

From the Knowledge Base of TranSystems' Legacy and Merger Firms



Enterprise-Wide Risk Management, Resiliency, Supply Chain Security and the Return on Investment

BY

Robert Tatum and Frank Galloway
TranSystems



EXPERIENCE | Transportation

Enterprise-Wide Risk Management, Resiliency, Supply Chain Security and the Return on Investment

By Robert Tatum and Frank Galloway

As 2008 unfolds, the economic climate has been catapulted as a primary concern. Corporations across the United States are absorbed with the economic upheavals, and otherwise continue to suffer from the repercussions of the subprime credit crisis. In such a time of turmoil, corporations are microscopically scrutinizing the bottom line, if not totally freezing or eliminating budgets. Where is the money going and is it spent wisely? What is the return on investment? Can the spending be deferred? Due to today's heightened budgetary scrutiny, corporations increasingly require a calculation of the value an investment will return. Given this situation, this report addresses the 'return-on-investment' issue, and provides information for the corporate risk manager to use when seeking funds for security investments.

The corporate security budget, at first glance, may appear an easy target for a funding cut. Since the tragic events of 9-11, the U.S. has been relatively incident free. In a period of calm, why should corporations upgrade their security technologies? Why should corporations plan for security? Why would corporations provide employee security awareness training? Security risk management, it appears, could take the back seat given the current security environment.

Just as corporations have been caught off guard financially, they could be caught off guard if a security incident occurred. High impact, low probability events are those that few corporations see coming, which can include catastrophic manmade and natural disasters (i.e., Hurricanes Katrina and Ike), product recalls, and the subprime credit crisis. Furthermore, corporations have an ongoing struggle with inventory shrinkage and other criminal threats. Obviously, terrorists and terrorism are not the only security threats.

Strategic Enterprise Risk Management

In a recent survey (Marsh | RIMS, 2008), corporate risk practitioners were asked to categorize their

approach to risk management as traditional, progressive, or strategic. The survey found that nearly two-thirds of respondents were not satisfied with the status quo— they aspire to be more strategic. The practitioner of strategic risk management views risk as something to optimize, not just to mitigate or avoid, taking an *enterprise-wide* view of risk and using it to *competitive* advantage.

Strategic firms that take an enterprise-wide consider their top three exposures as:

- brand and reputation,
- business continuity, and,
- regulatory / compliance

These firms are characterized by another interesting trait: they tend to do more. From education and training to investments in risk management, strategic firms are proactive in managing the risk to their organizations.

During the normal course of business, many issues demand attention, causing a loss of focus on events that may never affect an organization. However, companies need to be prepared for the unexpected, especially when such events can deal potentially devastating blows to their reputation, supply chains, and daily operations. Strategic enterprise-wide risk management balances daily necessities with forward thinking and planning.

Shrinkage: Investment in Physical Security Systems

Certainly, given the clear importance of risk management to corporations, spending on physical security system upgrades should be investigated. Unfortunately, a dearth of published information is available regarding the value of investing in physical security systems, security processes, and employee training (Beck, 2008).

However, among retailers at least, CCTV is considered the technology that performs at or beyond original shrinkage reduction expectations.

Measuring the Value of an Investment in Security

Risk managers and security directors are competing for a finite pool of funds within their organization. Also in competition for these finite resources are Human Resources, Real estate, Merchandising, Buyers, and any other group who is seeking funding for initiatives. Are the risk managers speaking the same language in terms of ROI or payback period? If they are not, security spending is a harder sell. (Palmer, 2001).

The language for measuring ROI has its origins in accounting and finance. Given the lack of consensus regarding what the actual terms mean when measuring the value of an investment in security, the terms are detailed below:

- **Capital Budgeting:** the process of planning expenditures that will generate income (or in relation to shrinkage, savings) over a given number of years.
- **Return on Investment (ROI):** The ratio of the net gain from a proposed security investment, divided by its total costs over a given time period.
- **Discounted Payback Period:** The period of time for the security investment to yield a positive cumulative cash flow (using Net Present Value).
- **Net Present Value (NPV):** a measure of the net benefit of the security project, in today's terms.
- **Internal Rate of Return (IRR):** The discount rate necessary to drive the NPV to zero; the value another investment would need to generate in order to be equivalent to the cash flows of the investment under consideration.

