 2010. While it came as a surprise and was highly disruptive, the possibility of volcanic activity in the region had long been noted. Or the terrorist attack of 9/11 which shook the world and transformed the notion of "homeland security." The specific type of attack was a shock, but the increasing anti-American sentiment behind it had been building in the Islamic world for quite some time.

That's why organisations need to understand their business environment, and the social and economic systems in which they operate. Careful observation can often turn up early indicators that a wildcard might be in the offing. And good planning is nearly always more effective than scrambling to react after the fact.⁸³

For transportation and logistics companies, supply chain security is one area where we think there are a number of potential wildcards that should already be on companies' radar. Our list of suggestions is only a starting point. They are designed to prompt you to think about how such events might affect your organisation. What would the financial consequences be? How vulnerable is your business model? How quickly can you adapt?

Most wildcards have potentially disastrous impacts, but it is important to remember that some wildcards may actually change the course of the future in a positive way. In those cases, too, good planning will mean making the most of the new status quo.

The detonation of a 10-20 kiloton weapon in a major seaport could cause damage of \$50 to \$500 billion

Source: CRS Report for Congress (2005)
Terrorist Nuclear Attacks on Seaports:
Threat and Response

What if terrorist attacks shut down logistics networks?

Logistics networks are the backbone of the global supply chain. That means disruptions could slow down national economies, making them potentially a preferred target for terrorist attacks. Important hubs, such as seaports and airports, could be shut down by physical aggression. Bridges or tunnels are also potentially vulnerable, since there often isn't a viable alternative way to cross from one land mass to another. Attacks on these targets could slow down traffic massively, or possibly bring it to a complete standstill on a given route.

Signs that you need to start taking notice:

- Increasing religious conflicts
- Increasing imbalance of wealth

How could it affect your business? A self-assessment checklist.

What would be the financial consequences? ☐ Minimal ☐ Moderate ☐ Disastrous

How vulnerable is your business model? ☐ Weak ☐ Stable ☐ Resilient

How quickly can you react? ☐ Tomorrow ☐ Next Month ☐ Next Year

How could it affect your business? A self-assessment checklist.

Signs that you need to start taking notice:

- Increasing number of terrorist attacks
- Increasing number of natural disasters

What would be the financial consequences? ☐ Minimal ☐ Moderate ☐ Disastrous

How vulnerable is your business model? ☐ Weak ☐ Stable ☐ Resilient

How quickly can you react? ☐ Tomorrow ☐ Next Month ☐ Next Year

What if insurance companies stop covering major risks?

Shippers have to pay tens of thousands of dollars a day in extra “war insurance” to cross dangerous routes

Source: Wall Street Journal (2009)
Piracy Causes Changes in Routes, Insurance

The financial crisis and global recession in 2008 and 2009 hit insurance companies hard, and many were forced to raise their fees. Many transportation and logistics companies have had to pay a high premium to cover possible risks to their assets and cargo. In the future, insurance companies might refuse to underwrite some types of large risks – for example damage resulting from natural catastrophes, or from terrorist actions. If transportation and logistics companies are no longer able to offset risk through insurance, logistics costs might soar.

How could it affect your business? A self-assessment checklist.

What would be the financial consequences? ☐ Minimal ☐ Moderate ☐ Disastrous

How vulnerable is your business model? ☐ Weak ☐ Stable ☐ Resilient

How quickly can you react? ☐ Tomorrow ☐ Next Month ☐ Next Year

Signs that you need to start taking notice:

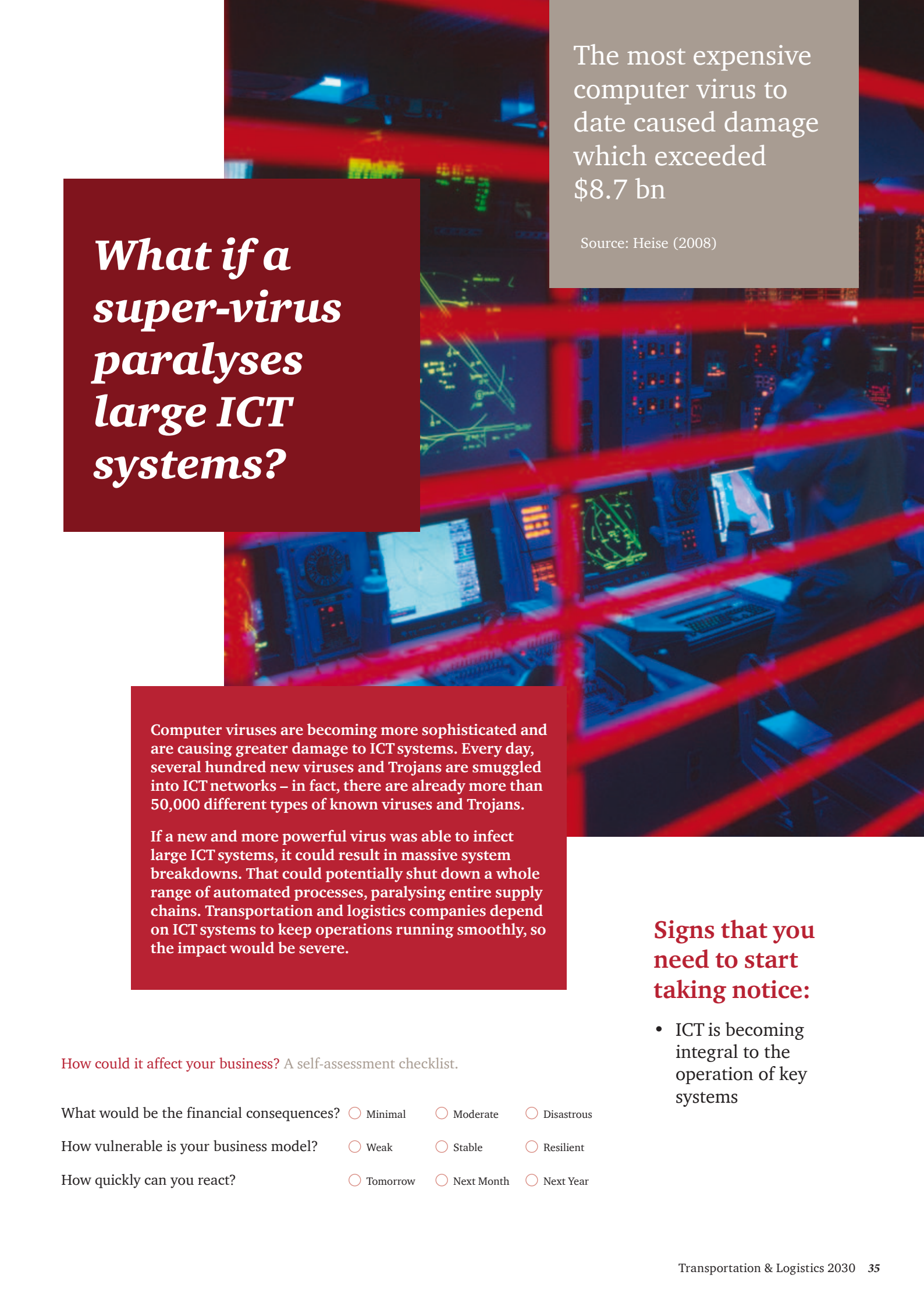
- Key transit points privatised or controlled by states with high deficits

