



**Deloitte.**

# Prospering in the Secure Economy

A Deloitte Research Study

# Table of Contents

- Executive Summary ..... 1
- From the War Room to the Boardroom ..... 3
- The Security Regulatory Environment ..... 6
- The Security Tab ..... 11
- The Business Case for Enhancing Security ..... 14
- Mastering the Challenges of the Secure Economy ..... 22
- Insets
  - Transformation of Homeland Security Structures ..... 7
  - Two Models of Security Compliance:  
Publicly Led or Privately Led ..... 10
  - Economic Impact of Visa Delays ..... 12
  - Security and Business Benefits of Radio  
Frequency Identification Systems ..... 17
  - Security and Global Trading Patterns ..... 21
  - Challenges of Public-Private Information Sharing ..... 28
- Appendix
  - Security Regulatory Environment ..... 31
- End Notes ..... 33



**About Deloitte Research**  
Deloitte Research, a part of Deloitte Services LP, identifies, analyzes, and explains the major issues driving today's business dynamics and shaping tomorrow's global marketplace. From provocative points of view about strategy and organizational change to straight talk about economics, regulation and technology. Deloitte Research delivers innovative, practical insights companies can use to improve their bottom line performance. Operating through a network of dedicated research professionals, senior consulting practitioners, and academic and technology partners, Deloitte Research exhibits deep industry knowledge, functional understanding, and commitment to thought leadership. In boardrooms and business journals, Deloitte Research is known for bringing new perspective to real-world concerns.

## Foreword

9-12. The global economy is forever changed. The new leaders—in both government and the private sector—will increasingly be defined by how well they respond in this period of maximum uncertainty. The organizations that prosper in the face of these new realities will not only proactively invest in compliance, processes, and tools to become more secure themselves, but also discover how to create economic value from relationships, processes, and even products that enable security.

The new environment created by heightened security concerns is much different than that experienced during the last major economic revolution—the dot.com period. This new period is defined by greater vulnerability, increased threat awareness, regulatory compliance, and rapid response to change. It is not only an environment signified by the global war on terrorism, but of enhanced visibility—and responsibility—across supply chains and cross-boundary relationships.

The emerging secure economy is a lot like the old one, only faster and with more threats of disruption. Advances in information technology, telecommunications, and transportation have enabled globalization to the point where no global organization in any sector is immune to events that occur halfway around the world. This new environment is one in which no single organization has the responsibility for success—but nonetheless may still be singled out by failure.

Prospering in the secure economy will require three essential capabilities:

- Continual CEO and leadership focus
- Greater collaboration between business and government
- Enhanced shareholder and constituent value from security

Organizations that don't translate the current period of increased security compliance requirements and standards into sustained performance will miss an opportunity in this period of rapid change. This report shares important insights into the new secure economy and explains what organizations need to do to get started.

I've spent most of these past three years working alongside government employees at the U.S. Department of Homeland Security—not to mention advising many other government leaders overseas. The passion, energy, and expertise these professionals bring to the challenges of responding to this new environment is inspiring. Their dedication and professionalism has made security one area where the government has become a major source of global best practices.

On behalf of Deloitte's global Public Sector group, I hope you find this Deloitte Research report useful as you lead your organization through this challenging period.



**Greg Pellegrino**

Global Managing Director, Public Sector



# Executive Summary

Since September 11, global business has had to confront additional terrorist strikes around the world, a steep rise in cyber attacks (at a cost of \$12.5 billion in 2003<sup>1</sup>), huge value losses, hefty increases in security spending and insurance premiums, and a spate of new government security regulations and requirements.

With the increased importance of security has come a fundamental shift in the way it's viewed by companies and governments: the concept of security has expanded from primarily protecting assets and people to sustaining business no matter what type of interruption might occur, from a sudden spike in interest rates or the spread of a computer virus, to an act of terrorism.

In short, the economic playing field has changed. We've entered the age of the secure economy, an era defined by five new realities.

- **Rapid change.** The global business climate has been nothing if not tumultuous in recent years.
- **New regulatory requirements.** On the heels of spending billions of dollars complying with Sarbanes-Oxley regulations, businesses now find themselves confronting a host of new government security requirements.
- **Heightened threats and greater uncertainty.** Companies remain unclear about what kinds of threats warrant the greatest concern, how they would be affected if particular kinds of attacks occurred, what marketplace conditions would follow particular kinds of attacks, and when the heightened threat will pass.
- **Complex and interdependent risks.** For all the advantages of the extended enterprise and its interdependent supply chains, this organizational model also puts firms at greater security risk due to the multiple partners and handoffs involved in production and distribution.

- **Globalization and the 24/7 news cycle.** Globalization and the 24/7 news cycle means companies now have only minutes—not hours or days—to respond proactively to a security incident before risking possible damage to their brand.

In the face of these conditions, ensuring the safety of goods, people, information, and facilities has become an important prerequisite of global commerce. Governments worldwide, and in particular the United States, are doing their part to try to bring this about. A raft of new government initiatives to secure critical infrastructure, the vast majority of which is owned and operated by the private sector, have been issued in the past three years — with more in the pipeline. New security requirements imposed on shippers, ports, truckers, airlines, food producers, retailers, financial institutions, and other industries are forcing fundamental changes in business operations. These changes will cost businesses tens of billions of dollars as companies reconfigure their business processes, purchase security technologies, hire new people, install new equipment, and harden their physical and information technology infrastructures.

## Beyond Compliance: The Business Case for Enhancing Security

For many firms, the most immediately compelling reason for investing additional resources in security will be to comply with the new government requirements. The prospect of hefty fines and the inevitable bad publicity that will ensue will be enough to convince many CEOs and boards to step up their security efforts. New industry security standards promulgated in energy, food, shipping, and other sectors will put additional compliance pressure on firms.

But if the business case for greater security is simply about compliance, the effort ultimately will fall short. Regulations and standards will be treated as only a burden, rather than a stimulus toward greater action. Many firms unwittingly do the bare minimum, treating security as just an add-on cost that should be minimized to the extent possible, while others will ignore the new requirements altogether. The inevitable result: persistent security gaps in the global supply chain and critical infrastructure.

Fortunately, achieving greater security need not involve only costs and little in the way of benefits. Corporate investments in secure commerce can go hand-in-hand with real, measurable business benefits.

- **Cost reduction.** Security investments can be used to drive more efficiency into the supply chain and thereby lower costs and raise productivity. Example: In one major public-private supply chain initiative, cost savings of between \$378 and \$462 per container per shipment were realized from employing a mix of IT tools to secure and streamline shipping.
- **Enhanced revenues.** In addition to providing important security benefits, enabling technologies like RFID (radio frequency identification system) tags can enable timelier and automatic information flows, thereby helping companies increase revenues by slashing the amount of time their goods aren't out on the shelves.
- **Better risk management.** Proactive security policies can help firms become more resilient by better managing the risks of a terrorist attack or other security incident.
- **Brand protection.** Security investments, especially in the areas of incident prevention and crisis response, can help to preserve and protect a brand, the most valuable asset for many companies.
- **Market share preservation.** With various government and industry initiatives inducing retailers and manufacturers to require a higher level of security assurance from their suppliers, verifiable security practices will become obligatory for competing in the secure global marketplace.

## Thriving in Today's Security-Conscious Environment

Prospering in the secure economy requires leading organizations to master the following five challenges.

- **Managing risks and uncertainty.** To cope with the growing risks and uncertainties of today's turbulent world, companies must understand industry-specific threats, assess vulnerabilities, and mitigate those with the greatest potential for disruption.

- **Enhancing crisis response management.** Companies today must be prepared to deal with a crisis immediately after it occurs. A poor response can do permanent damage to a brand.

- **Integrating security strategy across the enterprise.**

Many companies take a balkanized approach to security, and by doing so weaken the effectiveness of the overall security function. What's needed instead is a layered, integrated security model under the direction of an enterprise-wide chief security officer (CSO).

- **Extending supply chain protection end-to-end.** Firms that thrive in today's networked economy will have security and sustainability built into their supply chains and greater security compatibility with their partners.

- **Maximizing shareholder value.** Forward-looking companies can exploit their security investments to achieve competitive advantage in three ways: by enhancing their brand, by securing first mover advantage, or by gaining a foothold in a new market.

## The Role of Government

Governments, too, have a vital part to play in working with the private sector to secure critical networks, ranging from the transportation system to the food supply. To facilitate the transition to the secure economy, the public sector should:

- **Spearhead greater information sharing between the public and private sectors.** Public-private information sharing on threats and vulnerabilities has emerged as a critical element of country homeland security strategies.
- **Provide incentives for companies to invest in security.** Companies with exemplary security policies should be given certain advantages by government agencies, such as fewer inspections, liability protection, tax incentives, reduced reporting requirements, or lower compliance costs.
- **Promote global cooperation on standards.** A nightmare scenario for business: To be forced to comply with a hodgepodge of disconnected and incompatible country-specific security requirements as their goods move across the supply chain. Global standards (in shipping container and energy pipeline security, for instance) could keep this from happening.

## The Road Ahead

The secure economy is here to stay. While the threats and risks may never go away, by working together to bolster security, private firms and governments can make it a lot less likely that those who would do harm succeed.

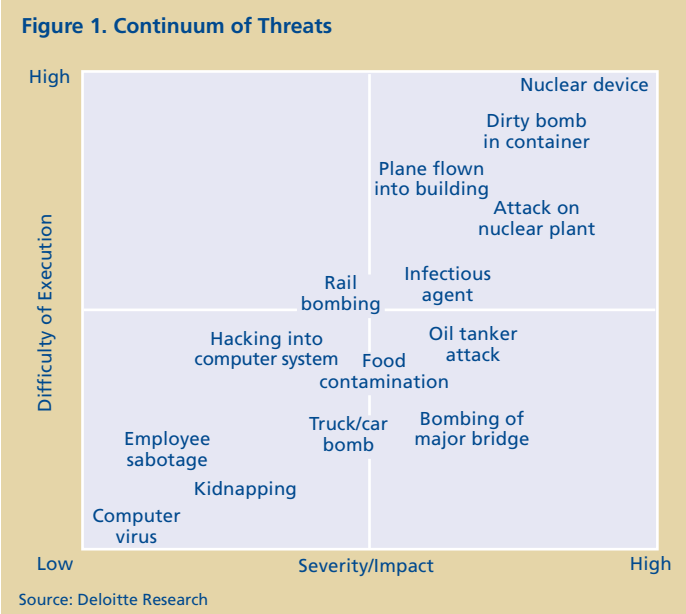
# From the War Room to the Boardroom

August 2003. A pipe bomb explodes at the Emeryville, CA corporate headquarters of biotech company Chiron, delivered by animal rights activists waging a prolonged campaign of intimidation against the company.

Half a world away, in November of the same year, British-owned HSBC bank in Istanbul, Turkey, is reduced to a smoldering mass of charred wreckage by a terrorist attack. The death toll: 27. Later that winter, in April 2004, Osama bin Laden urges his followers to take their global jihad to large multinationals, particularly Jewish-owned companies and American firms working in Iraq. “It is the warlords, the bloodsuckers, who are steering the world policy from behind a curtain,” he proclaims. Several months later, al Qaeda hijacks a California company’s website to show a video of Paul Johnson, an American contractor held hostage in Iraq. The next day, the aviation engineer is beheaded.

Across the globe, security has moved from the war room to the boardroom.

National security is no longer the province of governments alone. Whether they like it or not, private companies man the front lines in the battle against global terrorism. They own and operate the bulk of the power plants, nuclear energy facilities, power grids, and other critical infrastructure in the West—85 percent of it in the United States. They are generally an easier target than government buildings because of their geographic dispersion. And the ultimate goal of al Qaeda is to destroy a way of life, of which the private sector is a key component.



Though the sustained threat of terrorism is the most visible manifestation of the security threats to global businesses, it is by no means the only one (see Figure 1). The 18-year-old student hacking into a firm’s customer database; the disgruntled employee who places cyanide in a drug company’s medicine; or the activist organization threatening to punish a company unless it acquiesces to its demands all represent significant security threats to business.

The secure economy is characterized by a fundamental shift in the way security is viewed by companies and governments: while once mostly signifying the physical protection of assets and people, the *concept* of security has taken on a broader meaning. It now stands for sustainability and the ability to make rapid adjustments to the business, to enforce compliance, and to absorb unforeseen costs—all essential components of managing a business.

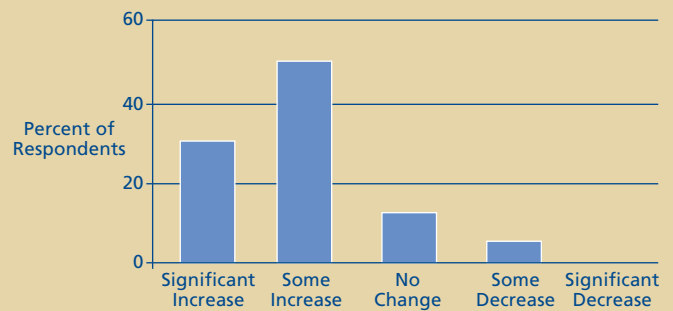
And while terrorism is only one of many security threats to global businesses, it represents the disruptive force driving security to the boardroom level and causing organizations to develop new capabilities, many of which will be relevant to other, more immediate threats. For example, the world's most secure barricades now protect the White House, the American embassy in Iraq and...Walt Disney World. Terrorists who attempt to drive a truck-full of explosives into the Magic Kingdom now have to first get past giant, hydraulically powered antiterrorist barricades designed to stop a 20,000-pound truck bomb traveling 70 mph.<sup>2</sup> Meanwhile in Tennessee, FedEx created its own police force to safeguard the company's packages, while in Washington, D.C., a financial services firm has equipped all of its employees with their own bicycles and gas masks in the event of a biological weapons attack on the nation's capital.

Survey data also demonstrate the growing centrality of security to corporate concerns. It's named a top or high priority by 87 percent of business executives.<sup>3</sup> Terrorism itself was cited as the fourth most pressing security concern among U.S. firms, up from number 17 in 2001, according to a Pinkerton survey.<sup>4</sup>

The greater attention to security is beginning to materialize in company budgets. More than half of the companies surveyed by the Yankee Research Group in 2003 said they would increase their security budget over the next three years.<sup>5</sup> Meanwhile, more than 80 percent of transportation executives interviewed by Deloitte in the spring of 2004 said they expected their firm to increase security spending over the next 12 months.<sup>6</sup>

These sentiments represent a dramatic turnaround. As recently as 2002, more than 90 percent of business executives didn't see their firms as a potential target of terrorism and not even half said their companies were prepared to handle a wide range of emergencies.<sup>7</sup> Now, more than two-thirds of company executives view terrorism as a significant threat to their organization, according to the RAND Institute Europe — and 83 percent believe the threat will rise in the next two years<sup>8</sup> (see Figure 2).

**Figure 2. Change in Perceived Terrorism Threat to Businesses Since 9/11**



Source: Rand Europe, Janusian Security Risk Management, and Financial Times Security Study

Concern with security may also be linked, to some degree, to corporate governance issues. Boards have a responsibility to assure that management has plans for securing people, facilities, information, and business continuity in the event of an incident. More specifically, under section 404 of the Sarbanes-Oxley Act, companies are required to report on the effectiveness of their internal controls, bringing to the surface the need to comply with information security standards.<sup>9</sup>

Meanwhile, companies and governments the world over are discovering just how large an impact the secure economy can have on their bottom line (see Table 1). American businesses, for example, have lost more than \$30 billion over the past two years due to delays in visas for foreign business travelers caused by tougher screening procedures.<sup>10</sup> Washington, D.C.-based Riggs Bank was fined \$25 million, a record sum, in 2004 for allegedly violating tough new anti-money laundering laws in its handling of tens of millions of dollars worth of cash transactions in Saudi-controlled accounts that were under investigation for possible terrorism-financing links. Riggs subsequently announced it would give up most of its international banking business. In the Middle East, meanwhile, foreign workers left Saudi Arabia in droves in 2004 as a result of terrorist attacks on Westerners.

**Table 1. Value Losses from Security Incidents**

Description	Cost
Estimated cost on the entire supply chain of a WMD shipped via container	\$1 trillion
Cost of the September 11 attacks on the two World Trade Center buildings (direct and indirect)	\$83 billion
Cost of cyber attacks against companies worldwide in 2003	\$12.5 billion
Cost to the Canadian beef industry of a case of mad cow disease found in Alberta in 2003	\$2.5 billion
Drop in the European markets (FTSE) immediately following the Madrid bombings	\$55 billion

Organizations that are lax in their efforts to protect their assets and employees or organizations that are unresponsive to government or partner security concerns risk being disaggregated from the marketplace. Explains Alastair Morrison, chairman and CEO of Kroll Security International:

Security has become a main boardroom focus. Since September 11 and the Madrid bombings, companies have been asking: What can bring this company down? In the past, it's been a corporate governance issue, but now it's a security issue. Companies are themselves much more accountable and have to become much more farsighted in their approach. They are aware of their own liability.

Companies must also accept that they will remain unclear about what kinds of threats warrant the greatest concern, how they would be affected if particular kinds of attacks or disasters occurred, what marketplace conditions would follow specific kinds of attacks, and when the heightened threat will pass. It's therefore hard to make assumptions about precisely what the best security investments are—concrete barriers? metal detectors? gas masks? passwords? RFID tags? vaccines? What companies need is a strategy that includes a careful appraisal of all the potential dangers. This will enable them to fashion a response that addresses whatever it is that appears to be the most worrisome for their specific profile, thereby avoiding the extremes of focusing on a narrow slice of concerns or trying to prepare a little bit for every conceivable risk.

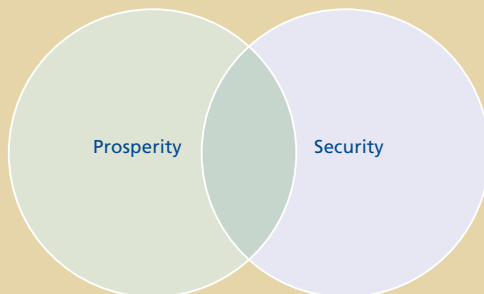
With the dawn of the secure economy we've reached a key inflection point. If done right—that is, if used as an opportunity to enhance business value—all the time and money spent by governments and businesses on security today could yield much better-prepared public and private organizations tomorrow. Innovation would be spurred as organizations seek inventive ways to achieve both greater security *and* higher productivity. Greater security and greater prosperity would go hand in hand (see Figure 3).