Palmer (2008, p. 20) suggests that risk managers use the accounting and finance terms above, and begin to determine how to measure the 'value' that the security spending will imbue to their organizations. Some potential measures are listed in Table 1.

Table 1: Possible measures for determining 'value' of security spending

Measure
Number of thieves caught directly by staff viewing cameras
Value of stock recovered
Number of thieves caught as a consequence of CCTV viewing
Number of thieves caught subsequently
Value of cash recovered
Value of stock losses
Number of staff caught directly by staff viewing cameras
Number of staff caught colluding with outsiders

Building a Business Case for Security Investment

Developing a sound case for investing in a particular intervention requires a series of steps to be completed (Beck, p. 28):

1. **Develop a Call to Action:** A persuasive Call to Action needs to clearly articulate the measurable benefits to the business of addressing a given issue. It also needs to show how this fits with corporate priorities and objectives. The Call to Action needs to be *measurable* and *realistic*.
2. **Identify the Problem:** Once a Call to Action has been identified, the next stage is to clearly identify the problem as it is affecting your business. This includes measuring the scale and extent, where the problem is located within the business and what the underlying root causes might be.
3. **Identify Possible Solutions:** Once the available data has been collected and analyzed and root causes identified, the next stage is to put together a list of possible solutions. Identification of a series of possible solutions is important in terms of generating credibility within the business.
4. **Test an Intervention:** Once a solution has been selected, it is important to understand what impact (if any) it will have on the business. This can be done in three ways: A

- Proof of Concept Trial, Pilot Study, or Field Experiment.
5. **Analyze Results:** Once an Intervention Test has been completed, the results can then be analyzed. It is important at this stage not to look simply at the difference in the test sites before and after the introduction of the intervention, but to compare the difference in values with those found in the control sites. Shrinkage data, for example, is notoriously variable and so the key purpose of the control sites in a trial is to provide a valid benchmark to compare the differences found in the test sites.
 6. **Prepare a Presentation for Senior Management:** Once the results have been analyzed from the Field Experiment, the next step is to prepare a presentation to senior management to make the case for using the intervention more widely in the enterprise. A key part of this presentation needs to include the financial costs and anticipated returns of investing in the proposed solution.
 7. **Establish an Implementation Plan:** If the presentation to senior management is successful, the next step is to develop an implementation plan to deliver the project. This requires the identification of all key stakeholders, selecting a project manager to oversee the implementation plan, setting a timetable and ensuring that employees are provided with training and resources to use the new intervention successfully.
 8. **Roll out the Intervention:** The primary task of the project manager is to ensure that the proposed intervention is introduced into at various sites successfully and with the minimum amount of interference. It is important that any training be provided at this stage to ensure that employees are fully prepared and understand the rationale for introducing the intervention. The project manager will need to work closely with the

suppliers to ensure compliance with agreed terms and conditions and act as an arbitrator between store management and installation staff.

9. **Evaluate the Impact:** Once the project has been rolled out to a selected site, it is important to monitor the intervention as results from trials may not always be seen over longer periods of time. This can in part be due to what is known as the 'Hawthorne Effect,' where changes occur not because of the intervention itself but because an experiment was carried out. Therefore, it is important continue to measure the performance of the intervention after it has been rolled out.

If the corporate risk manager follows the steps above, the path to justifying security spending will be much smoother. Security issues will have been defined; various interventions will have been tested and analyzed for results, and data will be available for senior management to use to make informed decisions regarding the security investment.