What if key transit points are blocked?

A large portion of total world trade passes through important transit points such as the Panama Canal, the Suez Canal and the Strait of Malacca. In 2008, a total of 21,415 vessels with a total value of more than US\$ 5 billion passed the Suez Canal. Today the access to such transit points is almost unrestricted. If access to important trade routes were limited or made prohibitively expensive by operators, it could have severe consequences for global trade. There are also a number of regional examples that would have a more limited, but still significant impact. The recently finished Gotthard Base Tunnel lets standard freight trains pass under the Alps. That will mean a major advantage to shippers – as long as it remains available for use at a reasonable cost.

7.5 % of world sea trade is carried via the Suez Canal

Source: Suez Canal Authority (2010)



What if a super-virus paralyses large ICT systems?

The most expensive computer virus to date caused damage which exceeded \$8.7 bn

Source: Heise (2008)

Computer viruses are becoming more sophisticated and are causing greater damage to ICT systems. Every day, several hundred new viruses and Trojans are smuggled into ICT networks – in fact, there are already more than 50,000 different types of known viruses and Trojans.

If a new and more powerful virus was able to infect large ICT systems, it could result in massive system breakdowns. That could potentially shut down a whole range of automated processes, paralysing entire supply chains. Transportation and logistics companies depend on ICT systems to keep operations running smoothly, so the impact would be severe.

Signs that you need to start taking notice:

- ICT is becoming integral to the operation of key systems

How could it affect your business? A self-assessment checklist.

What would be the financial consequences? ☐ Minimal ☐ Moderate ☐ Disastrous

How vulnerable is your business model? ☐ Weak ☐ Stable ☐ Resilient

How quickly can you react? ☐ Tomorrow ☐ Next Month ☐ Next Year

New computer systems will operate with more than 10 quadrillion operations per second – and crack any password?

Source: IBM (2011)

What if cryptography doesn't work anymore?

Cell-phones, Internet protocols, email conversations and many more communication processes are based on cryptography that prevents unauthorised parties from monitoring conversations. But what if new super computers are powerful enough to crack any cryptography system or password within seconds? Communications in the transportation and logistics industry, customer data, transport routes, freight content and further confidential data would be accessible to competitors, criminals, and other unauthorised parties.

Signs that you need to start taking notice:

- Computer systems are getting exponentially faster

How could it affect your business? A self-assessment checklist.

What would be the financial consequences? ☐ Minimal ☐ Moderate ☐ Disastrous

How vulnerable is your business model? ☐ Weak ☐ Stable ☐ Resilient

How quickly can you react? ☐ Tomorrow ☐ Next Month ☐ Next Year

How could it affect your business? A self-assessment checklist.

What would the financial benefits be?

☐ Minimal ☐ Moderate ☐ Significant

How adaptable is your business model?

☐ Set in Stone ☐ We can change, but it takes effort ☐ Flexible

How quickly can you react?

☐ Tomorrow ☐ Next Month ☐ Next Year

Homeland Security
is testing the next
generation of
security screening
— a scanner that
can read your body's
signals and sense
your intentions

Source: CNN (2008)

***What if you
know about
the crime
before it
happens?***

Terrorist attacks are a major social and economic threat. They're difficult to predict. But what if security systems could recognise the signs someone gives off when he or she is planning to commit a crime? If these new high-tech security scanners were installed at airports or in the camera surveillance system of a city, security could become much more effective. Crimes could be prevented before they occur.

Opportunities



How to optimise your security profile

So what can you do to stress-test and improve your supply chain security? In this chapter, we take a comprehensive look across five dimensions of supply chain security (see Figure 7):

- Personnel security
- ICT security
- Process security
- Physical security
- Supply chain security partnerships

and offer suggested activities for each area, supported by a key performance indicator (KPI) and the time horizon for when the activity could be put into practice.

Some areas we highlight will be most relevant for customs, law enforcement officials and governmental regulatory bodies, others may apply more to private sector businesses spanning the supply-demand network, including tiered suppliers, 3rd party service providers, OEMs and customers. But everyone will need to work together.

As a result of a generally increased focus on improving security, advanced technology to monitor and ensure the security of global trade flows has been refined and improved. Some governments have passed tighter security regulations and in some cases new standards have also been developed. These include the

establishment of the supply chain security standard ISO 28000, the 24 Hour Advanced Manifest Rule, Authorised Economic Operator and C-TPAT certifications, as well as joint cooperation between international military and private shipping firms sailing in high risk international waters (combating piracy). Most recently, the US has passed legislation introducing a 100% scanning requirement for all US bound maritime cargo. The European Commission is currently assessing a similar endeavor. These regulations and technologies can be viewed as today's state of the art in the field of supply chain security. These initiatives are likely to continue in the future and could develop into other opportunities.

What might such opportunities look like? There is a wide range of possibilities for improving supply chain security. On the following pages, we sketch out a range of possible options. Our list is not exhaustive, and not every activity will be a good fit for every organisation, particularly as existing legislation varies around the world. It should, however, serve as a pragmatic starting point for thinking creatively about how you can optimise your security profile. It can also help promote discussion with supply chain partners about how to work together to improve the security of shipments throughout the entire supply chain.