With the wrong decisions and wrong approaches, however, the terrorists could win without firing a shot. The increased emphasis on tightening corporate security vulnerabilities could simply result in overly prescriptive government regulations, higher costs for private companies with little tangible benefits, and grudging and uneven compliance. Governments, unwittingly, could restrict commerce so tightly that the economy slows to a crawl. Delays at borders, ports, and airports could cascade through offices and factories, upsetting entire supply chains. The hard-earned gains in global supply chain efficiencies and trade logistics of recent years—\$150 billion worth a year, by some estimates—could be lost.<sup>11</sup> Just-in-time delivery could become merely a distant memory. Distrust between the public and private sectors would retard collaboration.

Such a future is, of course, unacceptable. It's also eminently avoidable. Given the right strategies from business and sensible policies by government, instead of a drag on trade, security can be a means to enable commerce in a more uncertain world.



Figure 3. Business Value Opportunity



Source: Deloitte Research

# The Security Regulatory Environment

Much of the impetus for the increased emphasis on security is being driven by government. Public sector budgets are swelling with intensified security spending. New high-tech systems are being installed to secure borders, ports, airports, and government buildings, intelligence is being beefed up, information sharing improved, and grants to first responders dispersed.

Despite the tens of billions of dollars being spent by governments on strengthening security, however, there are real limits to how much more secure the public sector alone can make us. The reason: Many of the prime terrorist targets and most serious security vulnerabilities reside in facilities owned and operated by the private sector—port terminals and freight containers, airplanes and cruise ships, the food supply and bank systems, electricity grids, and water treatment plants. To reduce vulnerabilities in these and other areas, governments from Canada to Australia have passed a spate of new security-related laws that effectively enlist everyone from brokerage houses to shippers in the global struggle to augment security (see Table 1 for a summary of the regulations and the Appendix for a more detailed analysis). In the U.S., which has particularly emphasized steps to engage the private sector in security, improved collaboration between federal agencies and the private sector is a key goal of the country's homeland security strategy.

Understanding the multitude of new security requirements, directives, and partnerships is *de rigueur* for companies hoping to prosper in the secure economy. In ways both obvious and subtle, they are reshaping international trade.

Consider maritime commerce. One thing that keeps many government security officials awake at night is the prospect of a dirty bomb being smuggled into their country hidden in one of the millions of containers that come through the world's ports each year—few of which are ever inspected. It's almost universally considered one of the biggest security vulnerabilities (70 percent of transportation company executives rate shipping containers vulnerable according to a Deloitte survey<sup>12</sup>), prompting dozens of countries—as well as

several international organizations—to tighten maritime security. The United States has introduced the 2002 U.S. Maritime Transportation Security Act, the 24-Hour Advanced Manifest Rule, and the Container Security Initiative (CSI), among other major maritime security measures. Globally, the most significant maritime compliance issues revolve around the International Ship and Port Facility Security Code (ISPS), the first multilateral ship and port security standard ever created. The bottom line: Nearly every company engaged in global trade will be affected by new maritime regulations.

Tightened border controls will also affect commerce. Large-scale efforts to tighten security along land border crossings are under way in Europe and the U.S. The most ambitious initiative is the US-VISIT program, which, at a potential cost of more than \$10 billion, aims to create a new high-tech virtual border around the United States. Meanwhile in Europe, the EU has proposed expanding its border information system to include storage, transfer, and possible querying of biometric data, particularly photographs and fingerprints.

Rail travel represents another transport target of terrorists, as evidenced by the March 2004 Madrid train bombings. In response, Japan doubled the number of police officers at six major railway stations.<sup>18</sup> Across the Pacific, a U.S. Senate Committee approved a bill in August 2004 that requires the U.S. Department of Homeland Security (DHS) to perform a national rail vulnerability assessment, recommends security upgrades to the rail system, and allocates grants for the upgrades to be carried out.<sup>19</sup> And in Europe, where rail traffic is twelve times that in America, countries have increased police patrols, bomb detection measures, and electronic surveillance.<sup>20</sup>

## Transformation of Homeland Security Structures

A number of countries are trying to strengthen their ability to prevent and respond to terrorist attacks by merging the various agencies involved in air, sea, port, border, intelligence, and cyber security into one mega-department. These actions are important to business because they mean, in some cases, new missions, new people, new reporting relationships, and greater potential private-sector funding for security. These changes represent both new opportunities and new challenges for businesses. The largest such initiative, of course, is in the United States, where approximately 180,000 personnel from 22 different government components became part of the Department of Homeland Security (DHS) on March 1, 2003. DHS unified the agencies responsible for securing U.S. borders and is implementing a layered security strategy through an increased presence at key foreign ports, improved visa and inspection processes, strengthened seaport security, and improved security technology at airports and border crossings.<sup>13</sup> As Tom Ridge, the secretary of DHS, said at the 2004 Homeland and Global Security Summit about the formation of DHS: “The historical government reorganization that took place, the largest since the Truman presidency, presented the biggest ‘change management’ challenge of all time—simultaneously a merger, acquisition, divestiture, and start-up on the largest of scales.”<sup>14</sup> Other countries have also done some reorganization in order to address new security threats. Germany’s Federal Ministry of the Interior (BMI) was restructured to take the lead on anti-terrorism activities; it includes the Federal Criminal Police (BKA), the Federal Office for the Protection of the Constitution, legislation related to foreigners, and border control.<sup>15</sup> Canada has also aggressively reexamined its security apparatuses. The newly established Department of Public Safety and Emergency Preparedness (PSEP) is responsible for emergency preparedness, crisis management, national security, policing, oversight, crime prevention, and border functions.<sup>16</sup> Since 2001, the Canadian government has provided \$37 million for the federal/provincial/territorial Joint Emergency Preparedness Program (JEPP).<sup>17</sup>

Food security has also risen in importance on the governmental agenda. In the United States, the 2003 Bioterrorism Act requires companies to give advance notice to U.S. officials for all food products to be consumed by humans or animals before the shipments arrive in the country. Within the EU, Directive 178, Article 18 consolidates 17 existing hygiene directives and is intended to produce consistency and clarity throughout the food production chain from “farm to fork.”

Other areas of concern are health care, financial services, and energy. In the U.S., hospitals, doctors, insurance companies, and other health institutions are required to protect the privacy and security of individuals’ health information to comply with the Health Insurance Portability and Accountability Act (HIPAA). The financial services industry has also faced increased security regulations as governments try to shut down the money supply that finances terrorist organizations. Title III of the U.S.A. Patriot Act specifically requires the private sector to report money laundering transactions, while the UN Security Council has called on all member states to freeze the assets of those who commit or attempt to commit terrorist acts or facilitate the commission of terrorist acts.

With nuclear energy facilities, oil tankers and pipelines, oil refineries, and national and regional power grids prime targets of terrorists, the energy sector is another high-risk target. But unlike the transport sector, it generally hasn’t seen large new security-related regulatory burdens. Industry officials have successfully staved off calls for new regulations by arguing that existing procedures and planned enhancements are sufficient. This doesn’t mean, however, that the industry has forever escaped new security regulations. A number of reports have warned of inadequate security at nuclear plants and power grid vulnerability resulting in a host of bills proposed in various legislatures.

## Public-Private Partnerships to Secure the Supply Chain

On any given day, more than 15 million containers are moving across the seas of the world. Millions more are being transported across borders by truck, rail, or air. Each could contain a dirty bomb or a biochemical agent that could wreak horrendous damage. But it’s simply impossible to inspect each container before it enters a country—doing so would radically slow commerce. Security assurance must therefore begin long before the goods arrive in their port of destination.

For this and other reasons, governments have sought to enlist the private sector in securing the global supply chain through a number of high-profile, public-private partnerships. While voluntary today, many firms believe the lessons learned from these types of initiatives could to a large extent shape future regulations and requirements and thus they might feel compelled to participate. Here’s a look at some of these initiatives.

**Table 2. A Snapshot of Key Security Regulations**

Category	Regulations	Description	Date Enacted	Date of Compliance
<b>Aviation/ Transportation Security</b>	Aviation and Transportation Security Act (USA)	Federalized airport security. Stricter in-flight security measures. Screening of all goods, persons, and vehicles in secure areas.	November 2001	December 31, 2002 <sup>21</sup>
	ICAO Aviation Security Plan of Action (International)	Central to the plan are regular, mandatory, systemic, and harmonized audits to enable evaluation of aviation security in place in all 188 member states of ICAO.	June 2002	November 2003 <sup>22</sup>
	Common Rules for Civil Aviation Security—Regulation (EC) No. 2320/2002 (EU)	Requires EU members to adopt a national security plan for civil aviation and to appoint a national authority to coordinate the application of the security plan.	December 16, 2002	December 31, 2002
	Measures for the Implementation of Common Basic Standards on Aviation Security—Regulation (EC) No. 622/2003 (EU)	Requires EU members to adopt common basic standards for aviation security throughout the European Union.	April 4, 2003	April 19, 2003
<b>Maritime/Port/ Shipping Security</b>	Maritime Transportation Security Act of 2002 (MTSA) (USA)	Designed to protect nation’s ports and waterways from terrorism. Requires area maritime security committees, security plans for facilities and vessels that may be involved in transportation security accidents.	November 2002	July 2004 <sup>23</sup>
	International Ship and Port Facility Security Code (ISPS) (International)	Requires ships on international voyages and the port facilities that serve them to conduct a security assessment, develop a security plan, designate security officers, perform training and drills, and take appropriate preventive measures against security incidents. Enforced by domestic border agencies such as the U.S. Coast Guard. <sup>24</sup>	December 2002	July 2004
	24-Hour Advanced Manifest Rule <sup>25</sup> (USA)	Ships must file detailed manifest with U.S. Customs 24 hours before a U.S.-bound container is loaded onto a vessel in a foreign port. Advanced notification required differs depending on the means of transport: 4 hours for air cargo, 2 hours for rail, and 2 hours for trucks.	December 2002	February 2003
	Trade Act of 2002 Final Rule – Advance Electronic Information (USA)	Requires advance transmission of electronic cargo information to U.S. Customs & Border Protection for both arriving and departing cargo.	Published December 2003	January 2004
	Canada Shipping Act 2001	Establishes an inspection and enforcement program and ensures Canada can meet international obligations under bilateral and multilateral agreements with respect to navigation and shipping.	2001	July 2003

**Table 2. A Snapshot of Key Security Regulations, cont.**

Category	Regulations	Description	Date Enacted	Date of Compliance
<b>Food Safety/ Security</b>	Bioterrorism Act (USA)	Requires those shipping food products for consumption by humans or animals to the U.S. to give advance notice before shipments arrive.	June 2002	December 2003
	EU Directive 178 Article 18 (Europe)	Mandates manufacturers of all products destined for human consumption to document their flow of goods. Sets out specific requirements in regards to traceability for food and feed producers.		January 2005
	Food Standards Act 1999 (United Kingdom)	Established Food Standards Agency and amended legislation to make the Agency the enforcement authority for fresh meat controls and dairy hygiene legislation.	November 1999	
	National Livestock Identification System (NLIS) (Australia)	Combined government/industry venture which tracks individual animals from birth to slaughter for food safety, product integrity, and market access purposes.	July 2004	July 2005 <sup>26</sup>
	Food Sanitation Law (Japan)	Food business operators including distributors have responsibility to conduct testing and ensure safety of raw ingredients. They must retain records of raw ingredients and investigate the cause of food poisoning incidents. <sup>27</sup>	December 1947 Last amendment in August 2002	
<b>Financial Services Security</b>	Gramm-Leach-Bliley Act (GLBA) (USA)	Requires banks, insurance companies, brokerages, and other financial institutions to establish administrative, technological, and physical safeguards to ensure the confidentiality and integrity of customer records and information. Financial institutions are required to establish measures to monitor and manage security systems.	November 1999	July 2001 <sup>28</sup>
	Patriot Act (USA)	Requires mutual funds, operators of credit card systems, money services businesses, securities brokers and dealers, and futures commission merchants to implement anti-money laundering program.	October 2001	April 2002
<b>Health Care Security</b>	Health Insurance Portability and Accountability Act (HIPAA) (USA)	Requires health plans, clearinghouses, health care providers, Medicare/Medicaid agencies, and other health care organizations to comply with strict regulations regarding confidentiality of private health information.	August 1996	June 1997
<b>Energy Security</b>	National Gas Pipeline Safety Act (USA)	Responsible for setting standards for design, installation, inspections, emergency plans, and testing, and the construction, operation, and maintenance of interstate pipelines.	1968	
	Chemical Facilities Security Act (USA)	Mandates chemical operators to craft vulnerability assessments and site security plans and grants authority to the Department of Homeland Security to regulate those plans and oversee security at the nation's chemical plants.	October 2003	

- **Customs-Trade Partnership Against Terrorism (C-TPAT).** C-TPAT offers companies various benefits in exchange for signing up for the program and certifying to the U.S. Department of Homeland Security that they have put in place a security plan to cover the full length of their supply chain. As of June 2004, C-TPAT had signed up nearly 3,500 certified members, 288 of which had had their security plans validated by DHS.
- **Container Security Initiative (CSI).** An effort by the U.S. Customs Service to secure the shipping industry from terrorism and accidents, CSI consists of four core elements: 1) Establishing criteria to identify high-risk shipping containers; 2) pre-screening containers before they arrive at American ports; 3) using technology to screen high-risk containers; and 4) driving adoption of the use of smart containers. While a voluntary initiative rather than a mandate, there are strong pressures on governments and private businesses to agree to CSI rules at the risk of losing export business to the U.S.
- **Smart and Secure Tradelanes (SST).** SST, a multiphase industry-funded initiative, aims to improve both supply chain efficiency and security through the development of a security network that allows a shipping container to be monitored from its point of origin to its point of final delivery.<sup>29</sup>
- **Operation Safe Commerce (OSC).** OSC is a public-private partnership designed to develop best practices for safe and efficient movement of containerized cargo. Eighteen proposals, approved by the U.S. Transportation Security Administration (TSA) in June 2003, serve as pilot projects. These cover the three largest container load centers in the U.S.: the Port Authority of New York & New Jersey, the ports of Los Angeles/Long Beach, and the ports of Seattle/Tacoma, to which the TSA has distributed \$58 million in funding spread among the three ports.<sup>30</sup>
- **Secure Trade in the APEC Region (STAR).** Launched in October 2002, STAR is a public-private partnership of Asia-Pacific Economic Cooperation (APEC) countries, major private sector companies, and various international organizations focusing on identifying and examining high-risk shipping containers, securing them while en route, and providing advance information on them to officials before they arrive at a border.<sup>31</sup> STAR will be rolled out in several phases, with implementation of electronic customs reporting and improved baggage screening procedures at airports planned for 2005.<sup>32</sup>

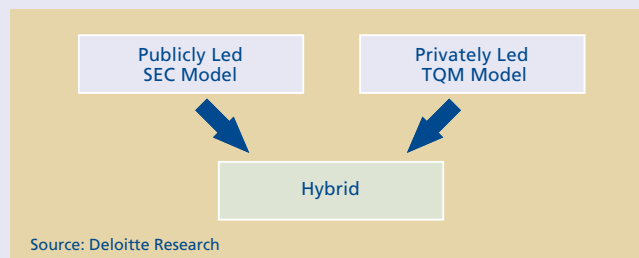
## Two Models of Security Compliance: Publicly Led or Privately Led

The stock market crash of 1929 not only devalued approximately \$25 billion of new securities offered in the 1920s, it also destroyed investor confidence in the capital markets. Subsequently, the 1934 Securities Exchange Act established the Securities and Exchange Commission (SEC) as the primary regulator of U.S. securities markets, and the SEC sought to restore investor confidence by providing more structure and government oversight of the markets. The financial services sector witnessed a sharp growth of government regulations after the 1929 stock market crash—the 1933 Glass-Steagal Act, the 1933 Securities Act, the 1938 Maloney Act—followed by decades of additional regulations on the financial sector.

The current regulatory environment around security shares some obvious parallels with financial regulations after the 1929 crash. Just as that event ushered in new regulatory controls on the financial sector, the cataclysmic events of 9/11 and Madrid have brought forth a stream of new security regulations, covering nearly every industry. Some analysts predict that, as with the SEC, these will represent only the first steps toward a sustained regulatory environment.

What makes such a bold prediction hazardous are certain parallels the current push for greater corporate security also shares with total quality management (TQM), a privately led standards movement. Instead of government regulation, TQM standards such as ISO 9000 were driven in part by industry's need for global standards to facilitate international trade. Similarly, the various voluntary, industry-led efforts to improve private-sector security, including the North American Electric Reliability Council (NERC), the Visa Cardholder Information Security Program (CISP), and the Global Food Safety Initiative (GFSI) can in some ways be seen as the next stage of the quality movement, though this time with a greater focus on information integration.

Right now, security appears to be moving toward a hybrid of the two models, with significant amounts of regulation in some industries such as transportation and more industry-driven standards in others, like energy. But all this could change. Companies need to prepare for either or both scenarios.



# The Security Tab

This much government activity, much of it focused on the private sector, is likely to come with a bill attached. The new security measures are no exception. Complying with new government regulations will cost businesses billions of additional dollars and countless work hours. More vulnerable industries like transportation and agriculture will likely see steep compliance costs, but they won't be the only ones affected. Nearly every major industry faces higher costs in responding to the new security environment. The additional burdens hit businesses in many ways: higher insurance premiums, reconfiguring business processes, purchasing new technologies and computer systems, hiring more people, and, in some cases, building a new infrastructure.

And these are just the direct costs.