Supply Chain Risk Management & Collateral Benefits

The global economy depends on the unrestricted flow of goods and services. The global supply chain is the mechanism that facilitates it. Given its importance, the risks to a corporation's supply chain are a foremost concern.

A failure in a sub-process anywhere in a corporation's supply chain could disrupt production, create safety issues, spur product recalls, and/or hurt the bottom line. Unfortunately, most firms do not have a strategic process in place to protect their supply chain. Raising the profile of supply chain risk is a good way that risk managers can make a significant contribution to their firm's competitive footing, market share, credit rating, and reputation.

Recent US efforts to assess and minimize the risk involved in international transportation of goods,

Enterprise-Wide Risk Management, Resiliency, Supply Chain Security and the Return on Investment

include, among others, the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), the Advanced Manifest Rule (AMR) and the Free and Secure Trade initiative (FAST). International efforts include the publication of the ISO/PAS 28000:2005 standard “*Specification for security management systems for the supply chain*” by the International Organization for Standardization (ISO); the development of the Framework of Standards to Secure and Facilitate Global Trade by members of the World Customs Organization (WCO); a series of measures that were presented by the European Commission to accelerate implementation of the WCO Framework, including the Authorized Economic Operator (AEO) program; as well as various initiatives that were taken by the World Trade Organization (WTO) to better facilitate trade. (Peleg-Gillai, 2006)

In addition to these government activities, businesses are also proactively seeking ways to mitigate similar risks. For example, in order to achieve **organizational resilience**, some companies choose to increase flexibility of their operations (e.g., by using interchangeable or generic parts, cross-training employees, postponing differentiating process steps to a later point in the production process, or diversifying the supplier base and locations) or to modify the corporate culture (e.g., encourage continuous communication among informed employees, and empower employees to take necessary actions in the face of adverse events). Another approach involves designing facilities to withstand infrastructure loss and resume operations faster following a catastrophic loss.

For the purposes of this report we use the following definition of ‘resilience.’

Resilience: an organization’s ability to identify, respond to and resolve problems – especially problems that are related to breaches in security or to delays and other issues organizations may face while their goods are in transit thru the supply chain.

Resilience is also the capacity for complex systems to survive, adapt, evolve and grow in the face of turbulent change. The Resilient Enterprise is risk intelligent, flexible and agile (Council on Competitiveness, p. 11).

While these and other initiatives allow companies to maintain their level of operations and/or to reduce risks, they require considerable investments. Unfortunately, making a business case to justify security investments is difficult for many reasons already mentioned. Corporations are reticent to incur large security investments which exceed the minimum necessary. Among the reasons for this reluctance is that companies have concentrated on security initiative direct expenses, and not on the collateral benefits that can be captured from investments (Peleg-Gillai, p. 3), such as:

- Higher supply chain visibility
- Improved supply chain efficiency
- Better customer satisfaction
- Improved inventory management
- Reduced cycle and shipping time, and
- Cost reductions following the above-mentioned collateral benefits

When properly leveraged, investments in supply chain security may not only be offset to some extent by benefits such as those just mentioned. They can, in fact, be outweighed by such benefits, and can have an overall positive impact on the bottom line.

Furthermore, Peleg-Gillai (p. 4) found that many innovators in supply chain security reported significant benefits to include:

- **Improved product safety** (e.g., 38 percent reduction in theft/loss/pilferage, 37 percent reduction in tampering);
- **Improved inventory management** (e.g., 14 percent reduction in excess inventory, 12 percent increase in reported on-time delivery);
- **Improved supply chain visibility** (e.g., 50 percent increase in access to supply chain

Enterprise-Wide Risk Management, Resiliency, Supply Chain Security and the Return on Investment

- data, 30 percent increase in timeliness of shipping information);
- **Improved product handling** (e.g., 43 percent increase in automated handling of goods);
- **Process improvements** (e.g., 30 percent reduction in process deviations);
- **More efficient customs clearance process** (e.g., 49 percent reduction in cargo delays, 48 percent reduction in cargo inspections/examinations);
- **Speed improvements** (e.g., 29 percent reduction in transit time, 28 percent reduction in delivery time window);
- **Resilience** (e.g., close to 30 percent reduction in problem identification time, response time to problems, and in problem resolution time); and
- **Higher customer satisfaction** (e.g., 26 percent reduction in customer attrition and 20 percent increase in number of new customers).