Figure 7: Dimensions of the supply chain security profile



Personnel Security			
Security dimension	Activity	KPI	Time horizon
Risk Profile	Risk profile set up for job applicants and employees ⁸⁴	Percentage of screened job applicants and employees	2015 - 2020
	Risk profile follow up: regular interviews with employees, annual police clearance certificate	Percentage of screened employees	2020 - 2025
	Drug testing for employees at regular intervals (on-demand)	Drug consumption, alcohol level etc.	2020 - 2025
	Continuous surveillance of employees in private and public	Percentage of employees observed	2025 - 2030
Security Training	Annual supply chain security training for employees	Percentage of employees who participated in trainings; days of participation	2011 - 2015
	Surprise drills for security preparedness	Number of surprise drills; percentage of employees involved; percentage of failed surprise drills	2020 - 2025
Security Guidelines	Security code manual for employees	Existence; level of familiarity	2011 - 2015
	Whistle blower management policy, hotline	Number of security related whistle blows	2015 - 2020
ICT Security			
Security dimension	Activity	KPI	Time horizon
Security Enabling Technologies	Sensor and actuator solutions for transportation assets	Percentage of supply chain activity covered by sensor and actuator solutions	2015 - 2020
	GPS, Zigbee connectivity with transport assets	Percentage of supply chain activity covered by GPS	2020 - 2025
	Ubiquitous RFID tags (active and passive)	Percentage of supply chain activity covered by RFID	2020 - 2025
	Analytic sourcing tool for supplier risk, inspection at source and security	Number of suppliers that are screened and monitored through the sourcing tool	2015 - 2020
	Intelligent, real time SCM security event management applications ⁸⁵	Number of intelligent applications used for decision making for core end to end supply chain	2025 - 2030
	Supply chain security robotics ⁸⁶	Number and functional depth of security robots in a facility	2025 - 2030
Vulnerability Check	Computer based simulations on supply chain security disruptions and vulnerabilities	Results of corresponding test	2015 - 2020
	Artificial intelligence applications for risk analysis and targeting for global shipments	Results of corresponding test	2015 - 2020
	Ubiquitous test attacks on ICT system	Number of successful attacks	2011 - 2015
Accessibility	Worldwide information sharing of high risk shipments between customs and law enforcement authorities	Performance results of tests conducted by external auditors	2015 - 2020
	Encryption, protective firewall and coding of information	Benchmark with leading technologies, scripts, etc	2011 - 2015
Process Security			
Security dimension	Activity	KPI	Time horizon
Transport Security	Real-time re-routing of ships sailing in dangerous waters based on GPS signal	Number of piracy threats avoided	2020 - 2025
	Armed crew members and special armoury stations in transportation assets	Number of armed crew and armouries of members on a ship, aircraft or rail asset	2015 - 2020
	Insurance of transported goods when appropriate	Percentage of goods insured	2011 - 2015
	Record of employees activities in product construction process	Percentage of value-adding processes that can be traced back to the respective employee	2015 - 2020
Handling security	Automated dispatch operations validation check	Percentage of automated checks within dispatch operations	2011 - 2015
	Automated receiving operations validation check	Percentage of automated checks within receiving operations	2011 - 2015
	Screening of goods between the various supply-chain steps	Percentage of goods being screened	2015 - 2020

Physical Security			
Security dimension	Activity	KPI	Time horizon
Inventory security	Inventory verification	Percentage of supplies being screened	2011 - 2015
	Safety stock levels	Percentage of inventory as buffer to suppliers and customers	2011 - 2015
	Surprise stock counts	Number of variance analyses conducted per year	2011 - 2015
	Insured inventory	Percentage of inventory covered by insurances	2011 - 2015
Access control	Biometrics and personalised access control for personnel	Percentage of supply chain activities supported by biometrics or personalised access control	2015 - 2020
	Specially designed locations within the logistics facility	Size of fully secured space within the logistics facility	2011 - 2015
	Intelligent camera systems with 3D facial recognition for identifying theft and pilferage	Number of intelligent cameras installed in a premises	2025 - 2030
	Controlled access to restricted areas or goods	Percentage of personnel that have access to restricted areas or goods	2015 - 2020
Transport equipment	Sealing of loading units	Percentage of loading units being sealed	2011 - 2015
	Electronic seal / smart containers / intelligent transport assets	Percentage of containers equipped with electronic seal	2015 - 2020
	Development of specially designed secure transport assets ⁸⁷	Percentage of specially designed secure transport assets in fleet	2020- - 2025
Security Partnerships			
Security dimension	Activity	KPI	Time horizon
Partnerships with suppliers	Supplier security certifications mandatory	Percentage of suppliers which have been certified	2015 - 2020
	Ability to substitute suppliers	Time required to shift from one supplier to another	2011 - 2015
	Full visibility over tiered supply network (suppliers' suppliers)	Percentage of suppliers revealing their suppliers; percentage of suppliers from high-risk countries	2015 - 2020
	Ability to track and trace value-adding processes of suppliers	Percentage of goods tracked while in supplier processes	2015 - 2020
	War-gaming practice	Performance in war-gaming exercises	2015 - 2020
Partnerships with standard setters and authorities	100% compliance with AEO/C-TPAT requirements	Number of supply chain partners that are 100% AEO/C-TPAT compliant	2011 - 2015
	ISO 28000 mandatory	Number of supply chain partners with ISO 28000 designation	2015 - 2020
	Centralised data repository for all cargo shipments and 100% of all global trade shipment in the central data repository	Percentage of shipment data flowing through the central data repository	2015 - 2020
SCM security standard development and implementation	Risk identification and analysis	Percentage of covered/insured risks	2011 - 2015
	Contingency planning	Number of prepared contingency plans	2011 - 2015
	Post crisis management	Time required to react to interruptions	2015 - 2020