Increased wait times at airports, longer holding times for cargo at border crossings and ports, larger inventories, and rising insurance and workers compensation premiums are just a few of the extensive indirect, security-related costs hitting businesses. Federal Reserve economist Bart Hobjin estimates that every year in the United States approximately 550 million passengers will spend an additional 90 minutes at the airport before boarding their flights. If their time is worth between \$10 and \$40 per hour, this will add as much as \$33 billion annually to private sector costs according to Hobjin.<sup>33</sup>

Just how big is the overall bill? One widely cited estimate published just months after 9/11 pegged the direct and indirect costs to American businesses at \$151 billion annually, including \$65 billion for higher supply chain, transportation, and inventory storage costs and \$35 billion for higher insurance and liability premiums.<sup>34</sup> And a previous Deloitte Research study estimated private sector homeland security spending to be between \$46 billion and \$76 billion in 2003. But these were all early estimates—published before many of the new security regulations were enacted. The actual number could be much higher or lower. The truth is no one really knows just how much new security imperatives are costing the private sector globally.

One way to get a better sense of the costs of new security regulations is by drilling down and looking at the effects by industry, each of which is being impacted differently.

**Maritime.** In the U.S., various maritime security mandates will impose up to \$8 billion in costs on the shipping industry over the next 10 years, and that is considered a very conservative number.<sup>35</sup> On top of that, shippers will spend another \$1.28 billion in up-front costs and \$730 million thereafter complying with ISPS—and that doesn't even include the costs of building new smart shipping containers or retrofitting existing ones.<sup>36</sup> Many shippers have complained vigorously about the new requirements, arguing that it is a low-margin industry with easily substitutable segments of business.

By some estimates, ports face even higher compliance costs, with developing countries confronting particularly large burdens in relation to their GDP. Jamaica, for example, estimates that complying with new port security regulations will cost the country around \$100 million.<sup>37</sup>

**Trucking.** Because dirty bombs or deadly biological agents can be transported by land, trucking companies face additional expenses from new security regulations. The Required Advance Electronic Presentation of Cargo Information rule devised by the U.S. Department of Homeland Security requires that cargo information be sent to the Bureau of Customs and Border Protection via an electronic data interchange system before being brought into the country. Annual cost to truckers: at least \$91 million.<sup>38</sup>

**Airlines.** In the U.S., the bill for the bulk of the direct costs to the aviation industry since 9/11 has been picked up by the passengers themselves via a \$10 per passenger security screening fee.<sup>39</sup> Airlines have had to contribute an additional \$315 million annually to help cover the enormous additional costs of passenger and baggage screening.<sup>40</sup>

These costs, along with longer waiting lines and other inconveniences, also impose an indirect cost on the industry by hindering the ability to raise ticket prices and even discouraging some passengers from flying.<sup>41</sup> Many companies, for example, have chosen to reduce their exposure to the risks associated with air travel by relying more on videoconferencing and less on face-to-face meetings. To help compensate for these indirect costs, the U.S. government distributed \$2.3 billion in May 2003 to the airlines in proportion to the amount of security fees they had paid to the TSA since February 2002.<sup>42</sup>

The EU has been less willing to pick up the tab for increased aviation security costs. Despite industry pleas, European airlines have received less than one-third of the \$3 billion in subsidies given to American airlines since 9/11.<sup>43</sup>

**Rail.** The U.S. mass transit industry has spent \$1.7 billion complying with mandatory security measures such as using bomb-sniffing dogs to screen baggage, terminals, and trains, conducting random inspections for suspicious items and replacing trash receptacles with bomb-resistant containers.<sup>48</sup> It is estimated that \$6 billion more is needed to upgrade radio systems, test for chemical and biological agents, and provide closed circuit televisions, fencing, increased staff, and staff training.<sup>49</sup> A bill proposed by U.S. Senator John McCain would authorize \$1 billion in taxpayer money to upgrade rail security, including over \$600 million to Amtrak.<sup>50</sup>



## Economic Impact of Visa Delays

One of the most contentious issues between government security agencies and business revolves around visa issues. In the U.S. almost three-quarters of companies have experienced visa delays or denials; 60 percent said that delays had hurt their company through lost revenue or increased costs.<sup>44</sup> Companies unable to obtain visas for foreign business travelers are conducting business elsewhere. Industry conferences are being relocated abroad. Applications for foreign business school students are dropping. And fewer engineers and scientists are opting to come to America to pursue advanced degrees and work opportunities.

The economic cost has been huge. According to a report from the National Foreign Trade Council, over the past two years, American businesses lost more than \$30.7 billion due to delayed and denied visas for foreign business travelers.<sup>45</sup>

One industry particularly hard hit by the more stringent visa delays is conferences. At the China Textile and Apparel trade show in New York in June 2004, a third of the booths were empty. According to Chinese officials, half of the Chinese executives who had applied for visas for this event had been turned down. This is in comparison to an 80 percent pre-9/11 visa acceptance rate. Similarly, the U.S. direct marketing group Amway decided to move its 2004 convention from Los Angeles to Japan because of difficulties in securing visas for its 8,000 South Korean participants. This alone cost the U.S. economy an estimated \$18 million.<sup>46</sup>

Universities are also feeling the pain. Many foreign students have been deterred from applying to U.S. business and other professional schools because of the cost and wait-time associated with obtaining a visa. In 2004, the number of foreign students taking the Graduate Management Admission Test, required for admission to a U.S. business school, fell 3.9 percent, but for overseas students the decline was a whopping 17.5 percent.<sup>47</sup> The number of scientists and engineers coming to America to work and study has also dropped significantly.

If this trend is not reversed, the long term economic loss to the U.S. could be severe. Foreign students who would have worked for American companies will seek employment in other developed countries, who will then benefit as America heretofore has from their smarts and entrepreneurship. Recognizing the magnitude of the problem, on September 2004, U.S. Department of Homeland Security Director Tom Ridge pledged to streamline the visa process.

**Financial Institutions.** Strict antiterrorist money laundering provisions designed to curb terrorist financing mean additional expenses for banks and other financial institutions. In America, the anti-money laundering provisions of the U.S. Patriot Act will cost banks, brokerages, and insurance agencies roughly \$10.9 billion through 2005 by some estimates.<sup>51</sup> Hit particularly hard by the new regulations are securities firms, which previously weren't subject to the stringent reporting requirements that banks have faced for years. Purchasing identity-tracking software, reconfiguring systems, training staff, and taking other compliance measures are expected to cost the securities industry nearly \$700 million over the next few years.<sup>52</sup> German financial services companies face similar pressures in the wake of the country's tough anti-money laundering provisions passed after 9/11.

Many financial institutions have complained that the considerable costs they have had to bear to comply with the Patriot Act yield few business benefits. In the U.K., financial regulators shelved plans to impose a new anti-money laundering rule on British financial institutions after an analysis revealed that compliance would impose too onerous a burden on the industry. The rule, which would have required all regulated financial institutions to perform a special review of their current customers' identities, would have cost the industry as much as \$274 million.<sup>53</sup>



**Table 3. Estimated Costs of Selected Security Mandates**

Regulation	Estimated Cost to Private Sector*
Aviation and Transportation Security Act 2001 – (USA)	\$315M (annual) <sup>54</sup>
ICAO Aviation Security Plan of Action	\$8.5M (annual) <sup>55</sup>
Maritime Transportation Security Act of 2002 (MTSA) – (USA)	\$7.244B (2003 to 2012) \$883M (annual) <sup>56</sup>
24 Hour Rule – (USA)	\$282M (annual) <sup>57</sup>
International Ship and Port Facility Security Code 2002 (ISPS)	\$1.28B (up-front) \$730M (annual) <sup>58</sup>
Canada Shipping Act 2001	\$88,000 (up-front per ship) <sup>59</sup>
Required Advance Electronic Presentation of Cargo Information (USA)	\$91M (total) <sup>60</sup>
Patriot Act Anti-Money Laundering Program 2001 (USA)	\$10.9B (through end of 2005) \$2.7B (annual) <sup>61</sup>
Bioterrorism Act 2002 (USA)	\$367M (up-front) Initial cost \$367 annual cost \$261M <sup>62</sup>

\*Many economists believe these largely agency estimates may understate the actual costs.

# The Business Case for Enhancing Security

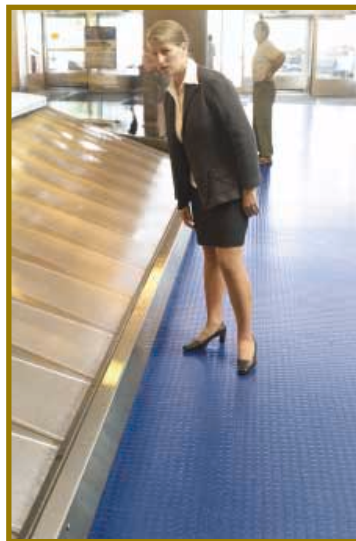
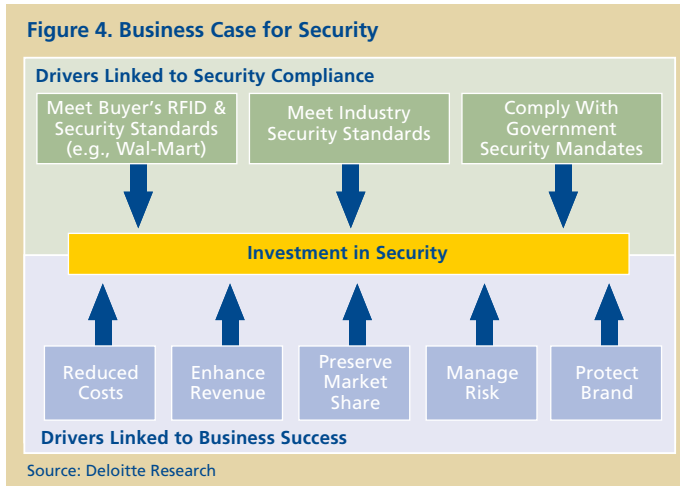
Businesses have essentially three choices when it comes to addressing the new realities of the secure economy and complying with the new security requirements. Option one: They can choose to ignore them in the belief that the costs of compliance are too steep compared to the potential benefits or the penalties from noncompliance. Such an approach, however, risks hefty fines and a subsequent run of bad publicity, as illustrated by the Riggs Bank case. Moreover, if a company is unlucky enough to suffer a security breach and is then found to have failed to comply with a key government or industry security requirement the very future of the organization could be threatened by the inevitable public outcry.

Second, firms can adopt a bare-minimum security compliance strategy—treating it as simply an add-on cost that should be minimized to the greatest extent possible. In an August 2004 Conference Board survey, for example, 39 percent of senior executives at mid-market companies (with revenues of between \$20 million and \$1 billion) saw security simply as a cost that should be strictly controlled.<sup>63</sup> While such a strategy may keep the firm out of the cross hairs of the regulators' sights, it will do nothing to enhance business value. Moreover, if widely emulated, this minimalist approach could, from a broader economic standpoint, lower productivity and slow trade, throwing sand into the gears of the economy.

A more promising option is the third one: Businesses can look to security compliance as a strategic issue—an opportunity to create business value and realize a positive return on their security investment. This more proactive approach moves security upstream: It becomes part of the business process, integrated into the normal course of operations, rather than simply a drain at the end. Investments in security go hand-in-hand with real, measurable business benefits. In the same Conference Board survey, 61 percent of executives said that security investments can provide value for their companies and a positive return on investment. Chris Mahoney, senior vice president of Global Transportation Services at UPS, captures a view held by a growing number of forward-thinking executives when he says:

*Emerging security regulations will force major changes by shippers and transportation companies and the promise of increased visibility in facilitating secure commerce. These demands—fueled by technology, globalization, and an increasingly empowered consumer—are shaping a new age of commerce. With this new age comes new rules...new models...new ways of looking at things...new challenges...and rich new opportunities.<sup>64</sup>*

The opportunities at which Mahoney hints are pronounced. They include: cost reduction occasioned by more secure and efficient transportation and shipping, enhanced revenues, better risk management, brand protection, and market share preservation. Add these together, throw in compliance for good measure, and you have a compelling business case for investing greater resources in security (see Figure 4).



## Cost Reduction

For some corporate executives, cost reduction will be the most persuasive argument for investing in security. The theory is simple: leverage security investments to drive more efficiency into the supply chain and thereby lower costs and raise productivity. Emerging evidence suggests that the right security investments can yield more efficient enterprises.

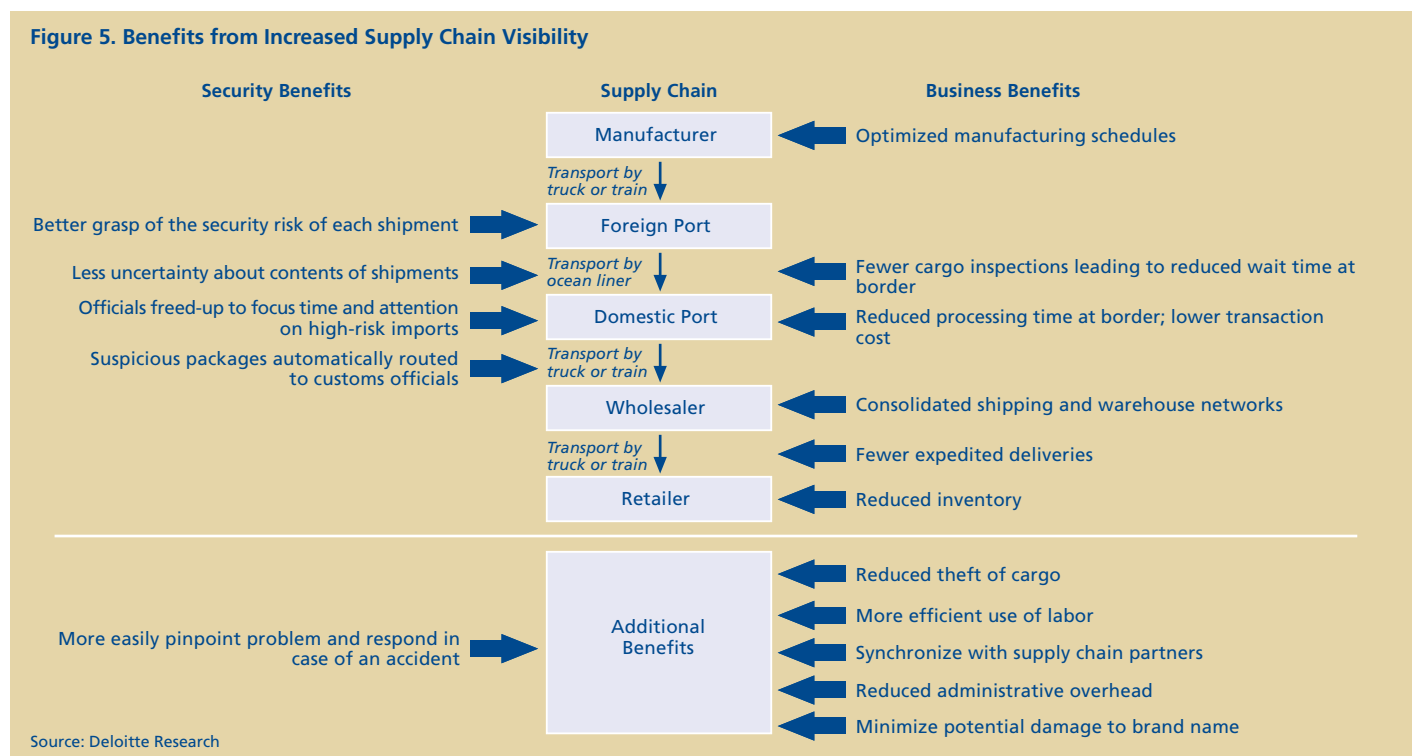
- **Manufacturing.** Torrington Co., a U.S. bearings manufacturer, slashed the time it takes to produce a manifest for port officials from a couple of days to just 20 minutes by digitizing its supply chain and logistics system. Instead of sorting through stacks of paper documents, the company now pulls in the needed information in real-time from electronic databases. The result: time savings and lower freight and handling costs.
- **Airlines.** Each year, Delta Airlines faces losses of up to \$100 million from baggage mishandling. Through the implementation of an RFID system, however, Delta believes it can slash these costs by up to \$37 million. In a program initially rolled out in two airports and eventually reaching 563 operating gates nationwide, Delta's plan is to tag 8.6 million pieces of luggage annually. With the ability to more easily locate misplaced bags, Delta can trim delivery, customer service, and other labor costs associated with locating lost luggage. At the same time, passenger satisfaction could improve enough to allow Delta to even gain a competitive advantage by having industry-wide recognition for low mishandling rates.
- **Food.** The most important factor determining the price a rancher receives for a steer is its weight. On the long, uncomfortable journey to the feedlots or the beef processing plant, typically lasting hundreds of miles, most cattle lose some body weight. Each pound costs the rancher money, providing a strong economic incentive to use trucking companies that are best able to minimize the animal's "shrink" during transport. Previously, it was nearly impossible to track which carriers were best at doing this. Not anymore. Using RFID tags, a cattle rancher can now track the weight of each animal from the beginning to the end of the journey. One rancher discovered that animals lost 4.5 to 6 percent of their weight when one trucking company was used, compared to only 3 to 4.5 percent when using another. The beef producer promptly switched all its transportation to the latter firm and realized a benefit of 1.5 percent less weight loss per animal.<sup>65</sup>

The common enabler to these efficiency gains is better visibility into the supply chain. Technologies such as RFID tags (see box), sensors, smart containers, and electronic reporting and supply chain software solutions, when combined with changes in business practices, can provide companies an unprecedented degree of visibility into their supply chains. This has manifest security and business benefits (see Figure 5 and nearby discussion of RFID tags). For example, a study of the first phase of the Smart and Secure Tradelanes initiative, involving 65 companies across three continents, documented net savings to shippers of \$378 to \$462 per container per shipment from employing a mix of IT tools to secure and streamline shipping. Efficiency was enhanced in five major ways: lower overhead, reduced transaction costs, increased labor productivity, reduced theft, and lower inventory costs.

One problem with existing logistics systems, for example, is the large number of containers that in transit deviate significantly from their original assigned routing, making it nearly impossible to estimate arrival times. Security-tracking tools can help resolve this problem by enabling suppliers and customers to track such changes—and better estimate arrival times.