Among the collateral benefits of supply chain security is the potential for a 90 percent reduction in theft/loss/pilferage and tampering, a 50 percent reduction in damages, 75 percent reduction in inventory and 90 percent cost savings attributed to improved visibility for the areas in which the security enhancements were put in place.

Wal-Mart's Supply Chain Resilience (Council on Competitiveness, p. 10)

It happens every spring: The snow starts melting, people trade in their winter parkas for swimsuits, barbecue grills are dusted off, and lawn mowers are started up. When this happens, customers expect their local Wal-Mart and Sam's Club to be ready for them as they buy the sunscreen, hamburgers, and lawn equipment for that first warm weekend.

Unfortunately, this shift occurs at a different time all across the country, and there is no way to peg it to a date on a calendar as one can with a holiday. That means that Wal-Mart's merchandisers and

transportation, logistics, and operations teams need to be ready to transition quickly, and in a manner that enables stores in Minnesota to continue stocking snow shovels while the Alabama stores start to stock flip-flops.

The same data management systems that allow Wal-Mart to meet changing customer needs during seasonal transitions, also allow them to react quickly to a disaster anywhere in the country, by flowing essential merchandise to the affected communities. This structure enables the right merchandise mixture as well: water, cleaning supplies and propane to communities in the strike zone; extra food, diapers and toiletries to towns with a sudden influx of evacuees.

This capability was most evident during Hurricane Katrina, when Wal-Mart was able to bring 66 percent of its stores in the affected region back into operation with 48 hours, and 93 percent within seven days. The company used its proprietary systems to start planning alternative routes and emergency staging areas—even while Katrina was still a tropical depression in the Atlantic Ocean. An automated inventory management system created visibility into the location of needed resources. And, since every truck is equipped with on-board computer technologies, shipments could be redirected at any time.

This kind of supply chain sophistication could not have been justified solely on disaster preparedness grounds. Disaster management is a key side-benefit of supply chain resilience, and the nation a key beneficiary. But its investment is rooted in enhanced productivity, inventory visibility, and supply chain continuity and flexibility, all of which are core to competitive advantage.

What Risk Managers Should Know

Globalization, technological complexity, interdependence, and speed are fundamentally changing the kind of risks and competitive challenges that companies— and countries—face. The

repercussions of a catastrophic event can quickly resound throughout a corporation's supply chain. Increasingly, disruptions can come from unforeseen directions with unanticipated effects. Global information and transportation networks create interdependencies that magnify the impact of individual incidents. These new types of risk demand new methods of risk management.

Resilience or Protection?

The focus should be on risk management and resilience, not security and protection. Resilience—anticipating risk, limiting impact, and recovering quickly—should be the objective of economic security and corporate competitiveness. The foundation for the business case for investment in resilience is that the security initiative should address a wide variety of business risks. It cannot be based solely on the possibility of disaster. In fact, most of the investments that leading organizations are making—investments that can run in the hundreds of millions of dollars—are aimed at managing the risks they face on a day-to-day basis (Council on Competitiveness, 2007).

For example, supply chain flexibility, the hallmark of Wal-Mart—enabled the company to operate despite the devastation wrought by Hurricane Katrina. Ironically, supply chain flexibility was not specifically created to cope with disaster. Rather, Wal-Mart's significant investments in RFID tags, software, and staging centers were intended to meet the day-to-day complexities of customer demand. But in the process, Wal-Mart's supply chain resilience also created extraordinary disaster management.