Methodology



RealTime Delphi Innovation

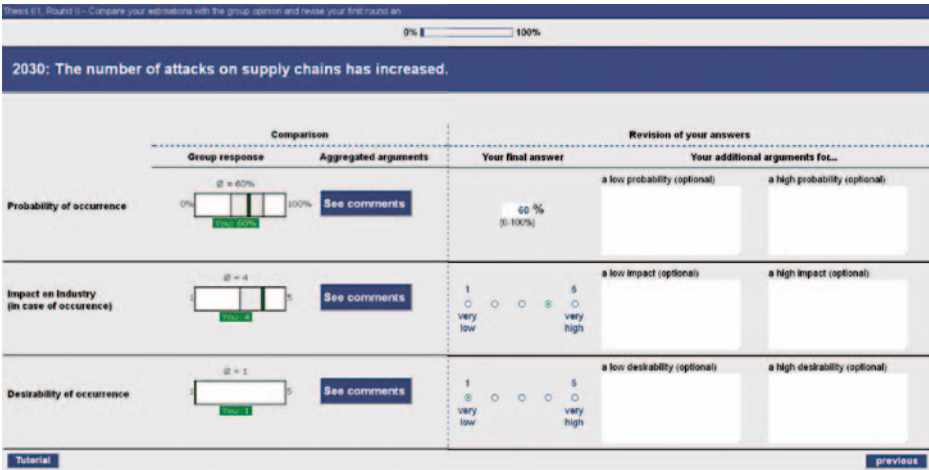
In this fourth volume of *Transportation & Logistics 2030* we continue to use a methodology of futurology known as the Delphi technique. Working together with the Center for Futures Studies at the Supply Chain Management Institute (SMI), we were able to use an improved version of the Delphi methodology, which we believe brings significant advantages for both surveyed experts and the monitoring team.

The classic Delphi technique was developed at US RAND Corporation in the 1950s. Their goal was to overcome some of the weaknesses that group studies often suffered from, for example, the ‘bandwagon’ effect, where group members follow the lead of the majority, or the ‘halo’ effect, where group members follow the lead of someone who they think is the most knowledgeable expert. Instead, they wanted to systematically develop expert opinion consensus about future developments and events.

The usual Delphi forecasting procedure takes place in the form of an anonymous, written, multi-stage survey process, where feedback of group opinion is provided after each round. We designed our Delphi as an Internet-based, almost real-time survey.⁸⁸ The use of an Internet survey form (RealTime Delphi) that provides immediate feedback streamlines the classical procedure. It makes the process more interesting and convenient for the surveyed experts, who can see data trends immediately. Using this technique, we were also able to automate much of the data analysis.

Based on extensive desk research, expert consultations, and workshop sessions, PwC and SMI developed 14 theses around the future of supply chain security (see overview of theses in Figure 12). Panellists rated each thesis' probability of occurrence (0-100%), the impact on the transportation and logistics industry if it occurred (5-point-Likert scale) and the desirability (5-point-Likert scale). They were also given the option to provide supporting arguments for all answers. Once a panellist finished giving answers for the first round, the statistical group opinion of all participants was calculated immediately. Panellists were then shown a second round screen (see Figure 8). The final results of the RealTime Delphi survey formed the framework to analyse future opportunities. Our team conducted additional expert workshops, where we used both the extensive qualitative survey data and the results of desk research to better understand future trends.

Figure 8: RealTime Delphi screen

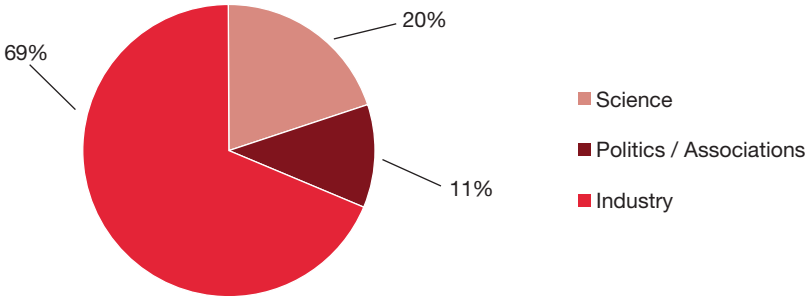


Delphi Panel

The objective of Delphi studies is not to obtain a representative sample of a population, as with most conventional surveys. Rather, Delphi research aims for a high inclusion of expertise. Our panel included a significant number of experts from business, mainly C-suite level executives and decision makers from global companies. Key criteria for our selection of RealTime Delphi participants were industry and educational background and work experience, as well as function in and outside the organisation.

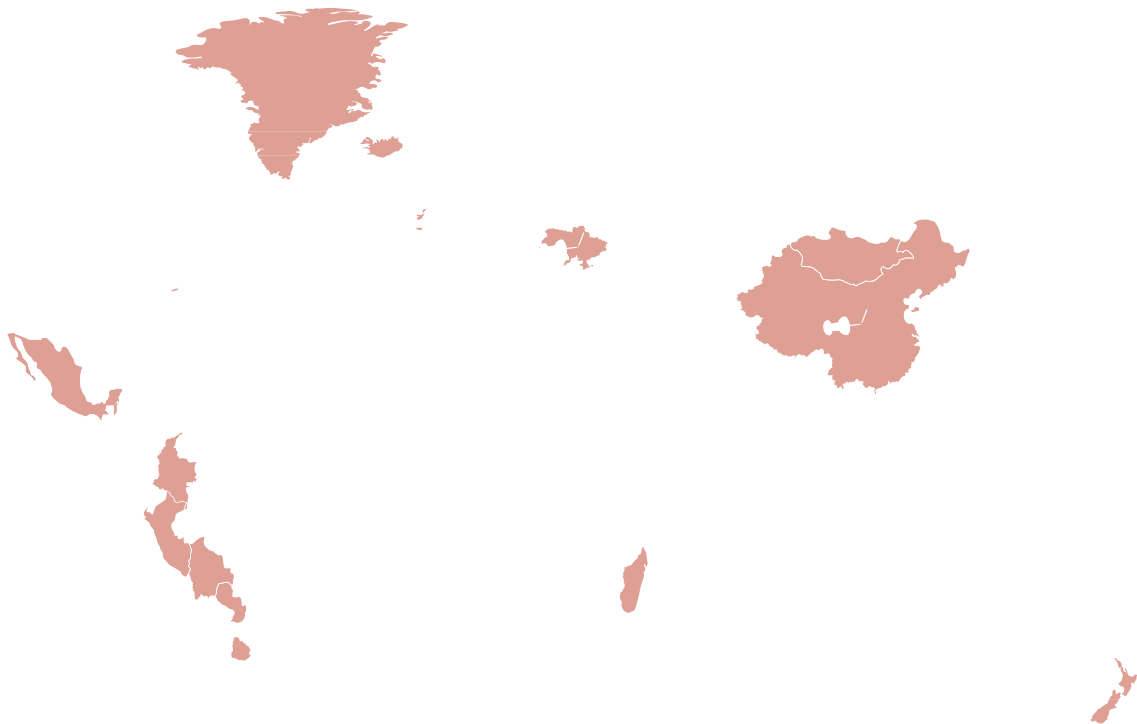
Overall 80 of the invited experts participated in the study, of which 55 (69%) were from industry, 16 (20%) were from science and 9 (11%) came from politics or associations (see Figure 9). The industry share included representatives from all modes of transport. That means we were able to develop a perspective that took into account a broad view of the industry.