New security technologies will eventually allow cargo to be cleared more quickly through customs. Once electronic devices can demonstrate that a shipping container remains in its original intact condition from the time it's packed and sealed to the time it's delivered (and we're still a long way away from that point), then customs officials could conceivably clear the container before it even arrives at port, enabling it to be delivered without delay.

Reduced maritime theft and fraud, which today costs companies between \$30 billion and \$50 billion a year, represents another potential benefit of security-driven modernization.<sup>66</sup> RFID tags, tamper-proof container seals, and wireless communications will all make pilfering much more difficult. In 1997, technology industry leaders joined together to form the Technology Asset Protection Association (TAPA). By combining best practices and developing security standards for freight carriers, TAPA was able to bring cargo theft numbers down by 30 percent between 2000 and 2004.<sup>67</sup> An added benefit: lower insurance premiums thanks to the reduced claims.



# Security and Business Benefits of Radio Frequency Identification Systems

Radio frequency identification systems (RFID), a technology first used more than half a century ago during World War II to track enemy aircraft, is a key enabler for achieving greater supply chain visibility. RFID systems use radio waves to wirelessly gather and transmit information ranging from the owner of luggage at an airport to the contents of a cargo container. Unlike a bar code system, RFID systems operate without human intervention to read the data on a tag—even when it's not within the reading device's line of sight. Information stored on the tag can range from as little as an identification number to kilobytes of dynamic information, such as temperature histories. This makes it possible to keep tabs on everything from giant pallets to small boxes of cereal at all times.

Government has been an early adopter of modern RFID technology. Many tollways use it so that drivers can pay road charges without having to stop at a toll booth. RFID technology is also beginning to play a major role in border security. The United States and Canada, for example, have a program called NEXUS to expedite border crossings by low-risk frequent travelers moving across the U.S. and Canadian border. NEXUS applicants go through an intense background check and are then given an RFID-enabled ID card that allows them to use the fast lanes at crossing points.

On the commercial side, RFID holds great promise to help retailers keep more accurate inventory records, increase logistic efficiency, restock store shelves faster, reduce shrinkage, improve forecasting, and lower labor costs. These benefits result from the bolstered tracking and tracing capabilities RFID systems give companies throughout their supply chains. An RFID system can tell a company manager what is available in inventory at any time and then automatically replenish the stock when inventory runs low. The result: no more costly excess inventory. RFID tags can also be used to track product life expectancy, lowering prices as the "sell-by" date approaches.<sup>68</sup>

Cost Savings from RFID Tagging		
Company	Benefit	Savings
The Gillette Company	Reduced shrinkage	\$180M
Kraft Foods	Improved inventory turns	\$2M
Sainsbury's	Reduced receiving time	\$14M
Scottish Courage Brewery	Faster cycle times/ reduced labor	\$22.7M

Source: Deloitte Research

At least two of the world's largest buyers of commercial products believe the benefits of RFID tags are so great that they are requiring their suppliers to put them on all shipments. The U.S. Department of Defense has set a December 2005 deadline for its 43,000 suppliers to put RFID tags on pallets and cases, and eventually on individual parts. Wal-Mart announced a similar requirement in June 2003; 300 of its largest suppliers will be required to use RFID tags by the end of 2006.

This is welcome news to government security officials, many of whom believe the tags provide the best opportunity to achieve the supply chain visibility necessary to meet their goal of knowing where the containers come from, when they're arriving, and what's in them. Combined with sophisticated data analysis programs, the information provided by RFID tags can help authorities flag abnormal patterns.<sup>69</sup> Moreover, the tags are capable of storing information on environmental conditions and, when used in connection with smart seals and containers, can identify whether the container has been compromised in transport.

Though poised to transform supply chains and raise security levels, RFID systems still face a host of challenges. One is interoperability—or the lack thereof. Instead of one universal technical standard for reading and encoding tags, competing standards now exist, meaning readers must be built to read more than one frequency and protocol—a far more complicated and expensive process than if there were just one standard. This battle over who will set the RFID industry standards—or whether there will even be common standards—is slowing business adoption of the technology.

Cost is another barrier. Deploying RFID tags entails reader, tag, infrastructure, and maintenance costs. Today, the cheapest RFID tags sell for about 40 cents each in large quantities. Until the cost drops to under 5 cents each, it generally won't be cost-effective to tag individual, mass-produced items (as opposed to just the pallets on which they are shipped).

Lastly, the potential efficiencies from RFID tags are highly dependent on accompanying business process improvements. Simply tagging items or cargo without business process redesign will yield little in the way of efficiency or cost reduction.

## Revenue Enhancement

Through the use of electronic tags, companies can also enhance revenues while increasing security. Consider the food industry today, where products are available on store shelves only about 90 percent of the time (the rest of the time the item is out of stock), resulting in millions of dollars a year in lost sales. Or take the apparel industry. Matching sizes and colors to potential consumer demand is a complex process requiring considerable coordination, rapid information flows—and a certain amount of educated guessing. Unfortunately, clothing companies don't always get this right, which is one reason why department stores never seem to carry your size during their big, annual sale. By enabling timelier and automatic information flows, RFID tags can help companies slash the amount of time their goods aren't out on the shelves and, by doing so, increase revenues.

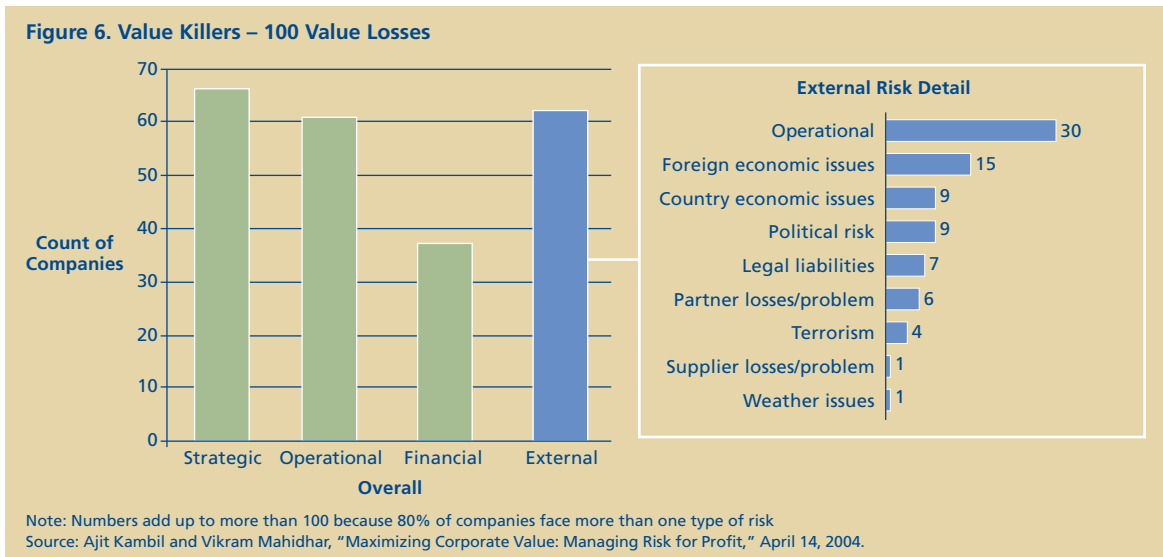
Tagging can also enhance revenues by helping firms meet the demands of the growing number of socially conscious consumers. The meteoric sales growth of everything from organic fruits and vegetables to free-range chicken in recent years illustrates that many consumers are willing to pay more for a product if its source can be guaranteed. Soon, consumers of meat will be able to read all about the animal it came from on the package, including the name of the individual farm. At a grocery store in Yamato, a small city near Tokyo, consumers can punch unique codes printed on

packages of steak into a computer and get information about the cow from which the steak came, including the date of slaughter and verification that the animal tested negative for mad cow disease. This level of transparency is possible because the steaks come from Japanese cattle that have been individually tracked from birth.

Other industries can also benefit from the growth of RFID-enabled information dissemination. Many socially conscious shoppers might be more likely to buy one product over another if they know the factory at which it was produced provided good working conditions and a fair wage.

## Better Risk Management

Companies today must prepare for a range of risks that were unthinkable just a short time ago. Political risks, natural disasters, deglobalization, product tampering, fractures in global supply chains, counterfeiting of trademarked goods, the spread of infectious diseases such as SARs, cyber crime, terrorism—these represent only a fraction of the external risks faced by firms in the 21<sup>st</sup> century. Each has the potential to destroy an enormous amount of shareholder value. In fact, our survey of Global 1000 companies found that 62 percent of the largest value losses to companies involved external risks such as terrorism and country political instability (see Figure 6).



Given the downside potential, it should come as little surprise that executives consistently cite risk management as the most important reason for investing in security. In another Deloitte survey, 80 percent of companies in the transportation industry cited risk management as a “very important” homeland security issue<sup>70</sup> (see Figure 7).

Likewise, according to a Deloitte financial institutions survey, more than 40 percent of financial services industry executives see their IT security investments as a risk management exercise—more than anything else.<sup>71</sup> The message is clear: Beefing up security is a vital component of any enterprise-wide risk management plan that seeks to protect a firm’s infrastructure, intellectual property, people, and brand assets.

Several factors, however, make managing security risks particularly challenging. For one thing, not all risks are created equal. Some are enterprise-threatening, others are just annoying. Some have solutions; for others, there is little that can be done.

According to conventional wisdom, companies should most be concerned with high-probability, high-impact risks. The problem with this approach is that most major company value losses actually come from low-probability, high-impact risks. These rare events include: terrorism, industry or country crisis, natural disasters, and business interruptions. Unfortunately, companies have a hard time figuring out how to deal with low-probability events with large-scale consequences. Many CEOs chafe at spending significant amounts of money to protect their firm against a risk that will likely never occur. It can feel like a waste of money—until, of course, an incident does happen and the firm is unprepared.<sup>72</sup>

Further complicating matters is that most companies are exposed to multiple types of risk at any given time, ranging from terrorism and cyber attacks to interest rate changes. Among the top 100 value losses identified by Deloitte Research, 80 percent were affected by more than one risk factor. The loss of business value often arises from the inter-dependency of these risks, in which measures were

taken to protect against a certain type of risk but not another. For instance, when Pan Am 103 crashed over Lockerbie, Scotland in December 1988, Pan Am had invested heavily in baggage security; the suitcase containing the bomb was loaded onto the plane because it had originated on an Air Malta flight and that airline hadn’t inspected the bag.<sup>73</sup>

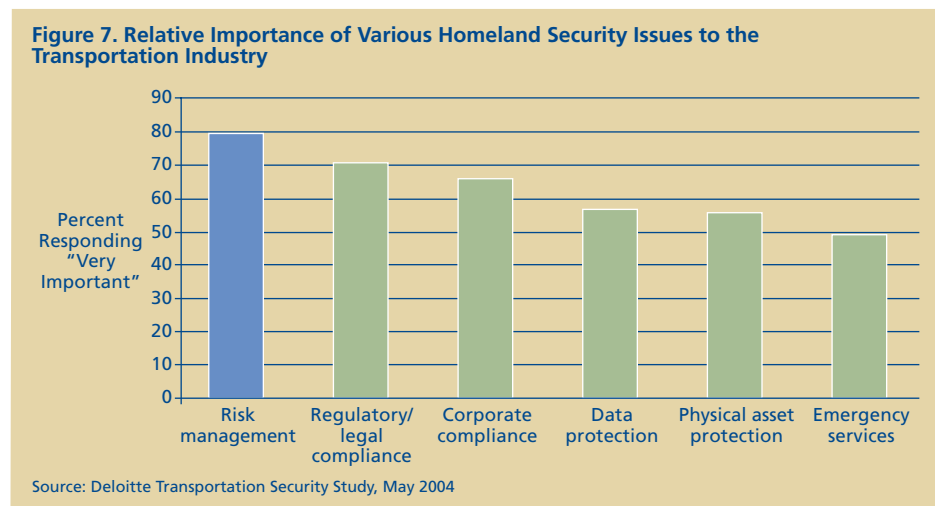
Moreover, despite the fact that minimizing risk is a key concern for nearly all companies (particularly in the aftermath of 9/11 and Enron), most firms continue to increase their risk profile—by entering and expanding in new markets, by spreading sourcing of products and inputs further around the world to take advantage of lower cost, off-shoring production and services, and by shifting R&D and other critical activities to new, low-cost, or high-growth locations.

We’ll have more to say later on in this paper and in upcoming studies about emerging strategies to mitigate against external risks, but for now the key point is that risks can to some extent be reined in by shoring up security.

## Protect Brand

For most companies, reputation is the most valuable asset. Like factories or intellectual property, brand is a quantifiable asset. (Coca-Cola’s brand name, for instance, has been valued at \$84 billion.) A majority of CEOs believe that 40 percent or more of their company’s market capitalization is represented by brand and reputation.<sup>74</sup>

A key threat that risk management strategies seek to mitigate is risk to brand. Survey after survey demonstrates that companies view brand risk as their single biggest business hazard. Perception, and the resulting risk to shareholder value, is often a greater economic threat than the loss of specific assets. If customers lose faith or trust in a company, it can put the very survival of the organization at stake. In the wake of a security-related incident, two questions will be asked: 1) Did the company do everything it could to prevent the incident; 2) Did it manage the response to the crisis well? If the public perceives the answer to either of these questions to be no, then the firm’s reputation would be at risk.



Brand risk is particularly pronounced for those companies in which security is an important attribute of the brand. Consider the overnight carrier known for securely providing overnight service, or the bank whose customer base expects it to protect the privacy of their information, or even an amusement park. Providing a family-friendly, safe environment is part and parcel of the customer experience offered by Walt Disney World. Parents expect their kids to be safe when they take them to the Magic Kingdom.

This is just one reason why Disney devotes enormous resources to security, investing in everything from motion sensors and video cameras to fast-response security teams that can react at a moment's notice to a perceived threat. Disney even worked with the federal government to close permanently the airspace above Disney World.

Of course, despite the best precautions, sometimes an incident can't be prevented. That's why effective crisis response mechanisms are just as important to protecting brand as taking the appropriate prevention measures in the first place. The 1982 Tylenol cyanide poisoning is a well-documented but nonetheless enlightening example of effective crisis management. When seven people in the Chicago area died suddenly after taking cyanide-laced Tylenol capsules, Johnson & Johnson, the maker of the drug, quickly recalled 31 million bottles. Far more potentially detrimental than the \$100 million loss on the recalled drugs, however, was the potential damage to the company's reputation. In the weeks after the cyanide was found, the market value of Johnson & Johnson fell by \$1 billion.<sup>75</sup> Countless experts said Tylenol was doomed as a brand name.

They were wrong.



What saved the day? Johnson & Johnson's textbook crisis management approach. The company moved swiftly to take the product off the market in the form of a mass recall, used advertising and free media to alert consumers across the nation against consuming any Tylenol product, and partnered with the Chicago police, the FBI, the FDA, and other government agencies to coordinate the response to the crisis. Johnson & Johnson emphasized protecting the public above all else, even when doing so might damage the company, and this approach paradoxically ended up salvaging the reputation and brand value of Tylenol.

In November 1982, less than six weeks after the sudden deaths in Chicago, Johnson & Johnson reintroduced Tylenol capsules into the market bearing new triple-seal tamper-resistant packaging—it was the first company to comply with a new national mandate for such package design. By December 1982, the drug had already recovered to the point where it had 24 percent of the market for pain relievers, a drop from the 37 percent it had held before the crisis, but only a temporary one that was not nearly as steep as it could have been.<sup>76</sup>

While Johnson & Johnson's reaction may seem, in retrospect, fairly routine, under similar circumstances many companies have acted quite differently. When traces of benzene were found in a major bottled water company's product in the 1990s, the firm initially claimed the contamination resulted from an isolated incident and recalled only a limited number of cases in North America. This fueled a public relations disaster when, soon after the North America recall, traces of benzene were found in the product in Europe, resulting in a worldwide recall. The media attacked the company mercilessly, criticizing it for lacking integrity and disregarding public safety.

## Preserving Market Share

A major thrust of many government security initiatives is to “push back the borders,” meaning to drive the security requirements back up through the supply chain. The idea is that officials at the Port of New Orleans, for example, can’t guarantee security without first knowing where goods entering the port originated and are confident that they were subject to appropriate security procedures at the point of origin and throughout their journey. The private sector is, in turn, being asked to bear the onus for certifying the security of shipping containers.

Participating companies are not only being asked to provide assurance that the goods they’re bringing in haven’t been tampered with but also to, in essence, vouch for the security policies of their suppliers. For all practical purposes, companies will be held responsible for any security lapses of their suppliers. Global brands such as Nike, Target, and Apple won’t

take this responsibility lightly. Target, for example, already rates countries according to a risk index the company developed and asks its suppliers to sign a memorandum of understanding ensuring they have certain security policies in place. Meanwhile, large European grocery chains like Tesco, where private label food products constitute about 40 percent of sales, are moving toward requiring higher levels of safety assurance from their suppliers than anything EU or member governments have in place.

The more companies participate in public sector-industry security initiatives, the more they will scrutinize the security policies of their vendors as a condition of doing business. Firms will seek out security-conscious sourcing partners so as not to do anything that could risk government fines or the withdrawal of privileges like fast-lane access or the right to an importer’s self-assessment. The overall effect of this is downstream companies that fail to enhance security risk being excluded from the marketplace.

## Security and Global Trading Patterns

The relative levels of security of a country have long been a consideration in business decisions about who to trade with and where to locate overseas operations. Countries perceived as not dealing adequately with security problems tend to have lower rates of economic growth than their more secure counterparts. A 1998 International Monetary Fund study found that terrorism was one of the most important security factors holding down economic growth. Reforms to increase security could improve private investment by 0.5 to 1.25 percent of GDP a year, according to the IMF.<sup>77</sup> Similarly, a 1996 study by economists W. Enders and T. Sandler demonstrated that heightened terrorism during the 1970s and 1980s shrunk average annual foreign direct investment inflows to Spain by 13.5 percent and to Greece by 11.9 percent.<sup>78</sup>

Relative levels of security also impact trade flows. A 2002 study of 200 countries estimated that a doubling of terrorist incidents resulted in a 6 percent drop in bilateral trade between targeted economies.<sup>79</sup> By taking certain steps to improve security and modernize trading systems, on the other hand, countries can better position themselves in the global trading system. Throughout much of the Asia Pacific region, many countries still use manual procedures to check imports.<sup>80</sup> This slows the delivery of operations and negatively impacts supply chain operations.