Regulatory Solutions Often Reinforce Risk Silos

For companies, an infinite number of disruption scenarios exist for a finite number of outcomes. Causes count less than creating the agility and flexibility to mitigate risks and manage outcomes.

Government, however, tends to see different categories of risk—terrorism and natural disaster, climate change, worker safety, and governance—as different problems requiring separate sets of

regulatory solutions. In today's risk environment, three potential problems can result:

- It often creates a 'check the box' response that is at odds with the need to create value by managing risk on an enterprise-wide basis.
- Because risks cascade across networks and private enterprises in complex ways, risk silos may actually increase risk exposure.
- It sets up the potential for inconsistent and often overlapping sets of regulatory requirements, which raise cost and complexity without actually improving outcomes.

What Should CEOs and Boards Know?

Enterprise Risk Management can be turned into a competitive advantage. Businesses make money by taking risks. They lose money by failing to manage them. A study by Deloitte Research (2006) indicates that many of the largest losses in value among the world's largest global companies resulted from management's failure to manage risk effectively and systematically. The study found that most firms were exposed to more than one type of risk—whether strategic, operational, market or financial — and failed to manage the relationships among the various risks. Actions taken to address one type of risk had the potential to increase exposure to other types of risk.

The failure to manage risk on an enterprise basis takes a huge toll. Between 1994 and 2003, almost half of the Fortune 1000 global companies suffered some kind of operational risk incident causing more than a 20 percent decline in share prices. And the value losses were often long-standing. By the end of 2003, share prices for one-quarter of the companies had not recovered to their original levels.

Managing Operational Risks is Key

The business equivalent to homeland security and critical infrastructure protection is operational risk management—a domain that many executives view

Enterprise-Wide Risk Management, Resiliency, Supply Chain Security and the Return on Investment

as the most important emerging area of risk for their firms. Increasingly, failure to plan for operational resilience can have “bet the firm” results.

- Research on supply chain resilience demonstrated that the 835 companies that announced a supply chain disruption between 1989 and 2000 experienced 33 percent to 40 percent lower stock returns than their industry peers, regardless of industry, cause of disruption or time period. Such firms experienced 7 percent lower sales growth and 11 percent higher costs. Changes in operating income, sales, total costs and inventories remained negative in the two years after the problems were disclosed.
- 25 percent of companies that experienced an IT outage of two to six days went bankrupt immediately. Ninety-three percent of companies that lost their data center for 10 days or more filed for bankruptcy within a year.

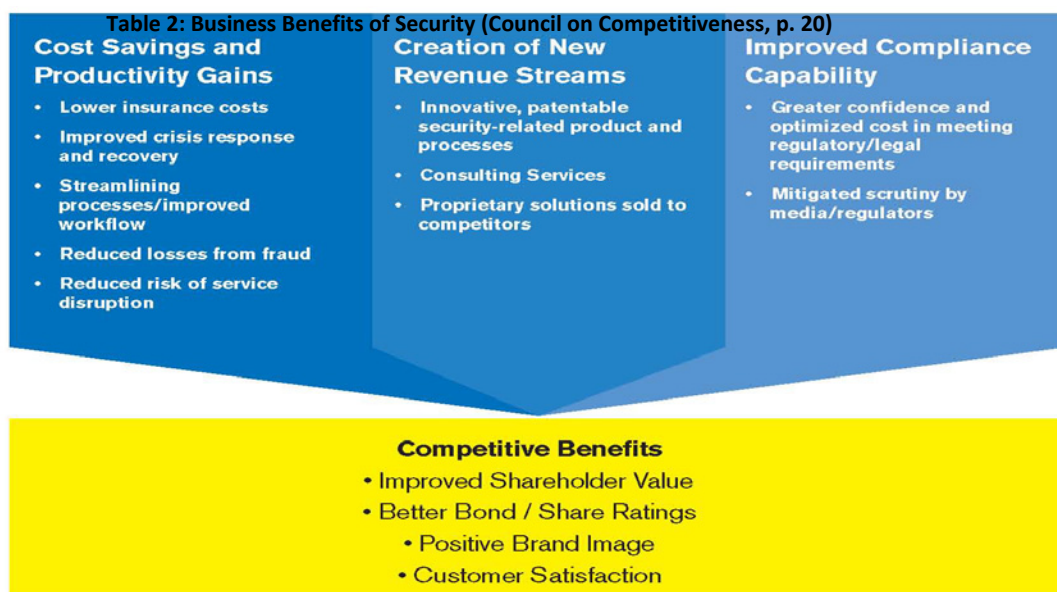
Operational Risks Remain Stove-piped and Under-measured