Figure 9: Segmentation of Delphi experts



The study also has a truly global perspective. Participants were based in 25 different countries, ensuring a balanced and global view (see Figure 10). Around 60% of the respondents came from developed countries, and around 40% were from emerging countries. Thereby, we were able to take into account the views of experts from both emerging and mature economies.

Figure 10: Geographic origin of Delphi panellists



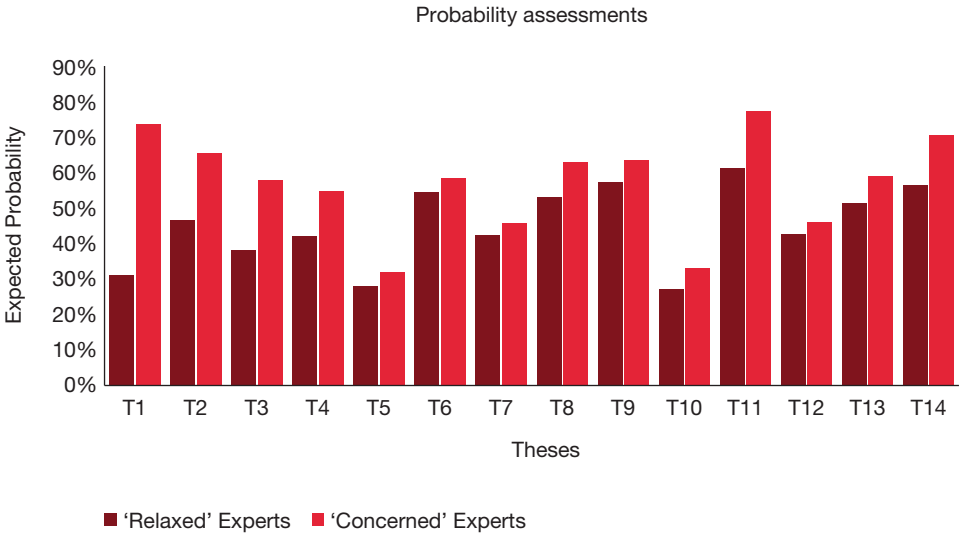
Experts’ underlying assumptions about attacks on supply chains

The Delphi survey results showed that panel experts fell into two distinct groups, ‘concerned’ (58.75%) and ‘relaxed’ (41.25%) panellists. The first group, concerned experts, believes that the number of supply chain attacks will strongly increase in the future. Concerned experts saw our first projection (i.e. “2030: The number of attacks on supply chains has increased”) as highly probable. In contrast, the

second group, relaxed experts, doesn’t believe that the number of attacks on supply chains will significantly increase in the future. They therefore rate the probability of our first projection as very low.

The experts’ assessment of the first projection sets the tone for their assessment of the entire range of projections. Compared to relaxed experts, concerned experts ranked every single projection as more probable, and many of them as significantly more probable, as shown in Figure 11.

Figure 11: Response behaviour of ‘concerned’ versus ‘relaxed’ experts



The survey process

One of the major advantages of the Delphi process is that experts can consider the views of their peers (anonymously) and potentially re-consider their own answers when presented with solid rationales for a different position. The panellists in our Delphi survey took full advantage of this dynamic process. During the eight weeks we ran the survey each participant took part on average in 2.1 Delphi rounds. That means each participant on average ran through both a first and second round per thesis and also logged on 1.1 additional times to re-assess their answers. The maximum number of rounds measured was six.

The statistical group opinion per thesis was provided in the form of a box plot, also known as a “box-and-whisker plot”. Numerical data is shown together with several characteristics of the data series (e.g. median, distribution, outliers). Participants were also able to review the comments and arguments already submitted by other experts for each projection. At the end of a full survey cycle, i.e. first and second round screens for all theses, each panellist was also shown a consensus portal. This meant the panellists could view how their answers compared to those of the group as a whole. Each respondent was then able to access each thesis separately at any time until the final closure of the portal, allowing the experts to check for updates and revise their own estimates. There were 1,220 written arguments provided; that is the equivalent of more than 15 comments per expert. The large number of comments shows a high level of engagement on the part of the panellists, underscoring the quality of the data.

Overview of theses

Figure 12: Overview of theses

No.	Theses for the year 2030	EP	C	I	D
1	The number of attacks on supply chains has increase	56%	34	3.7	1.4
2	Logistics hubs (including ports, airports) and infrastructural nodes (bridges, narrows, channels) are preferred targets for attacks	58%	29	3.9	1.2
3	Targeted attacks on supply chains or hubs have destabilised the economies of some regions	49%	35	3.5	1.3
4	Cyber attacks are causing more damage to supply chains than physical attacks	49%	40	3.7	1.4
5	The number of attacks on supply chains by competitors, for example in the form of sabotage, industrial espionage or manipulation has increased significantly	30%	30	2.9	1.3
6	Security has become one of the most important cost drivers for logistics	57%	30	3.5	2.2
7	Government institutions play the leading role in ensuring secure supply chains	44%	28	3.4	2.8
8	Using advanced technology is the best way to guarantee security	59%	25	3.5	3.0
9	Regional threats to security have caused shifts to transport routes	61%	25	3.6	1.9
10	Supply chain complexity has been reduced due to unresolved security problems	30%	20	3.2	2.2
11	Security audits are compulsory along the whole supply chain, from raw material delivery up to point of sale	70%	25	3.8	3.4
12	Strategies to cope with emergencies are a more effective means of dealing with supply chain disruption than preventative measures	44%	20	3.0	2.5
13	Concerns around data privacy are increasingly ignored in favour of greater security	57%	20	3.1	2.1
14	Additional security measures have resulted in increased transport times	64%	30	3.8	1.9

EP = estimated probability; I= Impact; D= Desirability

Measures of C = consensus (interquartile range <= 25); dissent (interquartile range > 25)