A study by the World Bank estimated that simply modernizing port infrastructure and information systems throughout the developing world could boost trade in these countries by 2.8 percent (or \$107 billion). “Altering the time it takes to get through the port changes the dynamics of trade,” says Dr. Catherine Mann, one of the authors of the report. “For some countries, this is both a threat and an opportunity. Those that comply first may gain first-mover advantage; those that don’t risk losing market share, at least for suppliers of the American marketplace.”



# Mastering the Challenges of the Secure Economy

Okay. Let's assume that you've by now determined you have no choice but to comply with the myriad new government security regulations. You conduct a business case. It convinces you that you can turn security compliance into business value. What then? How do you get from where you are—which in many cases isn't likely to be terribly secure—to where you need to be? What issues will you face? How can they be overcome? These are the questions to which we will now turn our attention.

Prospering in the secure economy will require organizations to master the five challenges discussed in more detail below.

## Managing Increased Risks and Uncertainty

*Understand industry-specific threats, assess vulnerabilities, and mitigate those with the greatest potential for disruption*

In today's uncertain environment, companies must first of all understand their greatest risks, threats, and vulnerabilities. While this sounds relatively obvious, many companies don't have a clear grasp of their "risk profile," or they're unaware of their biggest gaps in response capabilities. In fact, 36 percent of corporate directors surveyed admit they don't fully understand the risks their companies face.<sup>81</sup>

This lack of awareness could prove fatal in today's uncertain world. The first step in plugging the gap is to conduct a comprehensive security and risk assessment. This in-depth organizational audit, which would include scenario planning, would answer key questions such as:

- What are your security practices, and how are they varied so that they are not too predictable to those who would do you harm?
- If you had a crisis, where would it most likely occur?
- What are your biggest threats? Physical attacks? Cyber attacks? Sabotage?
- Is your company a potential target for terrorists?
- What constitute your biggest reputation risks?
- What crises have other firms in the industry faced? What can you learn from them?
- What elements of your supply chain are the most vulnerable?
- What is your surveillance system and how does it report and react?

Because not all risks are created equal, companies also need a mechanism to sort through the risks and vulnerabilities and prioritize them in terms of importance and likelihood. Diageo, a leading beverage company and owner of brands such as Johnnie Walker, Smirnoff, and Guinness, broke down all the risks the company had to cope with into a single “risk map” that laid out the type of risks, the likelihood of them happening, and the cost to the company if they did. One of the greatest risks: a change in the public perception and regulation of alcohol.<sup>82</sup> This type of analysis allows companies to make a more educated decision on how properly to allocate security spending.

In devising a risk management plan, two common errors should be avoided. First, traditional risk assessment tends to focus primarily on tactical, operational risks, such as business continuity planning, while giving short shrift to the broader, strategic risks a company must confront in today’s turbulent world. Take the instance of a ship that’s sailing to a small port in Southeast Asia. A traditional risk assessment analysis might ask what risks the vessel will face between the point it embarks on its voyage and when it arrives at its destination. A more strategic approach might first ask whether, given the lack of modern security systems and procedures at the port, it’s even the right place for the ship to be going in the first place.

Traditional risk management also often falls short in devising appropriate countermeasures to potential risks. One of the biggest challenges of traditional scenario-based planning is determining a “go forward” strategy based on the most plausible set of future occurrences. In a security context, the company might first ask what internal and external incidents might occur that could adversely affect the company. Contaminated products? Successful cyber attack? Terrorist bombing? Kidnapping of employee? Disruption of global shipping lanes caused by the discovery of a dirty bomb at a major port? And then because a company can’t possibly totally prepare for every potential eventuality, it typically adopts a core strategy that will work in as many of the scenarios as possible. The firm’s leadership then waits until events signal which of these scenarios appears to be materializing before committing the extra resources needed to address them. With this model, the company essentially bets that it can be fast enough out of the gate to avoid being caught completely unprepared.

Deloitte Research has developed a different framework called Strategic Flexibility that allows a company to be better prepared. As summarized in Table 4, a company using Strategic Flexibility still defines scenarios anticipating plausible futures and their corresponding risks. And it develops a core strategy. However, it doesn’t stop there. Recognizing that the

**Table 4. Illustrative Application of Strategic Flexibility to the Security Environment**

Identify Key Drivers	Define Scenarios	Formulate Strategy
<p><i>What are the factors that affect the nature and severity of threats to the company, and how might they change over the next five years?</i></p> <p><b>Technology:</b> What advances could occur affecting the methods and materials attackers might use? What about advances that enable better surveillance, data management, countermeasures, etc.?</p> <p><b>Society:</b> How might values change here and abroad in ways that promote or deter attacks?</p> <p><b>Government:</b> What military or homeland security policies could governments here and abroad adopt that might help or hurt the threat level?</p> <p><b>Geo-politics:</b> What trends or events might cause governments to be more cooperative or more hostile?</p> <p><b>Industry:</b> How could actions by individual companies and industry groups make attacks more or less likely?</p>	<p><i>If the threat drivers were to evolve in a certain way, what would be the prevailing risk environment?</i></p> <p><b>Who</b> is the most likely potential perpetrator in this scenario?</p> <ul style="list-style-type: none"> <li>• Terrorists, hackers, disgruntled employee, hostile state, etc.</li> </ul> <p><b>How</b> would the attack most likely in this scenario occur?</p> <ul style="list-style-type: none"> <li>• Attack on physical facilities, intellectual property, employees, computer systems, products</li> <li>• Car-bomb, nuclear device, dirty bomb, biological agent, chemical agent, kidnapping, hijacking, cyber-attack/hacking, computer virus</li> </ul> <p><b>What</b> would be the ramifications?</p> <ul style="list-style-type: none"> <li>• Vulnerability of the company – special risks v. same as the rest of society</li> <li>• Security measures – access restrictions, facility modifications, sampling and testing, tracking and sensing, record-keeping and reporting, stockpiles, emergency procedures, etc.</li> <li>• Impact on markets and the economy</li> </ul>	<p><i>What strategy will permit the company to address the widest possible range of future conditions while remaining competitive?</i></p> <p><b>Right moves for each scenario</b></p> <ul style="list-style-type: none"> <li>• What would the company do in each scenario to: <ul style="list-style-type: none"> <li>– Deal with the threat in the scenario</li> <li>– Comply with the requirements government would prescribe in the scenario</li> <li>– Address the threat and government mandates in ways that promote greater efficiency, better customer service, etc.?</li> </ul> </li> </ul> <p><b>Core elements of the strategy</b></p> <ul style="list-style-type: none"> <li>• In reviewing the strategies defined for the individual scenarios, what measures show up in all or most of those strategies?</li> </ul> <p><b>Contingent elements of the strategy</b></p> <ul style="list-style-type: none"> <li>• Of the measures that are needed for only one or two scenarios, how could the company position itself to put these into effect if the threat environment began to resemble the pertinent scenario?</li> </ul>

core strategy consists of initiatives that are necessary for all scenarios but aren't sufficient for success in any one scenario, the company builds a portfolio of real options on the various futures it has identified—in this case, alternative threat conditions. The real options are limited, provisional investments in the assets and capabilities that will be needed if, but only if, particular scenarios materialize. As time goes on and new developments make some scenarios more likely and others less likely, the company can adjust its investments accordingly, increasing some and abandoning others. By the time other companies are realizing they need to adapt their strategies to deal with the emergence of new conditions, a company applying the Strategic Flexibility approach is already well underway with its own preparations, leveraging the contingent investments it made earlier as protection against just this sort of threat environment. This approach allows the firm to deal with multiple contrasting versions of tomorrow's world and to better address extreme low probability events, like a terrorist attack.

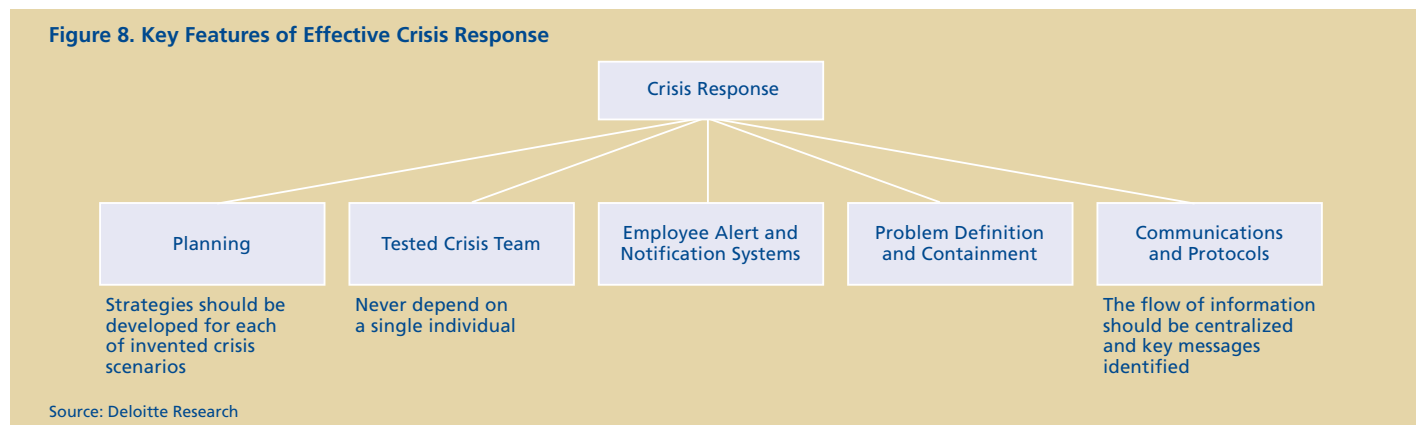
## Crisis Communications and Response Management

### *Strengthen incident and crisis management capabilities*

Companies must be ready to deal with a crisis immediately after it occurs; even the appearance of a slow response can cause long-term damage to the brand. Consider the utility industry where reputations are often made or lost based on their response to disasters, storms, or man-made threats. A full week after hurricane Isabel hit the East Coast of the United States in September 2003, thousands of homes still had no electricity. Local utilities were hammered in the press and by local officials for not responding quickly enough. Allegations ranged from poor customer communications and problems with the computerized systems to slow deployment of crew teams.<sup>83</sup> Criticism was so widespread that some political figures even called for formal investigations into the utilities' preparedness and response.<sup>84</sup>

A comprehensive and well-coordinated response, on the other hand, can help a firm gain a national reputation for crisis response. Take, for example, Florida Power and Light, renowned for its rapid response to hurricanes and tropical storms. To prepare for these events, FP&L employees conduct an annual "storm dry run" in which they simulate a statewide hurricane and test the company's ability to respond rapidly and efficiently. No detail is left unturned. Everything is reviewed, from the lists of food and hotel vendors needed to feed and house repair crews to restoration strategies for major damage.<sup>85</sup> One important lesson emerges from this example: Much of what must be responded to in a crisis can be prepared for in advance.

Strong response capabilities can even at times overcome the initial drop in confidence in a company caused by a major security breach. In the summer of 2003, ABSA Bank, one of South Africa's leading financial institutions, became the target of cyber fraud. Using keystroke software, hackers gained access to several customers' accounts, stealing the equivalent of nearly \$70,000.<sup>86</sup> The impact on the bank's finances was small. The greater impact was on ABSA's brand name, which had been built up significantly throughout the 1990s.<sup>87</sup> (Through an aggressive marketing campaign, ABSA had gone from zero percent to 95 percent brand recognition in just four years, gaining a reputation for providing the highest level of service.)<sup>88</sup> The security breach put ABSA's brand name in jeopardy. Its impact on the bottom line was tempered, however, by steps ABSA took to increase the security of online transactions. In an effort to reassure customers, the bank



installed stronger online authentication and security features.<sup>89</sup> Moreover, ABSA formed a special task force to identify points of compromise and track down leaders of fraud syndicates in Eastern Europe and Nigeria.<sup>90</sup> These and other actions helped to re-instill confidence in the bank. Earnings went up by nearly 30 percent between 2003 and 2004.<sup>91</sup>

Effective crisis response also demands modern alert notification systems. September 11 exposed the major holes in corporate crisis alert and notification systems. Technologies available today allow companies to deliver real-time, multi-channel alerts across the organization to virtually any device — phone, pager, PDA, e-mail, Blackberry, or instant messenger. T. Rowe Price, a Baltimore-based investment management firm, for example, can locate any person or group of people at any given time and deliver security warnings and instructions in response to natural, man-made, and IT disasters.<sup>92</sup>

## Integrating Security Strategy Across the Enterprise

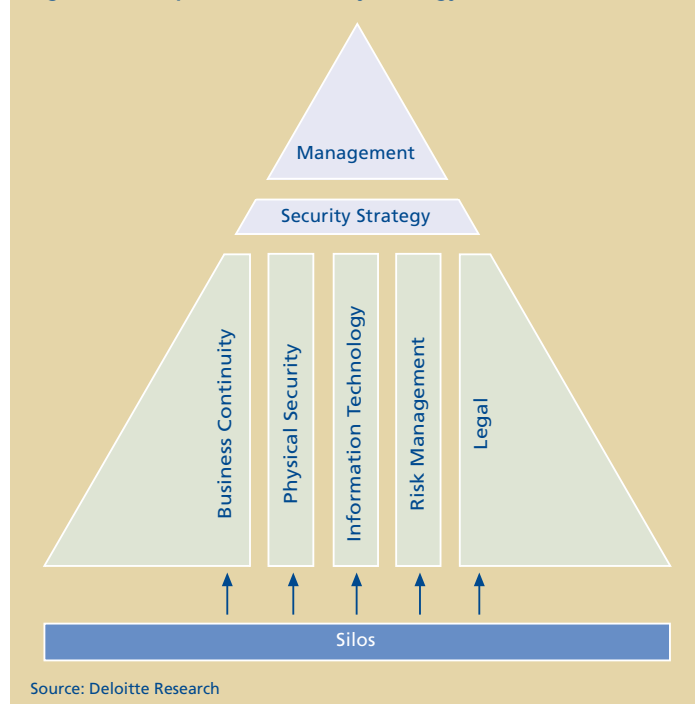
*Implement a layered, integrated approach to security activities*

Many firms today employ a balkanized approach to security. The security personnel handle the guards, the gates, the alarm systems, and other physical security. The computer team takes care of defending the firm from hackers and cyber terrorists—putting up the firewalls, patching the holes in the software, and making sure access to customer databases is strictly limited. The risk managers, meanwhile, do the risk planning, look at business continuity, and deal with the insurance companies. These groups tend not to communicate enough—or sometimes at all.

As security moves up the corporate ladder and attracts more attention from the board, the traditional siloed approach to corporate security will more and more be shown lacking. Having an assortment of security organizations within a single company weakens the overall effectiveness of the security function. Security must be treated not as so many discrete technical tasks relegated to specialized teams, but as a critical business function managed at an enterprise level which encompasses physical, technological, psychological, risk, and legal issues (see Figure 9).



Figure 9. Enterprise Level Security Strategy



Such a holistic security model is at the center of the U.S. Transportation Security Administration’s efforts to understand and reduce vulnerabilities in America’s transportation systems. The agency takes a “wrapper” approach, looking at vulnerabilities across all dimensions of the transportation network: physical, cyber, and human capital. TSA officials believe this approach to be the only way to really get a handle on the most serious risks faced by transportation networks, as well as understand the most urgently needed investments.

A welcome development is the rise of the chief security officer (CSO) and the evolving responsibilities of this position. More than half of companies with sales over \$1 billion have CSOs and the numbers are rapidly rising. While once concerned mostly with IT security or physical security alone, CSOs are slowly starting to be given more enterprise-wide security responsibilities and put in charge of consolidated security organizations. In this role, they have the challenge of driving the organization toward a common security posture. Other companies, finding it difficult to locate an individual with the right mix of expertise in IT security, physical security, risk management, and business continuity, have instead opted to create a high-level security group that brings together people in the organization who are well qualified in these varied skills.

Whether at the behest of a CSO or a security group, it is crucial that companies adopt a layered security framework—one in which multiple levels of defense and security are baked into the organization's business processes.<sup>93</sup> A good example is Walt Disney World. A host of well-integrated measures ensure that visitors to the park have a pleasant, but safe experience. Fountains, flower gardens, and other physical barriers at the Magic Kingdom dictate where people can walk. Access to certain areas is controlled by making exhibits viewable only from a moving vehicle.<sup>94</sup> And every employee from Mickey Mouse to the hot dog vendor subtly but actively plays a role in making the park secure. For Disney, security is an intrinsic part of what happens on an everyday basis and contributes to the proper functioning of the park as a whole.

## Extending Supply Chain Protection End-to-End

### *Evaluate, measure, and implement security standards across the supply chain*

As if it isn't hard enough for a firm just to get its own security house in order, in today's networked economy, companies must also concern themselves with the security practices of their supply chain partners. It typically requires 25 different parties and 30 different documents to get goods from one end of the supply chain to the other. With all these handoffs, the opportunities for tampering are plentiful.<sup>95</sup> "Our concern is not that a person is going to tamper with our coffee, but that without a monitoring system, it would be easy to disguise and hide something in one of the millions of containers we import," says Bruno Velcich, director of communications for Sara Lee Coffee and Tea Foodservice. "We don't want anything to happen to a container that belongs to Sara Lee."<sup>96</sup>

Disruptions in the supply chain, in turn, can have consequences far beyond their immediate geographic vicinity. A snowstorm in the Alps can affect train lines all throughout Europe. The closure of the ports in Hong Kong and Singapore, which together process more than one million containers a month, for just a few days would wreak havoc on global trade.

These are just a few of the reasons why so many of the major public-private security initiatives—Operation Safe Commerce, Container Security Initiative, C-TPAT—focus attention on securing the supply chain.