Different aspects of operational risk—physical and employee security, environmental health and safety, IT security, business continuity, disaster management, supply chain security, energy supply and quality— are frequently separated from one another within the organization, and sometimes delinked from overall corporate risk management.

On the financial side, there are increasingly sophisticated systems that measure market and credit risk— often using sophisticated algorithms and supercomputers to model risk exposure. By contrast, although operational risks are arguably at least as complex, operational risk exposure tends to be measured by checklists, which are often based on experience and instinct. In fact, boards are not as comfortable with their operational risk management as their financial risk management.

Industry Continues to Face a Risk of Reactive Regulation

Given that six years have passed since 9/11, it is tempting to believe that the danger of a major attack on the United States has abated. Unfortunately, a successful and devastating attack on U.S. soil remains the gold standard for global terrorism. To date, efforts to regulate security have been incremental and sector-specific. But regulatory incrementalism could become a regulatory avalanche if a major attack occurs and industry has not taken the necessary steps build up resilience.



Best Practices Among the Leaders

The challenges are not insurmountable. With ingenuity, innovative solution to challenges can be found. Some of the largest corporations in the US agree that the following best practices have played a role in their successful approach to risk management:

- **Walk the Talk at the Top:** Enterprise risk management requires an enterprise-wide approach, and that means that the impetus for change has to come from the top. The first steps are to connect the organizational silos and embed risk management in day-to-day business operations, to engage the entire workforce, and to create cultural change.
- **Treat Risk as a Continuum:** One of the limitations of most organizations is that risks are managed in silos, not strategically. Emergency preparedness is handled separately from business continuity, which in turn is not always part of strategic risk management. This fragmented approach impedes a clear understanding of the tradeoffs between different risk management strategies (avoid, accept, mitigate, transfer) and the different kinds of investments that can be made to implement those strategies.
- **Taking a Systems Approach:** Business continuity requires a systems approach that identifies potential weak links and how disruption might unfold throughout the organization. Sometimes, the ability to map business continuity not only helps to understand the modes of failure, but it clarifies business processes in ways that enhance efficiency or streamline costs.
- **Manage with Metrics:** It is often said that you manage what you can measure. A resilient enterprise needs to adopt a common definition of resilience and measurement framework that supports the operational and cultural values of the organization. An enterprise must quantify

just how resilient it is before adopting strategies to improve or leverage resilience.

- **Harness Technology to Reinforce Resilience:** Technology creates new vulnerabilities, but strategic applications of technology also can reinforce a company's ability to anticipate problems, weather turbulence and respond to crises. Nowhere is this more evident than in the IT arena. Organizations that focus on protecting the keys to the kingdom (increasingly their data and IT systems)—and use that capability to monitor their operations—do better across a variety of measures: security, business continuity, efficiency and customer confidence.
- **Put Plans in Place that Anticipate:** With so many different permutations of things that can go wrong, it is impossible to plan for every contingency. The leading companies are putting plans in place to manage outcomes, rather than specific scenarios. They are creating a capabilities-based approach.

Customs-Trade Partnership against Terrorism (C-TPAT)

It is apparent the participation in C-TPAT, and by extension in enterprise-wide risk management, corporations are becoming more resilient. In a recent survey, C-TPAT members cited the many benefits for joining the program (Diop, 2007).