References

- 1 Eye for transport. (2011). Maritime piracy costs global community up to \$12 billion a year. Retrieved 22, February 2011 from <http://www.eyefortransport.com/content/maritime-piracy-costs-global-community-12-billion-year>
- 2 English News CN. (2011). Terror attacks at Russian transport double in 2010. Retrieved 05, March 2011 from http://news.xinhuanet.com/english2010/world/2011-03/02/c_13756267.htm
- 3 BBC News. (2011). Moscow bombing: Carnage at Russia's Domodedovo airport. Retrieved 30, January 2011 from <http://www.bbc.co.uk/news/world-europe-12268662>
- 4 Rudd, M. (2011). Terrorist attack on global supply chain could threaten food, medical and fuel supplies.
- 5 Voice of America News. (12 January 2009) . Central Bank Says Bangkok Airport Closure Cost Economy \$8 Billion
- 6 ABC News. (2010). Icelandic Volcano Airline Costs Keep Climbing, April 16, 2010; International Air Travel Association and U.S. Travel Association
- 7 Foodnavigator USA. (2005). Huge costs of terror attack on US milk supply
- 8 National Counter Terrorism Center. (2011). Worldwide Incidents Tracking System (WITS); Retrieved 07, June 2011 from <https://wits.nctc.gov/FederalDiscoverWITS/index.do?t=Records&N=0>
- 9 Transported Asset Protection Association. (2011). Retrieved 05, March 2011 from <http://www.tapaemea.com/public/>
- 10 International Chamber of Commerce. (2011). Retrieved 05, March 2011 from <http://www.icc-ccs.org/piracy-reporting-centre/imb-live-piracy-map>
- 11 Kaz Kotlow. (2011). Countering Extremism in Yemen: Beyond Interagency Cooperation
- 12 Rafi Melnick, Rafi Eldor (2007). Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center (IICC). Small investment, large returns: Terrorism, Media and the Economy
- 13 Department of Homeland Security. (2007). Strategy to enhance international supply chain security. Retrieved 10, January 2011 from <http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf>
- 14 Online News Hours. (2002). On the waterfront. Retrieved 14, January 2011 from http://www.pbs.org/newshour/bb/economy/july-dec02/docks_09-19.html
- 15 Jean-Paul Rodrigue, Claude Comtois and Brian Slack. (2009). The Geography of transport systems; second edition. New York: Routledge, 352 pages. ISBN 978-0-415-48324-7
- 16 Hofstra University (2006). World's Major Gateway Systems, Retrieved 23, February 2011 from http://people.hofstra.edu/geotrans/eng/ch2en/conc2en/map_worldglobalgateways.html
- 17 CRS Report for Congress. (2005). Terrorist Nuclear Attacks on Seaports: Threat and Response
- 18 Container Security. (2003) Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors. July 2003, GAO-03-770, US GAO.
- 19 Dahlman et al. (2005). Container Security – A proposal for a comprehensive Code of Conduct
- 20 BBC News. (2004). Kyrgyzstan 'foils plutonium plot'. Retrieved 25, January 2011 from <http://news.bbc.co.uk/2/hi/asia-pacific/3695588.stm>
- 21 Guardian.co.uk. (2008). Nuclear bomb blueprints for sale world black market, experts fear. Retrieved 31, January 2011 from <http://www.guardian.co.uk/world/2008/may/31/nuclear.internationalcrime>
- 22 US Department of Homeland Security, Bureau of Customs and Border Protection, "Remarks by Commissioner Robert C. Bonner, Council on Foreign Relations, New York, New York," January 11, 2005.
- 23 Retrieved 11, January 2011 from <http://www.supplychaindigital.com/tags/supply-chain/terrorist-attack-global-supply-chain-could-threaten-food-medical-and-fuel-supplies>
- 24 Rudd, M. (2011). Terrorist attack on global supply chain could threaten food, medical and fuel supplies. 2011
- 25 Retrieved 20, February 2011 from http://www.eia.doe.gov/cabs/World_Oil_Transit_Chokepoints/Full.html
- 26 China Daily. (2010). Shanghai may pass Singapore as world's busiest port. Retrieved 20, December 2010 from http://www.chinadaily.com.cn/bizchina/2010-07/14/content_10104780.htm
- 27 National Center for Ecological Analysis and Synthesis. (2008). University of California, Santa Barbara. Retrieved 27, January 2011 from <http://www.nceas.ucsb.edu/globalmarine/impacts>
- 28 28 Department of EU International Relations and Diplomacy Studies. Issue 1 2011: The EU, China and new transport routes on the top of the world. Retrieved 07, June 2011 from www.coleurope.eu/file/content/studyprogrammes/ird/research/pdf/EUChinaObserver/2011/EU%20China%20Observer%201_2011.pdf