Companies that thrive in the secure economy will have security and sustainability built into their supply chains and greater security compatibility with their partners. JC Penney, a C-TPAT participant, evaluates the security of each of its suppliers based on a 22-question checklist that include questions such as: Are containers inspected before loading? Are seals being rechecked and reloaded?<sup>97</sup> Facilities are then graded as "acceptable" or "unacceptable." Those that get a failing grade are given 90 days—and some technical

assistance—to get security up to par. If the problems still aren't fixed, the supplier is suspended.

Exhaustive security evaluations, however, entail sizable transaction costs. It's expensive and time consuming to go through such a process for every new and existing supplier. It could also distort markets: Firms might become more reluctant to change suppliers or add new ones due to the additional costs involved in conducting the evaluations.

One way to avoid such a disruptive outcome is via the standard-setting process. Industry-wide security standards and certification processes could help firms to quickly ascertain which potential partners are and are not security conscious. Here again, the ISO 9000 model proves instructive. ISO 9000 provides a single set of quality standards for organizations that people everywhere can recognize and trust. By becoming ISO 9000 certified, a firm can enhance its appeal as a possible supply chain partner. For end product manufacturers the ISO certification process reduces their search and evaluation costs, thereby facilitating trade. An ISO standard, ISO 17799, already exists for information security. With security rising to the top of the government and corporate agenda, a broader ISO standard covering the full range of security practices is needed.

By creating their own compliance programs, the private sector can not only satisfy existing regulatory pressures and stave off future regulations, but also address industry-specific issues (such as secure transmission of private financial or medical data). The North American Electric Reliability Council (NERC), for example, proposed a mandatory security standard for the electric utilities industry in April 2003. The NERC security rules are based on standards that the government has been contemplating and include such measures as cyber security training programs, new security policies, and identification of critical cyber assets. It also includes requirements for compliance monitoring and sanctions for noncompliance.

The food industry is pushing aggressively toward global standards. The Global Food Safety Initiative (GFSI), launched in 2000 by a group of global retailers, aims to establish global food safety standards, build and implement an early warning system, and encourage more cooperation between the food sector and national governments. All indications are that the standards, which are getting a great deal of attention in Europe, will be even tougher than those already adopted by the U.S. Congress and the European Commission.

## Maximizing Shareholder Value

### *Seek competitive advantage through security*

As the secure enterprise becomes the standard, not the exception, it will become harder for companies to move far enough ahead of the pack security-wise to gain an edge over their competitors. But security is just beginning to catch on as a corporate imperative. This leaves a window of opportunity for forward-looking companies to exploit their security

investments to achieve competitive advantage in three ways: by enhancing their brand, securing first-mover advantage, or gaining a foothold in a new market.

Security is growing in importance as a brand differentiator in a host of key sectors. Consider the software industry. With the proliferation of viruses, Trojan horses, worms, and other kinds of cyber attacks, Fortune 1000 companies are becoming more aggressive in insisting that software providers build more secure products. It's an area where security will increasingly become a source of competitive advantage. More broadly, we are moving into an era in which security will become more and more a proxy for a well-managed company.

First-mover advantage is another way to achieve competitive advantage through security. Thousands of companies have voluntarily signed up for public-private security initiatives such as C-TPAT and Operation Safe Commerce. At least one reason for participating is the belief that if they are able to get out there first, they can control and influence standards and therefore avoid having to retool their organizations down the road. By so doing, companies gain important advantages over their competitors.

Lastly, the large and growing market for security services and technologies provides an untapped opportunity for many technology and professional service firms. Security services will grow 8.3 percent a year over the next few years—much of it outside the U.S.<sup>98</sup> According to the Freedonia Group, the market for security services will double by 2006 in Asia/Pacific (excluding Japan), Latin America, Eastern Europe, Africa, and the Middle East relative to their pre-9/11 size<sup>99</sup> (see Figure 10).

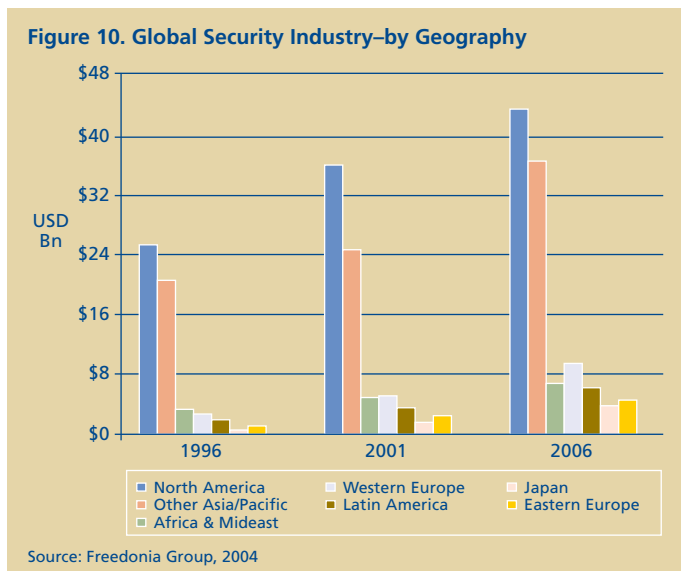
Considerable opportunities also exist to leverage “civilian” technologies to security applications and vice versa. Consider Genex Technologies of Kensington, Maryland. The electronic imaging company is developing a 3-D facial recognition system for identification and verification. While this biometric technology has these security applications, it also can be used for reconstructive surgery. Similarly, Santa Monica-based Utopia Compression is working to improve the compression ratio of images used for surveillance in order to avoid bottlenecks and transmission delays. This technology will also have important applications in the medical imaging and entertainment industries.<sup>100</sup>

To help fund these kinds of investments, firms can tap into billions of dollars in government funds set aside for promising security technologies in countries such as Germany and the United States. The U.S. government's Advanced Technology Program (ATP) funds start-up technologies deemed too risky by the marketplace. From 1990 to May 2004, ATP paid out a total of \$2.2 billion, with single company project awards averaging \$1.8 million.<sup>101</sup> In 2002, 40 grants were given, with an average size of \$2 million.<sup>102</sup> Five of the 40 had homeland security applications, a number that should grow dramatically in upcoming years.<sup>103</sup> Meanwhile, the U.S. Department of Homeland Security has budgeted \$2 billion a year to fund the R&D of more than three dozen long-term security technology initiatives. The private sector will be a principal recipient of this money, along with university laboratories and companies working with U.S. defense labs.<sup>104</sup>

## The Role of Government

Government, too, has a vital role to play in securing critical infrastructure and in helping the private sector to beef up security. First and foremost, of course, is government's core role in preventing attacks through enhanced intelligence and enforcement.

In addition to this, governments must also assume an active role in the effort to reduce private sector vulnerabilities. In doing so, governments must walk a fine line between being too prescriptive and heavy-handed—and thereby saddling the private sector with a host of onerous requirements that will be resisted and may be ill-conceived—or being too timid and risk being accused of being asleep at the switch if a devastating attack is successful. Getting the balance right requires nuance, open lines of communication, platforms for knowledge sharing, and, most of all, considerable outreach. To date, government efforts have fallen short in some of these areas. Many private companies are unclear about the magnitude of the requirements they must meet and exactly how to meet them. Others simply aren't convinced governments will vigorously enforce the new rules.



To rectify this situation and facilitate secure commerce, governments should:

## Solve the Information-Sharing Conundrum

*Create protocols for greater information sharing with the private sector*

Public-private information sharing on threats and vulnerabilities has emerged as a critical, but largely absent, element of country homeland security strategies. Intelligence agencies and various other government departments responsible for securing borders and critical infrastructure have access to actionable intelligence which may not be available or apparent to the private sector. These agencies can identify and bring focus to new threats and prospective risks to the private sector.

On the other side of the coin, as private firms ramp up their security efforts they may have access to particular information on potential threats—cyber attacks, for example—well before government agencies.

Given the importance of the issue, it's no surprise that there is no shortage of efforts under way to increase the sharing of information about threats, breaches, and other matters:

- **MIS**, the United Kingdom's domestic intelligence and security agency, has launched an initiative within its National Infrastructure Security Co-ordination Centre (NISCC), to partner with the private sector to prevent attacks on critical infrastructure.
- **TSA**. The U.S. Transportation Security Administration's Transportation Security Operations Center (TSOC) serves as a single point of contact for all security-related transportation concerns and coordinates intelligence reports of threats with responses by law enforcement and the transportation industry. TSA's 24-hour watch routinely communicates with industry representatives about security events or information of potential security interest.
- **ISACS**. In the U.S., nearly every major industry sector (energy, transportation, financial services, and so on) has its own Information Sharing and Analysis Center (ISAC)—private computer networks that allow private industry and government to share information and keep in touch in case of a large cyber attack. The centers send out crisis alerts to government agencies and member firms about attacks and vulnerabilities. For instance, the Water ISAC, launched in December 2002, is a centralized resource that gathers, analyzes, and disseminates threat information specific to the water community. It collects information from utilities' security incident reports, federal law enforcement, intelligence agencies, and public health and environment agencies and serves as a link between utilities and federal agencies.

- **Initiative D21**, a German public-private initiative, promotes cooperation between the government and industry concerning security-related topics, especially IT security.

While these initiatives are a step in the right direction, much more needs to be done. Intelligence sharing between the public and private sector is an entirely new terrain. For different reasons, both sectors have traditionally closely guarded intelligence information on threats and vulnerabilities. Getting to a point of institutionalized public-private information sharing will therefore entail daunting challenges (see box below).

### Challenges of Public-Private Information Sharing

- **Figuring out what to share:** Quickly and routinely separating unclassified information from classified information to pass along to the private sector.
- **Compromising sources:** Commercializing threat information and intelligence without compromising valuable intelligence sources or obstructing law enforcement efforts.
- **Privacy:** The difficulties of sharing information without violating privacy laws which prohibit the sharing of certain types of information between the sectors.
- **Lack of trust:** Firms worry that sensitive information such as a damaging hacker incident may become public and blemish corporate reputations or make those companies involved with the reported threat even more conspicuous and vulnerable to crimes. They want guarantees from government that threat information that may damage a company's reputation with stockholders, customers, and the general public will be exempt from public disclosure.

These and other issues need to be sorted out before robust intelligence sharing between the sectors will become routine. These four guidelines can help both parties work through the main issues involved in public-private information sharing (see Figure 11).

Figure 11. A Framework for Public/Private Information Sharing



Source: Deloitte Research

**Set goals.** Both sides need to establish what it is that they hope to achieve from sharing information. The chief security officers (CSOs), and others responsible for security in the private sector, want two-way information flow with the government. Many of them say that government agencies must do a better job understanding private sector needs. For its part, the private sector must identify the business drivers behind the need for various types of information and determine which government agency can best provide the specific types of information pertinent to their industry.

**Create a governance model.** Criteria spelling out requirements for each side need to be agreed upon at the outset. The inability to detail requirements and priorities and to establish standard protocols typically results in a lack of actionable intelligence.

**Establish protocols.** Government security and intelligence agencies have previously been criticized for their inability to classify and organize information and then disseminate it to the proper parties. Definitions and classifications are the first steps in improving this situation. Government entities need to institute strict guidelines on what should be produced and shared and how such sharing should take place.

**Mitigate risks.** The private sector must understand for what other purposes the information they provide to the government could be used. Legal contracts governing how various classifications of information may be used by both sides might even be necessary.

One promising model for public-private information sharing is the U.S. State Department's Overseas Security Advisory Council (OSAC). Begun in 1985, the collaborative partnership between U.S. multinationals and the State Department was formed to identify security risks in foreign locales. OSAC provides American firms with timely information to help them make decisions on how best to protect investments, facilities, personnel, and intellectual property abroad. Both private firms and government agencies are represented on the council.

## Provide Incentives for Companies to Invest in Security

### *Expand public-private partnerships on security initiatives*

Governments can also facilitate the transition to the secure economy by applying just the right mixture of carrots and sticks. Where it makes sense, companies with exemplary security practices could be given certain advantages by government agencies, such as liability protection, fewer inspections, reduced reporting requirements, tax incentives, lower compliance costs, and other privileges.

Similar incentives are already being offered via several government-industry initiatives. For example, after going through a validation process to prove that they have secured all aspects of their supply chain, companies participating in C-TPAT are entitled to certain privileges such as a reduced number of inspections at the border, electronic access to

customs data, their own account manager at Customs, and the ability to pay fees through a monthly statement instead of the current per-transaction method.

Several prominent public-private partnerships are also under way to improve food safety and security. In Australia, the National Livestock Identification System (NLIS), a combined government/industry venture, tracks individual animals from birth to slaughter for food safety, product integrity, and market access purposes. Meanwhile, the Canadian Cattle Identification Program traces individual animal movements from the herd of origin to slaughter. Businesses have strong incentives to participate in such initiatives. In addition to the specific privileges such as fast-lane access, the goodwill they generate with leading government officials may give them a better opportunity to weigh in early on any new requirements.

Lastly, governments can ease the costs of complying with new security requirements by providing extensive compliance assistance to the private sector. Security and customs agencies might consider emulating the U.S. Department of Labor (DOL) which helps firms understand and comply with government labor requirements through outreach, training, and by offering more than 30 online customized compliance assistance tools. Based on answers to a dynamically created series of questions, DOL's online expert advisors explain exactly what needs to be done to comply with a particular labor regulation. The tools save participating businesses hundreds of millions of dollars a year by providing them with customized compliance assistance reports that previously would have required days or weeks of research and analysis to generate.

## Promote Global Cooperation on Standards

### *Work with international bodies to harmonize security standards*

The ultimate nightmare scenario for businesses would be to have to comply with a hodgepodge of disconnected and incompatible country-specific security requirements as their goods move across the supply chain. Costs would skyrocket. Global trade would slow.

This scenario seemed plausible, if not probable, just a short time ago, as the European Community, various national governments, and some international bodies resisted aggressive efforts by the United States to set security standards. The highly public spat between the U.S. and the EU over attempts to require detailed information on every passenger from airlines before they entered the U.S. was just one indication of the deep tensions around security guidelines. International standards seemed like a pipe dream.

Fortunately, ample recent evidence suggests this is turning around. The major countries seem to have realized it's in their interest to cooperate on security. In areas from food to maritime security, momentum is building toward global standards (see Table 5). In the container security area, for

**Table 5. Emerging Global Security Standards**

Industry	International Body	Global Security Standard/Regulations
<b>Import/Export</b>	World Customs Organization (WCO)	Customs data model: common data sets for import and export manifests and goods declarations
<b>Aviation</b>	International Civil Aviation Organization (ICAO)	Mandatory aviation audits
<b>Shipping</b>	International Maritime Organization (IMO)	International Ship and Port Facility Security (ISPS) Code
<b>Financial Services</b>	Egmont Group: 84 nations provide forum for financial intelligence units (FIUs) to fight against financial crimes	UN Resolution 1373: calls on all member states to freeze assets of those who commit or attempt to commit or facilitate the commission of terrorist acts
<b>Food Safety</b>	CIES (The Food Business Forum)	Global Food Safety Initiative (GFSI)
<b>RFID</b>	Organization for the Advancement of Structured Information Standards (OASIS), Wireless Strategic Initiative (WSI)	None—three competing standards

example, the World Customs Organization (WCO) in June 2004 unanimously approved tough new cargo security standards modeled after the United States' Container Security Initiative (CSI).<sup>105</sup> Each of the 156 member nations of the WCO must now decide individually whether to adopt the standards.

Global standards have also been established to strengthen maritime security. The International Ship and Port Security Code (ISPS), which went into effect in July 2004, applies to all vessels over 500 tons engaged in international voyages and all port facilities serving such ships. The Code requires ships on international voyages and the port facilities that serve them to conduct a security assessment, develop a security plan, designate security officers, perform training and drills, and take appropriate preventive measures against security incidents.

The current momentum toward global standards cannot be maintained without the continued leadership of the G-8 countries, the EU, and international bodies such as the WCO, the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), and the World Trade Organization (WTO). Attention should be focused first on country adoption of the WCO standards and then on the promulgation of security standards in other high profile areas like air cargo, border crossings, and visa issuance. International standards and measures should be crafted with regard to maintaining and improving security and supply chain efficiency and aim at uniformity, simplicity, and ease of deployment from country to country.

## Toward a Secure and Prosperous Future

Companies can no longer afford to be complacent about security. For their own good and as critical warriors in the global security battle, they must prepare for the worst. What if there were reliable reports that a dirty bomb was being smuggled into the United Kingdom through a container and

the government reacted by shutting down the entry of any goods into the country for weeks? How should a firm react? What options would it have? Preparing for such scenarios is unpleasant, but absolutely necessary in this age of heightened threats.

And contrary to the conventional wisdom, better security and business value need not conflict. Being more secure can go hand in hand with maximizing shareholder value. Improved supply chain visibility, for example, has proven business benefits beyond security, from lower overhead and transaction costs to reduced theft. Strengthened cyber security and privacy protections help to reduce risk. Strong crisis response capabilities enhance brand.

On the other side of the table, as government officials focus more and more attention on reducing private-sector vulnerabilities, they must do a better job laying out the business case for security, taking into account both benefits and costs, providing the right mix of carrots and sticks and then communicating the new requirements to business.

For their part, legislators must take care to avoid falling into the trap of enacting security regulations that are so onerous that they would cause more harm to society than an attack itself. One bill proposed in the U.S. Congress, for example, would require logistics companies such as FedEx and UPS to examine every package they delivered. If enacted, the result would be the end of overnight delivery. Rigorous cost benefit analyses and extensive outreach to the private sector can help keep at bay trade-crippling legislative proposals.

The secure economy is here to stay. While the threats and the risks may never go away, by working collaboratively to bolster security, private firms and governments can make it a lot less likely that terrorists and others who would do us harm succeed.

# Appendix

## Security Regulatory Environment

### Aviation

Some of the strongest new measures in the aviation industry are in the United States where the American public lost some confidence in airline security after 9/11. In response to the 9/11 security breaches, the federal government federalized aviation security and mandated far stricter security measures in airports and on planes.

In Europe, where aviation security standards were more strict than in the United States prior to 9/11, a European Parliament regulation enacted in December 2002 called for all EU members to adopt common security measures mandated by the European Civil Aviation Conference. Each EU member must implement common security measures and verify them through audits.