- **Benefits Outweigh Costs:** More than half (56.8%) of businesses indicated that C-TPAT benefits outweighed the costs.
- **Reduced Inspections:** More than one third (35.4%) of Importers reported that their participation in C-TPAT has decreased their number of U.S. Customs and Border Protection (CBP) inspections. In a follow up question, these importers indicated that their

number of CBP inspections decreased by more than half (51.7%).

- **Increased Supply Chain Visibility & Lead Time Predictability:** Importers said that their participation in C-TPAT has increased their supply chain visibility and nearly one quarter (24.3%) indicated that their participation in C-TPAT has increased their ability to predict lead-time. Nearly 3 out of 10 Importers (28.9%) reported that their participation in C-TPAT has decreased the disruptions in their supply chain.
- **Decreased Wait-Time at Border:** Of highway carriers, 41.5% reported that their participation in C-TPAT has decreased their wait times at the borders.
- **Risk Management Improvement:** The vast majority (81.3%) of businesses that had a formal system in place for assessing and managing supply risk agreed that their businesses' ability to assess and manage supply risk has been strengthened as a result of joining C-TPAT.
- **Improved Supply Continuity and Contingency Plans:** Three quarters (75.2%) of businesses that had formal supply continuity and contingency plans before joining C-TPAT reported that their supply continuity and contingency plans have been strengthened as a result of joining C-TPAT.
- **Remain with C-TPAT:** While more than one-third (38.4%) of businesses indicated that their management was concerned about the potential impact on cost when their companies were considering joining C-TPAT, the vast majority of businesses indicated they have never considered leaving the C-TPAT program (91.5%) and that they would definitely remain C-TPAT compliant (78.1%).

Conclusion

Understanding the big picture on risk enables companies to prioritize spending on security investments. In our complex world of interdependencies, armchair decisions no longer suffice. The new risk paradigm requires business teams to integrate their strategies, and bring their varying perspectives to the table. Rather than addressing every disaster scenario, building up capacity to respond will increase resilience no matter what the disruption. Enterprise resiliency, once it becomes a part of the operations and culture of an organization, can provide strategic competitive advantage and confidence to pursue new opportunities. This paper demonstrates the importance of professionalizing risk management and the benefits of security investments. It has focused on trying to establish how risk managers should measure the impact of security investments within their business environment. It has tried to create clarity in the meaning of the terms used, the types of variables that can and should be collected to measure different types of interventions, and the way in which a business case should be assembled to persuade a business to invest in a particular solution. To this end, the majority of risk managers today are turning more and more to an enterprise-wide approach to risk management.

TranSystems believes that you find something of value in this report. We believe the articles and surveys we have reviewed represent the best ideas that can serve as a meaningful discussion point and education tool for companies as they discuss their risk management direction.

Bibliography

Beck, A. (2008). *Preventing Retail Shrinkage: Measuring the 'Value' of CCTV, EAS and Data Mining Tools*. Leicester: University of Leicester.

Council on Competitiveness. (2007). *The Resilient Economy: Integrating Competitiveness and Security*. Washington: The Council on Competitiveness.

Deloitte Research. (2006). *Disarming the Value Killers*. Deloitte.

Diop, A. (2007). *C-TPAT Partners Cost/Benefit Survey: Report of Results*. U.S. Customs and Border Protection, University of Virginia Center for Survey Research.

Marsh | RIMS. (2008). Viewing Risk Management Strategically. (T. Walsh, Ed.) *Excellence in Risk Management, An Annual Survey of Risk Management Issues and Practices*, V.

Palmer, W. (2001, Fall). Return on Investment: Turning Accounting Rules to Management Tools. *Loss Prevention*.

Peleg-Gillai, B. (2006). *Innovators in Supply Chain Security: Better Security Drives Business Value*. Stanford: Stanford University and The Manufacturing Institute.