- 29 Asia News Networks. (2010). Terror risk prompts new uranium import route for Japan. Retrieved 07, June 2011 from <http://www.asianewsnet.net/home/news.php?id=14838&sec=1>
- 30 Eye for transport. (2011). Maritime piracy costs global community up to \$12 billion a year. Retrieved 22, February 2011 from <http://www.eyefortransport.com/content/maritime-piracy-costs-global-community-12-billion-year>
- 31 Wall Street Journal. (2009). Piracy Causes Changes in Routes, Insurance Retrieved 15, March 2011 from <http://online.wsj.com/article/SB123923616654003355.html>
- 32 Eye for transport. (2011). Retrieved 20, January 2011 from <http://www.eyefortransport.com/content/maritime-piracy-costs-global-community-12-billion-year>
- 33 AON. (2009). Terrorism threat map
- 34 Retrieved 15, March 2011 from http://www.eia.doe.gov/cabs/World_Oil_Transit_Chokepoints/Full.html
- 35 The Shippers Voice (2011). Shippers warn: Piracy is not a local issue but a global concern for all. Retrieved 15, March 2011 from <http://www.shippersvoice.com/2011/02/25/shippers-warn-piracy-is-not-a-local-issue-but-a-global-concern-for-all/>
- 36 New York Times (2011). Shippers concerned over possible suez canal disruption. Retrieved 21, March 2011 from http://www.nytimes.com/2011/02/03/world/middleeast/03suez.html?_r=2
- 37 Ibid.
- 38 PwC (2010). Retrieved 21, March 2011 from <http://www.logkompass.de/>
- 39 Congleton, Roger D. (2002). Terrorism, Interest-Group Politics, and Public Policy. Independent Review 7(1) Summer: 47-67.
- 40 European Commission Working Paper (2010). Secure trade and 100% Scanning of Containers.
- 41 Ibid.
- 42 Kuhn, F. (2011) Krieg im Netz. ddp Nachrichtenagentur, accessed via LexisNexis
- 43 Dan Verton. (2003) Black Ice: The Invisible Threat of Cyber-Terrorism, McGraw-Hill, 2003, p. 110. Keith Lourdeau, Deputy Assistant Director of the FBI Cyber Division, testimony before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security, February 24, 2004. Ryan Naraine reporting remarks of Roger Cressey at Infosec World 2005, Cyber-Terrorism Analyst Warns Against Complacency, eWEEK.com, April 4, 2005, at <http://www.eweek.com/article2/0,1759,1782288,00.asp>
- 44 Heise online. (2011). Deutsches Cyber-Abwehrzentrum nimmt Arbeit auf. Retrieved 01, April 2011 from <http://www.heise.de/newsticker/meldung/Deutsches-Cyber-Abwehrzentrum-nimmt-Arbeit-auf-1220106.html>
- 45 Spectrumdirekt. (2010). Vernetzte Welt. Retrieved 15, December 2010 from <http://www.wissenschaft-online.de/artikel/1035613>
- 46 CRS Report for Congress. (2003). Terrorist Capabilities for Cyberattack: Overview and Policy Issues
- 47 Spiegel. (2002). Bei Skyguide war die Telefonleitung gestört. Retrieved 15, December 2010 from <http://www.spiegel.de/panorama/0,1518,204126,00.html>
- 48 Spiegel. (2002). Millionenklagen gegen Schweizer Flugsicherung. Retrieved 15, December 2010 from <http://www.spiegel.de/panorama/0,1518,213643,00.html>
- 49 BBC News Europe. (2011). German train crash near Magdeburg leaves 10 dead. Retrieved 30, January 2011 from <http://www.bbc.co.uk/news/world-europe-12082035>
- 50 Spiegel Online. (2010). Zugangslück verursacht Millionenschaden. Retrieved 29, November 2010 from <http://www.spiegel.de/panorama/0,1518,731597,00.html#ref=rss>
- 51 PwC (2010). Respected – but still restrained: Findings from the 2011 Global State of Information Security Survey.
- 52 AME info. (2010). Global IT security spending estimated to rise to \$60bn, as cybercrime continues to grow. Retrieved 15, January 2011 from <http://www.ameinfo.com/238919.html>
- 53 Ifw. (2010). Hi-tech suppliers link up to fight cyber-crime. Retrieved 22, December 2010 from <http://www.ifw-net.com/freightpubs/ifw/technology/hi-tech-suppliers-link-up-to-fight-cyber-crime/20017835705.htm;jsessionid=661B75B6D8FB9F4447C12FDE471E8373.f11b1cef6ac76ad95c7627468fee9bde7e866d022>
- 54 Corporate Trust. (2007). Studie: Industriespionage – Die Schäden durch Spionage in der deutschen Wirtschaft
- 55 Global Economic Crime Survey. (2009). Economic Crime in a Downturn; Pricewaterhouse Coopers; Retrieved 14, December 2010 from http://www.pwc.com/en_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf
- 56 Bill Mongelluzzo. (2010). The Journal of Commerce. Cargo Thieves go online. Retrieved 8, March 2011 from <http://www.joc.com/logistics-economy/cargo-thieves-go-online>
- 57 Interpol (2010). Retrieved 7, March 2011 from <http://www.interpol.int/Public/ICPO/PressReleases/PR2011/News20110117.asp>
- 58 Guedo Fanony (2010). Surveillance and Security Equipment: New Technologies and New Markets. Retrieved 29, March 2011 from <http://www.newshotram.com/surveillance-and-security-equipment-technologies-look-to-drive-into-new-markets/221682/>
- 59 Earth Times. (2010). Paris catching up to London in terms of video surveillance. Retrieved 22, December 2010 from <http://www.earthtimes.org/articles/news/359173,london-terms-video-surveillance.html>
- 60 Potoglou D. et al. (2010). Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK, Transportation Research Part A 44, p. 169–181
- 61 Mueller, J. (2005). Reactions and overreactions to terrorism. Ohio State University
- 62 IMF (2001). World Economic Outlook: The Global Economy after September 11
- 63 Bhat B., Peleg-Gillai G; and Sept, L; 2006; "Innovators in Supply Chain Security Better Security Drives Business Value." Manufacturing Innovation Series.
- 64 Unisys (2005). Secure Commerce Roadmap: The Industry's View for Securing Commerce, Unisys Corporation White Paper, p. 22
- 65 D. Blanchard (2006). Industry Week. Retrieved 22, February 2011 from http://www.industryweek.com/articles/the_benefits_of_a_secure_supply_chain_13103.aspx
- 66 Freight Watch International (2009). US Cargo Theft Review
- 67 Eye for Transport. (2011). Maritime piracy costs global community up to \$12 billion a year. Retrieved 29, March 2011 from <http://www.eyefortransport.com/content/maritime-piracy-costs-global-community-12-billion-year>
- 68 Peleg-Gillai, B; Bhat, G.; Sept, L. (2006). Innovators in Supply Chain Security: Better Security Drives Business Value, Stanford University
- 69 Peleg-Gillai, B; Bhat, G.; Sept, L. (2006). Innovators in Supply Chain Security: Better Security Drives Business Value, Stanford University
- 70 TAPA web site. Retrieved 25, January 2011 from <http://tapaemea.com/public/index.php>
- 71 ISO web site. Retrieved 25, January 2011 from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44641
- 72 Defense daily (2011). Retrieved 7, March 2011 from http://www.defensedaily.com/sectors/homeland_defense/Briefing_12410.html
- 73 Otago Daily Times (2010). Retrieved 7, March 2011 from <http://www.odt.co.nz/news/world/130124/voiceprint-technology-used-against-terrorism>
- 74 NATO. (2010). Defense against Terrorism (DAT) program. Retrieved 29, March 2011 from http://www.nato.int/cps/en/natolive/topics_50313.htm#works
- 75 Ibid.
- 76 Homelandsecurity Newswire. (2010). Retrieved 7, March 2011 from <http://homelandsecuritynewswire.com/dhs-2011-budget-increased-3-percent-436-billion>
- 77 Marnie Hunter, CNN (2009). Body scanners not 'magic technology' against terror. Retrieved 7, March 2011 from http://articles.cnn.com/2009-12-30/travel/airport.security.screening_1_full-body-scanners-aviation-security-greg-soule?_s=PM:TRAVEL
- 78 Gil Yaron. (2010). Sicherheit trotz Terrorgefahr. Retrieved 28, March 2011 from <http://www.news.de/politik/855039084/sicherheit-trotz-terrorgefahr/1/>
- 79 Russell, D.M. and Saldanha, J.P. (2003). Five tenets of security-aware logistics and supply chain operation. Transportation Journal, 42, 4: 44-54.
- 80 Sheffi. Y. (2001). Supply Chain Management Under the Threat of International Terrorism. International Journal of Logistics Management, 12 (2), pp. 1-11.
- 81 SGS (2011). Retrieved 21, March 2011 from http://www.supplychainsecurity.sgs.com/security_assessment_process
- 82 Quality Management International. (2011). Retrieved 21, March 2011 from <http://www.aworldofquality.com/content/training/SupplyChainMSandISO28000.aspx>
- 83 Däneke, E., von der Gracht, H., Gnatzy, T., & Linz, M. (2010). Systematische Wildcard-Analyse mit Hilfe der Delphi-Methode am Beispiel „Future of Aviation 2025“. In J. Gausemeier (Ed.), Symposium für Vorausschau und Technologieplanung. Berlin
- 84 This will include checking a potential criminal background and obtaining a police clearance certificate.
- 85 Such applications will capture events taking place in the supply chain real-time, e.g. loading of goods, dispatch, geo location etc. If an alert is triggered based on an event (breach of security), then the intelligent agent makes a decision on the mitigation of security breach automatically without human intervention (artificial intelligence based system).
- 86 This will include robots specifically designed and built to monitor and guard high value, high risk goods in transit and maximum security storage areas. In addition, these robots can be used to detect and remove dangerous goods from transportation assets such as ships, rail wagons, trucks, etc.
- 87 E.g. secure ship design, lightly designed armored trucks and rail wagons
- 88 Gnatzy, T., Warth, J., von der Gracht, H. A. (2011). Validating an Innovative Real-Time Delphi Approach - A methodological comparison between real-time and conventional Delphi studies. In: Technological Forecasting & Social Change, accepted and corrected proof (in press).