Similarly, Japan, Hong Kong, Australia, mainland China, and Indonesia have all agreed to mandatory aviation security audits imposed by the International Civil Aviation Organization (ICAO). The Australian government has also mandated that 100 percent of checked baggage be screened for all international and domestic flights by December 31, 2004.<sup>106</sup>

Many countries have also turned to advanced technology to help secure airports. Chile's General Directorate of Civil Aviation (DGAC) has established Stage One, a latest generation screening system that has the ability to detect IED (improvised explosive device) components and examine 6,000 bags per hour. It also contains an intelligent system that can detect explosives and automatically reject suspicious luggage.<sup>107</sup>

Meanwhile, in Israel, where aviation security is widely considered the best in the world, El Al, the national airline, is defended from hijackings and other acts of sabotage by a stringent passenger screening system that uses both psychological profiling and high-tech equipment. Those passengers perceived to be high-risk after the initial screening go through more extensive screening that takes on average 57 minutes per passenger and involves personal interviews with security personnel, a search of all carry-on bags, and the use of sophisticated explosion detection devices on luggage. The procedures have been highly successful; the last hijacking of an El Al aircraft was in 1968.<sup>108</sup>

### Seaways and Ports

The goal of new requirements for container, port, and vessel security is to know ahead of time when the ships are coming in to port, what is in the containers, and where they're from.

Much of the pressure for heightened container security is being driven by the U.S. government. In February 2003, vessel arrival notification requirements in the United States were modified from 24 to 96 hours, and an advance manifest rule was imposed on carriers to submit cargo declarations for vessels bound for the country. The aim is to allow customs officials to be better prepared to identify and inspect higher-risk cargo.

Closely related to the container security initiatives are various government measures designed to protect ports and waterways from terrorist attacks. The 2002 U.S. Maritime Transportation Security Act (MTSA) imposes uniform standards of security throughout the U.S. port environment and creates new maritime safety and security

teams in San Francisco, Houston, New York, and St. Mary's, Georgia. The ultimate goal is to develop multiple, elite security teams capable of conducting rapid, nationwide response and deployment via air, ground, or sea.

Another important development is the Container Security Initiative (CSI), an effort by the U.S. Customs Service to secure the shipping industry from terrorism and large-scale accidents. While CSI is a voluntary partnership rather than a mandate, there are strong pressures on governments to agree to CSI rules at the risk of losing export business to the United States. Eighteen countries, including the Netherlands, Belgium, France, Germany, Italy, the U.K., Spain, and Sweden, have agreed to inspect selected export containers identified by U.S. Customs as posing a potential threat. U.S. Customs officers stationed in foreign ports use shipping data filed by carriers prior to departure to indicate to local customs officials which containers to target for x-ray and radiation scans. CSI is reciprocal: Countries like Japan and Canada have also stationed inspectors at U.S. ports to prescreen outbound shipments.

The downside of CSI? Heightened inspections can cause customs delays, which in turn can result in supply chain inefficiencies. To counteract such effects, the U.S. Customs Service is working with its foreign partners to implement advanced technology such as radio frequency identification (RFID) systems to streamline the inspection and customs process.

Globally, the International Ship and Port Security Code (ISPS) applies to all entities that could potentially be involved in a transportation security incident, including various tank vessels, barges, large passenger vessels, cargo vessels, towing vessels, offshore oil and gas platforms, and port facilities that handle dangerous cargo. Designed to strengthen and add additional protective layers of defense to port security, ISPS requires all nations to develop port and ship security plans, as well as requiring ships to display permanently marked identification numbers on their hulls and to keep a Continuous Synopsis Record (CSR) onboard showing vessel history.

### Border Security

The US-VISIT program in the United States requires visa holders to be digitally photographed and fingerprinted at ports of entry and to be checked against watch lists of terrorists and criminals. The key to making this system work efficiently without creating unduly long wait times is new technology like smart cards with RFID capacity which could send information about the holder of the smart card to the immigration inspector as she approaches the booth.

US-VISIT requires most foreign visitors traveling to America on a visa to have their two index fingers scanned and a digital photograph taken to verify their identity at the port of entry. These are then compared to watch lists of known terrorists and criminals. Other biometric identification techniques like iris scanning, facial recognition, and radio-frequency chips will also be explored for the purpose of tracking visitors entering and leaving the United States.

By employing networks of computer databases and biometric sensors for identification at sites abroad where visitors apply for visas to the United States, US-VISIT also seeks to supplant the nation's physical borders with virtual borders. DHS officials believe that if foreign visitors are properly screened through a global web of databases, the actual border guard becomes the last, rather than the first, point of defense.

In Europe, the Schengen Agreement provides for the gradual abolition of internal border controls.<sup>109</sup> The Schengen Agreement was signed by five member states of the European Union, France, the Federal Republic of Germany, and the Benelux countries. The Convention implementing the agreement was signed in 1990 and entered into effect in March 1995. To reduce the risks associated with free movement of people within the Schengen zone, the EU took the following compensatory actions: strengthened controls at the external borders of the signatories; harmonized visa, asylum and migration policies; created the Schengen Information System (SIS); and enhanced cooperation between the police, immigration and judicial authorities of the Schengen countries. Currently, 23 EU countries have incorporated the Schengen rules with Ireland and the United Kingdom opting out.

In June 2003, the EU Justice and Home Affairs Council called for expanding Schengen's information system.<sup>110</sup> The expanded system, nicknamed Schengen II, is expected to function similarly to US-VISIT by incorporating biometric measurements in new passports containing embedded computer chips. Furthermore, the updated information system will be linked to the visa identification system to more effectively track persons who pose a security threat.

In February 2004, Germany's largest airport, Frankfurt/Main, introduced a voluntary iris scanning program in which the biometric information is stored on the traveler's passport. One of the biggest trials for the use of iris recognition in airport security, the program involving Lufthansa passengers residing in any EU nation and Switzerland aims for faster cross-border checks for frequent flyers and increased security.<sup>111</sup>

The abolition of internal borders puts an even greater onus on strongly reinforcing the EU's external borders. The ten new EU member states that make up the eastern border of the EU now face the immense responsibility of securing that border. One challenge is dealing with possible restrictions on long-established patterns of cross-frontier movements of people and goods between the newly enlarged EU and non-EU countries. Before acceptance into the EU, many Eastern European countries had maintained liberal terms of entry with their eastern borders, a point of little comfort to countries like France and Germany that now must devolve their border security to the less developed former East Bloc countries.

The United Kingdom, which is not part of the Schengen zone, will reinforce its border through an electronic tracking system called eBorders. The goal: Modernize and integrate the management of passenger information in order to expedite the movement of people and safeguard the country against organized crime, terrorism, and illegal immigration.<sup>112</sup> A key issue centers on how to link the country's airports, seaports, and Eurostar terminals with a real-time passenger checking system. The Foreign Office has also introduced iVisa, which it hopes will eventually connect worldwide visa operations with U.K. immigration systems and incorporate biometric visas.

## Food

Governments are enacting tougher legislation, issuing new industry guidance, forming public-private partnerships, and devoting more R&D to food safety and security. In addition to requiring companies to give advance notice to U.S. officials for all food products to be consumed by humans or animals before the shipments arrive in the U.S., the 2003 Bioterrorism Act also requires domestic and foreign

food facilities that manufacture, process, pack, or hold food for humans or animal consumption in the U.S. to register with the Food and Drug Administration (FDA). With registration records, the FDA can quickly identify and locate affected food producers in the event of deliberate or accidental food contamination. The U.S. Department of Agriculture (USDA) is also pressuring U.S. food producers to voluntarily adopt new technologies that enable any individual animal to be traced back to its birthplace within 48 hours.

New EU food hygiene legislation will also go into effect in January 2005. Directive 178, Article 18 consolidates 17 existing hygiene directives across the EU.<sup>113</sup> Elsewhere, China has established a quarantine system for animal, plant, and special items and has formulated a list of harmful creatures. However, the country has yet to implement food trade-related electronic information sharing with relevant foreign government agencies.<sup>114</sup> Meanwhile, Chile also has a quarantine system that deters the entry and spread of transmissible diseases. The system is put into practice through risk analysis centers, health barriers at cargo and passenger entry points, and certification of quality and origin of national livestock products.<sup>115</sup>

## Health Care

In America, hospitals, doctors, insurance companies, and other health institutions must comply with the Health Insurance Portability and Accountability Act (HIPAA). Hospitals and other health care organizations could face steep government fines — not to mention the wrath of their customers — by failing to take adequate steps to secure their databases from cyber attacks.

## Financial Institutions

A key aim of the war on terrorism has been to shut down the money supply that finances terrorist organizations. Accomplishing this difficult task has meant putting much tighter controls and more stringent reporting requirements on financial institutions who have been asked, in effect, to help governments identify and close down suspicious financial activity. In Canada, for example, financial institutions must determine whether they have any assets belonging to a person or organization listed by the government as having committed or attempted to commit a terrorist act and, if so, to freeze all their assets.

In addition to Title III of the U.S.A. Patriot Act, "The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001," President George W. Bush signed Executive Order 13224 on September 24, 2001. This order expands the U.S. Treasury Department's power to target the financial support structure of terrorist organizations.

At the multinational level, Japan, Australia, and Canada are among those countries that have signed and ratified the 1999 International Convention for the Suppression of Financing of Terrorism. In addition, in September 2001 the UN Security Council unanimously adopted United Nations Resolution 1373 which calls on all member states to freeze the assets of those who commit, attempt to commit, or facilitate terrorist acts. Further, 84 nations are participants in the Egmont Group, a forum for the Financial Intelligence Units (FIUs) from various countries to improve support to their respective governments in the fight against financial crimes.

## End Notes

- <sup>1</sup> George V. Hulme, "Under Attack," *Information Week*, July 5, 2004, p.54.
- <sup>2</sup> "Disney Installs High-Security Anti-Terrorist Barricades." May 15, 2004. <<http://www.local6.com>>.
- <sup>3</sup> Debra van Opstal, "Private Sector Stepping up to the Plate on Security," *Competitiveness Watch*, Council on Competitiveness, November 5, 2003.
- <sup>4</sup> Paula Moore, "Threat of Workplace Violence Remains No. 1 Concern among U.S. Corporations," *Wichita Business Journal*, August 22, 2003.
- <sup>5</sup> George V. Hulme, "Spending to Fend Off Online Attacks to Grow," *CMP TechWeb*, December 29, 2003.
- <sup>6</sup> Deloitte, "The Unfinished Agenda—Transportation Security Survey," Deloitte Services LP, Aviation and Transport Services Industry, August 2004, p.4.
- <sup>7</sup> Chad Evans, "The State of Private Sector Security: A Year Out from 9/11," *Competitiveness Watch*, Council on Competitiveness, October 7, 2002.
- <sup>8</sup> Terrorism and Business Continuity Survey 2004, RAND Corporation and Janusian Security Risk Management Ltd, May 9, 2004, <<http://www.janusian.com/survey/>>.
- <sup>9</sup> Thomas P. Vartanian and Mark Fajfar, "Sarbanes-Oxley Act Underscores Importance of Information Security," *Community Banker*, June 1, 2004.
- <sup>10</sup> Of those companies surveyed, three quarters had been hit with unexpected delays in visa processing or arbitrary visa denials, and two thirds said that visa delays had hurt their bottom line. See: Edward Alden, "Visa Delays 'cost US business \$30bn,'" *Financial Times*, June 3, 2004.
- <sup>11</sup> Preserving these gains should be an important goal for governments and businesses as they work together to enhance security. Jack Riley, RAND Corporation, NABE teleconference, February 4, 2004.
- <sup>12</sup> Deloitte, "The Unfinished Agenda," p.4.
- <sup>13</sup> "President Highlights a More Secure America on First Anniversary of Department of Homeland Security," <<http://www.whitehouse.gov/homeland/index.html>>.
- <sup>14</sup> Remarks by Secretary Tom Ridge at the Center for Homeland Security's 2004 Homeland and Global Security Summit, March 31, 2004, Washington, DC.
- <sup>15</sup> In 2002, 60 percent of the total BMI budget of 3.5 billion euros was dedicated to domestic security, and in 2003 additional funds were allocated for the implementation of the Anti-Terror Act. See: "What can and what must Germans and Americans do to fight terrorism?" Speech by Otto Schily, Federal Minister of the Interior, February 02, 2003, <<http://www.eng.bmi.bund.de>>.
- <sup>16</sup> "About the New Department of Public Safety and Emergency Preparedness," <<http://www.psepc-sppcc.gc.ca>>.
- <sup>17</sup> "Government of Canada Announces \$8 Million to Strengthen Canadian Emergency Preparedness," <<http://www.psepc.sppcc.gc.ca>>.
- <sup>18</sup> "Japan Beefs Up Rail Security Following Threat," *The Milwaukee Journal Sentinel*, March 19, 2004.
- <sup>19</sup> "Sen Snowe Advocates Swift Action on 'Rail Transportation Security Act' States News Service," *States News Service*, April 1, 2004.
- <sup>20</sup> Patrick E. Tyler and Don Van Natta, "Europe Steps up Security Intelligence Officials had Expressed Fear over Rail Networks," *International Herald Tribune*, March 13, 2004, p. 1.
- <sup>21</sup> Air carriers and foreign air carriers that are not in compliance with the independent audit submission requirement after December 31, 2002 face civil enforcement. <[http://www.tsa.gov/interweb/assetlibrary/67\\_FR\\_66071.pdf](http://www.tsa.gov/interweb/assetlibrary/67_FR_66071.pdf)>.
- <sup>22</sup> ICAO set a deadline of November 2003 for installing new cockpit doors that are fortified against intrusions and small-arms fire or fragmentation devices. This deadline was seven months after the deadline for U.S. carriers.
- <sup>23</sup> July 1, 2004 was the international and domestic deadline for implementation of MTSA regulations & ISPS requirements. After the July 1, 2004 deadline, non-compliant operators are subject to having their operation shut down until an approved security plan is in place. <<http://www.uscg.mil/hq/g-m/mp/pdf/Part104Vesselsfaq.pdf>>.
- <sup>24</sup> Requires actions such as Ship Identification Number permanently marked on vessel hulls and the Continuous Synopsis Record (CSR) kept onboard showing vessel history.
- <sup>25</sup> The 24-Hour Advanced Manifest Rule is different from the 96-Hour Rule in that the 96-Hour rule was imposed by the Coast Guard after 9/11 and requires a 96-hour advance notice-of-arrival. Before 9/11, any ship coming into a U.S. port only had to give a 24-hour advance notice.
- <sup>26</sup> Starting July 1, 2004, only calves born after this date will have to be identified with an NLIS device before leaving property of birth. Starting July 1, 2005, all cattle, irrespective of age, will have to be identified with an NLIS device before leaving any property for any reason. <<http://www.agric.nsw.gov.au/reader/19968>> .
- <sup>27</sup> "Report on the Duty Visit to Study the Food Regulatory Systems in Japan," *Legislative Council of the Hong Kong Special Administrative Region*, January 2004, p. 10, <<http://www.legco.gov.hk/yr03-04/english/hc/papers/hc0430cb2-2190e.pdf>>.
- <sup>28</sup> The compliance deadline for federal banking agencies and Securities and Exchange was July 1, 2001. The compliance deadline for the Federal Trade Commission was May 23, 2003.
- <sup>29</sup> "Phase One Review: Network Visibility: Leveraging Security and Efficiency in Today's Global Supply Chains," A Smart and Secure Tradelanes White Paper, November 2003, p. 1, <[http://www.chainlinkresearch.com/parallaxview/whitepapers/SST\\_PhaseOneReport\\_Synopsis.pdf](http://www.chainlinkresearch.com/parallaxview/whitepapers/SST_PhaseOneReport_Synopsis.pdf)>.
- <sup>30</sup> Transportation Security Administration website. <<http://www.tsa.gov/public/display?content=090005198000c0be>> .
- <sup>31</sup> "Fact Sheet: Secure Trade in the APEC Region ('STAR')," White House Press Release, October 26, 2002, <<http://www.whitehouse.gov/news/releases/2002/10/20021026-8.html>>.
- <sup>32</sup> APEC website, <<http://www.apecsec.org.sg>>.
- <sup>33</sup> Bart Hobijn, "What Will Homeland Security Cost?" *Federal Reserve Bank of New York*, November 2002, p. 29.
- <sup>34</sup> Anna Bernasek, "The Friction Economy," *Fortune*, February, 3, 2002. <<http://www.fortune.com/fortune/investing/articles/0,15114,367800,00.html>>.
- <sup>35</sup> "Largely Unfunded U.S. Maritime Security Requirements have been Slammed as a 'Tax' on a Shipping Industry Already 'taking an enormous financial hit' by the Former Chair of the U.S. Federal Maritime Commission." *The Shipping Times*, Singapore, July 25, 2003.
- <sup>36</sup> Toby Shelley, "Shipping Industry Steams for Safe Haven: The Cost of Meeting New Security Standards is High and Those Affected have a July Deadline to Meet." *Financial Times*, April 15, 2004, p. 11.
- <sup>37</sup> Ibid.