Global T&L Contacts

Africa Central

Vishal Agarwal
+254 20 2855581
vishal.agarwal@ke.pwc.com

Australia

Joseph Carrozzi
+61 8266 1144
joseph.carrozzi@au.pwc.com

Belgium

Peter van den Eynde
+32 3 259 33 32
peter.van.den.eynde@be.pwc.com

Brazil

Luciano Sampaio
+55 11 3674 2451
luciano.sampaio@br.pwc.com

Canada

Stephen D. Shepherdson
+1 403 509 7486
stephen.d.shepherdson@ca.pwc.com

Central and Eastern Europe

Nick C. Allen
+42251151330
nick.allen@cz.pwc.com

China & Hong Kong

Alan Ng
+852 2289 2828
alan.ng.@hk.pwc.com

Cyprus

Liakos Theodorou
+357 25 555 160
liakos.m.theodorou@cy.pwc.com

Denmark

Bo Schou-Jacobsen
+45 3945 3639
bo.schou-jacobsen@dk.pwc.com

France

Vincent Gaide
+33 1 56 57 8391
vincent.gaide@fr.pwc.com

Germany

Klaus-Dieter Ruske
+49 211 981 2877
klaus-dieter.ruske@de.pwc.com

Greece

Socrates Leptos-Bourgi
+30 210 4284000
socrates.leptos.-bourgi@gr.pwc.com

India

Bharti Gupta Ramola
+91 124 3306020
bharti.gupta.ramola@in.pwc.com

Indonesia

Thomson Batubara
+62 21 5289 0400
thomson.batubata@id.pwc.com

Italy

Luciano Festa
+39 6 57025 2465
luciano.festa@it.pwc.com

Japan

Yas Furusawa
+81 3 3546 8460
yasuhisa.furusawa@jp.pwc.com

Luxembourg

Anne Murrath
+352 4948 481
anne.murrath@lu.pwc.com

Malaysia

Azizan Zakaria
+60 (3) 2173 0512
azizan.zakaria@my.pwc.com

Mexico

Martha Elena Gonzalez
+52 55 5263 5834
martha.elena.gonzalez@mx.pwc.com

Middle East

Alistair Kett
+971 2694 6831
a.kett@ae.pwc.com

New Zealand

Karen Shires
+64 4 462 7667
karen.f.shires@nz.pwc.com

Norway

Rita Granlund
+47 95 26 02 37
rita.granlund@no.pwc.com

Philippines

Anjji M. Gabriel
+632 459 3005
anjji.m.gabriel@ph.pwc.com

Portugal

Jorge Costa
+351 213 599414
jorge.costa@pt.pwc.com

Russia

Alexander Sinyavsky
+7 495 2325469
alexander.sinyavsky@ru.pwc.com

Singapore

Kok Leong Soh
+65 6236 3788
kok.leong.soh@sg.pwc.com

South Africa

Akhter Moosa
+27 12 429 0546
akhter.moosa@za.pwc.com

South and Central America

Henrique Luz
+55 11 3674 3601
henrique.luz@br.pwc.com

South East Europe

Momchil Vasilev
+359 2 9355 223
momchil.vasilev@bg.pwc.com

South Korea

Moon-Sub Song
+822 709 0217
moon-sub.song@kr.pwc.com

Spain

Ignacio Rel Pla
+34 963 032 064
ignacio.rel.pla@es.pwc.com

Sweden

Fredrik Göransson
+46 31 793 11 46
fredrik.goransson@se.pwc.com

Switzerland

Thomas Bruederlin
+41 58 792 5579
thomas.bruederlin@ch.pwc.com

Taiwan

Charles Lai
+886 (0) 2 27296666 25186
charles.lai@tw.pwc.com

The Netherlands

Jeroen Boonacker
+31 88 792 3673
jeroen.boonacker@nl.pwc.com

Turkey

Cenk Ulu
+90 212 3266060
cenk.ulul@tr.pwc.com

United Kingdom

Clive Hinds
+44 1727 892379
clive.p.hinds@uk.pwc.com

United States of America

Kenneth Evans
+1 305 375 6307
kenneth.evans@us.pwc.com