- <sup>38</sup> "Department of Homeland Security, Bureau of Customs and Border Protection: Required Advance Electronic Presentation of Cargo Information, GAO-04-319R," GAO Report, December 18, 2003, <<http://www.gao.gov/decisions/majrule/d04319r.htm>>.
- <sup>39</sup> The government has collected \$2.45 billion over the past two years from the passenger screening fee. See: John Crawley, "US Wants Airlines to Keep Paying Security Costs." *Reuters News*, November 5, 2003.
- <sup>40</sup> Sara Kehaulani Goo. "Fuel Prices Hurt U.S. Airlines." *Washington Post*, April 29, 2004, p. A5.
- <sup>41</sup> "U.S. Airlines Balk at Security Cost Increases." *AirWise News*, April 28, 2004, <<http://news.airwise.com/stories/2004/04/1083186259.html>>.
- <sup>42</sup> "TSA Allocates \$2.3 Billion to U.S. Carriers to Offset Security Costs." Transportation Security Administration website, May 15, 2003, <<http://www.tsa.gov/publicdisplay?theme=44&content=0900051980027028>>.
- <sup>43</sup> "KLM Complains of Security Costs, Timeline for U.S. Flights." *Dow Jones International News*, March 24, 2004.
- <sup>44</sup> Edward Alden, "The Americas: Visa Delays 'Cost U.S. Business \$30bn.'" *Financial Times*, June 3, 2004, p. 4.
- <sup>45</sup> Ibid.
- <sup>46</sup> Edward Alden, "U.S. Counts the Costs of Securing its Borders," *Financial Times*, July 1, 2003.
- <sup>47</sup> Sarah Murray, "Visa Worries Deter Foreign Students," *Financial Times*, June 20, 2004.
- <sup>48</sup> John M. Doyle, "Rail Directive Boosts Operators' Costs but could Aid Security Equipment Vendors," *Homeland Security and Defense*, May 26, 2004.
- <sup>49</sup> "Feds Stepping up Security Against Rail System Terror," *Associated Press*, May 21, 2004.
- <sup>50</sup> Teresa Anderson, "Rail Security," *Security Management*, Aug 1, 2004, p. A12.
- <sup>51</sup> Russ Wiles. "Funds to Safeguard Against Laundering." *Chicago Sun-Times*, September 15, 2003.
- <sup>52</sup> Tamara Loomis. "Anti-Terrorism Compliance." *Legal Times*, May 19, 2003.
- <sup>53</sup> Patrick Tracey. "U.K. Drops Plans to Force Identity Checks on Current Customers." *BNA's Banking Report*, July 28, 2003.
- <sup>54</sup> Sara Kehaulani Goo, "Fuel Prices Hurt U.S. Airlines," *Washington Post*, April 29, 2004. Airlines contributed \$315 million in both 2002 and 2003.
- <sup>55</sup> "ICAO Aviation Security Plan of Action," <[http://www.icao.int/cgi/goto\\_atb.pl?icao/en/atb/avsec/overview.htm;avsec](http://www.icao.int/cgi/goto_atb.pl?icao/en/atb/avsec/overview.htm;avsec)> Total cost of \$17 million for period 2002 to 2004. About \$15 million of the total cost of \$17 million will have to come from contributions from member states, international organizations, and the civil aviation industry.
- <sup>56</sup> "Informing Regulatory Decisions: 2004 Draft Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities," Office of Management and Budget. This number is the result of adding up the costs for Area Maritime Security (\$477 million), Vessel Security (\$1.368 billion), and Facility Security (\$5.399 billion). The total, \$7.244 billion, is the cost for period 2003 to 2012.
- <sup>57</sup> "Combating Terrorism in the Transport Sector: Economic Costs and Benefits," Australian Government, Department of Foreign Affairs and Trade, Economic Analytical Unit, 2004, p. 23.
- <sup>58</sup> Shelley, "Shipping Industry Steams," p. 11.
- <sup>59</sup> Canada Gazette, <<http://canadagazette.gc.ca/partII/2001/20010815/html/sor294-e.html>>. The cost in Canadian dollars is CAD \$116,000. This figure was converted to USD on 7/14/04 using exchange rate 1CAD=0.756418 USD.
- <sup>60</sup> "Department of Homeland Security, Bureau of Customs and Border Protection: Required Advance Electronic Presentation of Cargo Information," U.S. General Accounting Office, GAO-04-319R, Washington, D.C.
- <sup>61</sup> "Anti-Money Laundering: A Brave New World for Financial Institutions," Published by Celent Communications LLC, September 27, 2002, <<http://www.celent.net/PressReleases/20020927/AntiMoneyLaundering.htm>>. To achieve compliance, the U.S. banking, securities, and insurance industries will spend combined total of \$10.9 billion through the end of 2005. The Patriot Act was enacted in October 2001, and the compliance deadline was April 2002. \$2.7 billion is the result of dividing \$10.9 billion by four years (2002 to 2005, including 2005).
- <sup>62</sup> "Prior Notice of Imported Food Under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002," GAO Report, October 23, 2003, <[www.gao.gov/decisions/majrule/d04194r.pdf](http://www.gao.gov/decisions/majrule/d04194r.pdf)>.
- <sup>63</sup> Tom Cavanaugh, "Security in Mid-Market Companies: The View from the Top," *Executive Action Number 102*, The Conference Board, New York, August 5, 2004.
- <sup>64</sup> Chris Mahoney, "Speed and Security: Coexistence in the Global Supply Chain," Speech to business leaders at the World Trade Center Detroit/Windsor in Detroit, MI, September 17, 2003.
- <sup>65</sup> Interview with Will Pape, CEO, AgInfolink, May, 2004. The firm in question was a client of AgInfolink.
- <sup>66</sup> Organization for Economic Co-operation and Development, "Security in Maritime Transport: Risk Factors and Economic Impact," OECD Directorate for Science Technology and Industry, Paris, July 2003.
- <sup>67</sup> Interview with Dan Purtell, President, Supply Chain Security Division, First Advantage Corporation.
- <sup>68</sup> Ajit Kambil, "Radio Frequency Identification (RFID): Critical Considerations for Manufacturers," *Deloitte Research Emerging Technologies Brief*, 2003.
- <sup>69</sup> Stephen Flynn, *America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), p.98.
- <sup>70</sup> Deloitte, "The Unfinished Agenda," August 2004. The transportation survey data was obtained from a major survey conducted by the U.S. Chamber of Commerce Statistics and Research Center on behalf of Deloitte in March through May of 2004. Survey participants represent 103 companies in the following industries: air cargo/passenger, maritime, rail, third party service/logistics providers, and trucking.
- <sup>71</sup> Adel Melek and Marc MacKinnon, "2004 Global Security Study," Global IT Risk Management and Security Services group, Deloitte and Touche, 2004. The data on the financial services industry was obtained in the first quarter of 2004. The survey targeted financial service providers such as banks, investment management companies and insurance firms in North America, Europe, the Middle East, Africa, Asia Pacific and Latin America. Respondents included 31 of the top 100 global financial services institutions ranked by 2002 assets, 23 of the top 100 global banks ranked by tier-1 capital, and 10 of the top 50 global insurers ranked by 2002 assets.
- <sup>72</sup> "Be Prepared," *The Economist*, January 24, 2004.
- <sup>73</sup> "How Will Insurers Deal With Their Most Expensive Catastrophe?" *Knowledge@Wharton*, Wharton Business School, May 7, 2003, p. 13.
- <sup>74</sup> "Corporate Brand Reputation Outranks Financial Performance as Most Important Measure of Success," World Economic Forum annual meeting survey, January 22, 2004, <<http://www.weforum.org/site/homepublic.nsf/Content/Corporate+Brand+Reputation+Outranks+Financial+Performance+as+Most+Important+Measure+of+Success+>>>.

- <sup>75</sup> Scott J. Glober, "Improving Transportation Security: U.S. Perception of Threat & Concepts for Responding," Unisys Corporation, August 1, 2003.
- <sup>76</sup> Tamara Kaplan, "The Tylenol Crisis: How Effective Public Relations Saved Johnson & Johnson," Pennsylvania State University, <<http://www.personal.psu.edu/users/w/x/wxk116/tylenol/crisis.html>>.
- <sup>77</sup> Helene Poirson, "Economic Security, Private Investment, and Growth in Developing Countries," International Monetary Fund Working Paper, African Department, Washington, DC, January 1998, p.3.
- <sup>78</sup> W. Enders and T. Sandler, "Terrorism and Foreign Direct Investment in Spain and Greece," *Kyklos*, vol. 49, 1996, pp. 331-352.
- <sup>79</sup> V. Nitsch and D. Schumacher, "Terrorism and Trade," paper for The Economic Consequences of Global Terrorism workshop, DIW/German Institute for Economic Research, Berlin Germany, 2002.
- <sup>80</sup> Mahoney, "Speed and Security," September 2003.
- <sup>81</sup> Robert Felton and Mark Watson, "Informed Change, *Directorship*, June 2, 2002, p.3.
- <sup>82</sup> "Be Prepared," *The Economist*, January 24, 2004.
- <sup>83</sup> "Power Companies Again Defend Response to Isabel," *Associated Press Newswire*, October 20, 2003.
- <sup>84</sup> Jamie Wellington, "Lawmakers Quiz Utilities on Hurricane Response," *Capital News Service*, October 21, 2003. <<http://www.newline.umd.edu/business/specialreports/isabel/powerpowwow102103.htm>>.
- <sup>85</sup> "FPL's Simple Storm Season Strategy – Plan as Though Another Andrew is Coming; Customers Also Are Encourage to Plan for Two-Week Service Outage – Just in Case," *Business Wire*, May 10, 2004.
- <sup>86</sup> "Internet Security – Risking Your Reputation," *Banking Technology*, October 31, 2003, p. 36 and "Internet Fraud," *Business Day (South Africa)*, July 23, 2003, p. 8.
- <sup>87</sup> Ibid.
- <sup>88</sup> Ron Irwin, "Corporate Social Investment and Branding in the New South Africa," *The Journal of Brand Management*, May 2003, vol. 10, no. 4-5, pp. 303-311(9).
- <sup>89</sup> "ABSA Reassures Internet Banking Customers," *Johannesburg Stock Exchange*, October 6, 2003.
- <sup>90</sup> "Beware Bank Card Fraud," *All Africa*, September 12, 2003.
- <sup>91</sup> ABSA website, [www.absa.co.za](http://www.absa.co.za).
- <sup>92</sup> "MessageOne Launches most Affordable Enterprise Emergency Notification and Escalation Service," *Business Wire*, June 29, 2004.
- <sup>93</sup> Flynn, *America the Vulnerable*, p. 61.
- <sup>94</sup> Clifford D. Shearing and Philip C. Stenning, "From the Panopticon to Disney World: the Development of Discipline," in *Situational Crime Prevention: Successful Case Studies*, (Albany, NY: Harrow and Heston Publishers), pp. 249-255.
- <sup>95</sup> Randy Koch, "A Secure Supply Chain Blueprint," *Unisys White Paper*, 2004, p. 5.
- <sup>96</sup> Michael Garry, "Securing the Food Industry," *Supermarket News*, August 11, 2003, p.39.
- <sup>97</sup> Ken Cottrill, "Changing Priorities" *Logistics*, June 30, 2003, p.13.
- <sup>98</sup> "World Security Services to 2006," *Freedonia Group Report*, April 2003.
- <sup>99</sup> Ibid.
- <sup>100</sup> "Agency Awards \$10 million for Five Homeland Security Projects," *Inside the Pentagon*, October 31, 2002.
- <sup>101</sup> "Distribution of Funding of 763 ATP Awards (Total Funding Dollars for 1990 – May 2004)," Advanced Technology Program, <<http://www.atp.nist.gov/eao/factsheet/distribution.htm>>.
- <sup>102</sup> Ibid.
- <sup>103</sup> "Agency Awards \$10 million for Five Homeland Security Projects."
- <sup>104</sup> Richard Sammon, "From IT to Air Filters, Security Fuels Boost in Federal Spending," *Kiplinger Business Forecasts*, May 6, 2003.
- <sup>105</sup> Gary Fields, "World Customs Body Urges Strict and Uniform Security," *The Asian Wall Street Journal*, July 5, 2004.
- <sup>106</sup> "Counter Terrorism Action Plan: Australia," Asia-Pacific Economic Cooperation (APEC), Counter Terrorism Task Force Meeting, August 20, 2003.
- <sup>107</sup> "Counter Terrorism Action Plan: Chile," Asia-Pacific Economic Cooperation (APEC), Counter Terrorism Task Force Meeting, August 20, 2003.
- <sup>108</sup> Jonathan B. Tucker, "Strategies for Countering Terrorism: Lessons from the Israeli Experience," Homeland Security Institute, March 2003, <<http://www.homelandsecurity.org/journal/Articles/tucker-israel.html>>.
- <sup>109</sup> The Schengen Agreement was signed by five member states of the European Union, France, the Federal Republic of Germany, and the Benelux countries. The Convention implementing the agreement was signed in 1990 and entered into effect in March 1995. To reduce the risks associated with free movement of people within the Schengen zone, the EU took the following compensatory actions: strengthened controls at the external borders of the signatories; harmonized visa, asylum and migration policies; created the Schengen Information System (SIS); and enhanced cooperation between the police, immigration and judicial authorities of the Schengen countries. See: Eiki Berg and Piret Ehin, "Schengen – Consequences for National Migration Policy," <<http://www.isp.org.pl/docs/PM/eng/Estonia/rep1esto.pdf>>.
- <sup>110</sup> Testimony of Theresa Papademetriou, Senior Legal Specialist, The Law Library of Congress, on the European Union at an oversight hearing on "Visa Overstays: A Growing Problem for Law Enforcement" before the United States House of Representatives, Committee on the Judiciary, Subcommittee on Immigration, Border Security, and Claims, October 16, 2003.
- <sup>111</sup> "Iris Recognition System Selected for German Border Control," *Asia Pulse*, February 16, 2004.
- <sup>112</sup> Sarah Arnott, "eBorders Project Takes First Steps," *Computing*, June 2, 2004.
- <sup>113</sup> "Consolidating and Simplifying EU Food Hygiene Legislation," Food Standards Agency, <<http://www.food.gov.uk/foodindustry/regulation/europeleg/eufoodhygieneleg/>>.
- <sup>114</sup> "Counter Terrorism Action Plan: China," Asia-Pacific Economic Cooperation (APEC), Counter Terrorism Task Force Meeting, August 20, 2003.
- <sup>115</sup> "Counter Terrorism Action Plan: Chile," Asia-Pacific Economic Cooperation (APEC), Counter Terrorism Task Force Meeting, August 20, 2003.

## About the Author

William D. Eggers  
Tel: 202 378 5292  
e-mail: weggers@deloitte.com

William D. Eggers is a Director in Deloitte Research. His research focuses on government reform and the intersection of the public and private sector in areas ranging from security to regulation. He is also a Senior Fellow at the New York-based Manhattan Institute for Policy Research and former appointee to the Office of Management and Budget's Performance Measurement Advisory Council (PMAC). The co-author of *Revolution at the Roots: Making our Government Smaller, Better, and Closer to Home* (The Free Press, 1995), he is also the author of two upcoming books: *Governing by Network: The New Shape of Government* with Stephen Goldsmith (Brookings Press, 2004) and *Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy* (Rowman and Littlefield, 2005).

## Acknowledgements

This study was really a team effort in every sense of the word. The study was the brainchild of Greg Pellegrino, Deloitte's Global Managing Director for the public sector. He is also directly responsible for many of the study's most important insights. The study would also not have been possible without the months of hard work from Deloitte Research interns Ani Ahn and Eleanor Keppelman. They both played a major role in all facets of the study and their work product was always of the highest quality. Deloitte Research colleague Dwight Allen (McLean) provided valuable observations and advice throughout the process and was instrumental in developing several of the figures and sections of the paper. Other helpful comments came from Deloitte colleagues Bob Campbell (Austin), Hans Bossert (Den Haag), Ajit Kambil (Boston), Carl Steidtmann (New York), Alessandro Cassinas (Milan), Heino von Schuckmann (Berlin), Marc Von der Linden (Dusseldorf), Peter Zimmerman (Den Haag), Rick Funston (Detroit), Bruce Beebe (Wilton, CT), Michael Raynor (Toronto), Peter Koudal (New York), Paul Mansell (London), Scott Ladd (New York), Dan Helfrich (Washington, DC), Lawrence Hutter (London), John Greaves (Chicago), Michele McGuire (Chicago), Mark Steinhoff (Boston), and Eli Racin (Tel Aviv). We would also like to thank the dozens of government officials, corporate executives, and security experts we interviewed for the study, particularly Al Martinez-Fonts, Brian Staples, Will Pape, Stephanie Race, Catherine Mann, and Gary Becker.

ISBN 1-892383-22-5

## Recent Deloitte Research Thought Leadership

- **Tracking RFID's New Wave to Gain Strategic Advantage**
- **Mastering Innovation:** Exploiting Ideas for Profitable Growth
- **Globalization and Energy Supply:** Strategic Risk in the 21st Century
- **Globalization at Risk:** Why Your Corporate Strategy Should Allow for a Divided and Disorderly World
- **Synchronicity:** An Emerging Vision of the Retail Future
- **Globalization Divided?** Global Investment Trends of U.S. Manufacturers
- **The Titans Take Hold:** Offshoring in the Global Financial Services Industry

## Deloitte Global Leadership

**William G. Parrett**  
Chief Executive Officer  
Deloitte Touche Tohmatsu

**Jerry Leamon**  
Global Managing Partner,  
Clients & Markets  
Deloitte Touche Tohmatsu

## For Further Information, Please Contact

### Deloitte Global Industry Leaders

**Aviation & Transport Services**  
**Libero Milone**  
Tel: +39 06 3674 9214  
e-mail: lmilone@deloitte.it

**Consumer Business**  
**Ed Carey**  
Tel: +1 312 374 3048  
e-mail: ecarey@deloitte.com

**Energy & Resources**  
**Chris Nicholson**  
Tel: +1 804 697 1516  
e-mail: cnicholson@deloitte.com

**Financial Services**  
**Jack Ribeiro**  
Tel: +1 212 436 2573  
e-mail: jribeiro@deloitte.com

**Life Sciences and Health Care**  
**Bob Go**  
Tel: +1 313 324 1191  
e-mail: rgo@deloitte.com

**Manufacturing**  
**Katsuaki Takiguchi**  
Tel: +81 (3) 6213 3631  
e-mail: ktakiguchi@deloitte.com

**Gary Coleman**  
Tel: +1 908 673 5280  
e-mail : gcoleman@deloitte.com

**Public Sector**  
**Hans Bossert**  
Tel: +31 70 337 2413  
e-mail: jbossert@deloitte.nl

**Greg Pellegrino**  
Tel: +1 617 437 2776  
e-mail: gpellegrino@deloitte.com

**Technology, Media & Telecommunications**  
**Igal Brightman**  
Tel: +972 3 608 5500  
e-mail: ibrightman@deloitte.co.il

## About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting, and financial advisory services—and serves more than one-half of the world’s largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other’s acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names “Deloitte,” “Deloitte & Touche,” “Deloitte Touche Tohmatsu,” or other related names.