



The Business Case for Preparedness

An Annotated Bibliography

Overview

This annotated bibliography provides organizational decision makers with a series of arguments to support the business case for preparedness.

InterCEP understands preparedness from an all-hazards perspective to encompass a variety of business functions and concepts such as: risk management, enterprise risk management, corporate resiliency, business continuity planning, disaster recovery, IT and physical security, emergency preparedness, and so on. We understand the business case in the general terms of value creation, as return on investment (ROI), profit, revenue, asset protection, etc.

The question driving this research activity is: why would investments in preparedness make business sense? In an effort to see how this question is currently being answered in the field, InterCEP searched the Internet and other electronic databases for business research and academic journal articles. From an initial set of several hundred publications, we selected those that provide clear arguments to support action by managers, executives and decision makers.

As a research effort, this annotated bibliography is only a first step toward a meta-analysis of how the business case for preparedness is currently evolving in the field. InterCEP therefore solicits feedback from readers of this bibliography – what sources have we missed? Have we properly understood and annotated the sources we've found? We intend to incorporate feedback and update this document with additional sources on a regular basis.



Table of Contents

The bibliographical sources are organized in the following sections:

- General Management.....3
- Business Functions.....22
 - Information Technology.....22
 - Supply Chain Management.....27
- Vertical Industries.....37
 - Financial Services.....37
 - Chemical.....41
 - Energy.....42
 - Aviation.....44
- Regional Economic Resilience.....45

Research Team

Primary research to identify and annotate the sources presented here was undertaken by Eknor Salaria, InterCEP Intern, during the summer of 2007. The effort was directed and supported by InterCEP Director, Bill Raisch; Associate Director, Matt Statler; and Program Associate, Margaret Della.



GENERAL MANAGEMENT

1. “Risks That Matter”, Dr. Deborah Pretty, Oxford Metrica, 2002.

InterCEP Highlight: For Global 1000 firms, there is a high probability of a crisis resulting in substantial decline of stock price during any five year period. How management responds is “destiny determining” for both the company and its CEO.

Key Points:

- The study analyzes the Global 1000 portfolio to examine extreme shifts in corporate stock price due to crises events.
- “The majority of sudden negative value shifts were driven by a failure to adapt to changes in the business environment, customer mismanagement and poor investor relations.”
- “There is a 40% chance of experiencing a negative shareholder value shift of over 30% (relative to the market) in a five-year period.”
- “...the research indicates that the ways in which CEOs manage the aftermath of corporate crises are significant determinants of share price recovery... Given the prevalence of these major value shifts, and the ‘destiny-determining’ nature of the value recovery patterns, ongoing management of the underlying events and their consequences becomes a priority issue for CEOs and investors.”
- “...these shifts in shareholder value tend to be sustained, and management of the underlying events emerge as “destiny-determining” for the firm, i.e., defining the likely future shareholder value performance and, therefore, reputation of the incumbent CEOs.”
- “The larger (Global 500) firms in the portfolio experienced two-thirds of the negative value shifts. Large firms, therefore, are in no way immune to sudden falls in value and appear to have even more to gain from effective risk management than the smaller firms.”
- “Overall, the CEO and the Board should take explicit ownership for the management of the drivers of value and associated strategic risks, and regularly review the performance of the overall risk management and control infrastructure. By doing so, they should be rewarded by sustained growth and protection of shareholder value”

Link: <http://www.oxfordmetrica.com/pdf/RisksThatMatter.pdf>



2. “Improving Risk Quality to Drive Value”, Oxford Metrica, FM Global, 2003

InterCEP Highlight: Firms that invest in and manage their property risks effectively tend to also create value for the firm.

Key Points:

- “The premise of this study is that a company need not experience a disruption to its business to demonstrate the value of investing in risk quality.”
- “This research provides the first empirical evidence that there is a clear correlation between companies’ risk quality and their financial performance. In the context of this study, risk quality is defined in terms of property risk management. It is driven by the core operational activities of a business, the physical location of those activities, and how they are managed and protected. The research identifies a strong correlation with value and provides evidence for what is intuitively understood but, to-date, has not been demonstrated quantitatively. The research finds that diligently pursuing property risk improvement practices is a characteristic of value-creating firms. Risk quality is demonstrated to be a core component of effective corporate governance policy and value management.”

Link: <http://www.oxfordmetrica.com/pdf/OMRiskQualityReport.pdf>

3. “The Impact of Catastrophes on Shareholder Value”, Rory F. Knight & Deborah J. Pretty, Oxford Metrica, 1996

InterCEP Highlight: How much insurance a company purchases doesn’t help in recovering the loss of shareholder value after a crisis; instead quality management and contingency planning are vital.

InterCEP Highlight: Effective management of crisis by corporate management can actually lead to an increase in shareholder value.

Key Points:

- The paper examines the harmful impacts catastrophes pose to corporations including the possibility of never recovering from the damage. Impacts on



shareholder value and survivability are discussed along with the presentation of specific case studies.

- “This research presents evidence which suggests that a firm’s recovery of shareholder value immediately following a catastrophic loss is independent of the presence of insurance cover. This raises interesting issues for the consumers (companies) and the providers (insurers and brokers) of risk management services... This suggests that a company’s insurance strategy should not be considered in isolation and should not be viewed as a substitute for high quality risk management and contingency planning systems and procedures.”
 - “...the issue of management’s responsibility for accident or safety lapses appears to explain the shareholder value response. By contrast, whether the losses were fully covered by insurance does not appear to have much influence.”
- “Why would some catastrophes lead to an increase in shareholder value? One explanation from our research is that there are two elements to the catastrophic impact. The first is the immediate estimate of the associated economic loss. The second hinges on management’s ability to deal with the aftermath. Although all catastrophes have an initial negative impact on value, paradoxically they offer an opportunity for management to demonstrate their talent in dealing with difficult circumstances. Effective management of the consequences of catastrophes would appear to be a more significant factor than whether catastrophe insurance hedges the economic impact of the catastrophe.”
- Example of a non-recoverer: Union Carbide- “Poor safety measures, the storage of large quantities of lethal gas (methyl isocyanate) at the wrong temperature, the accidental or deliberate introduction of water to one of the gas storage tanks, confusion in detecting a rise in pressure in the tank and ineffective response to its detection - all these factors are believed to be responsible for the gas leak tragedy at Union Carbide’s chemical plant in Bhopal, India.”
- The Bhopal incident cost the company more than \$527 million.
Cumulative abnormal returns at 50 days (-29%)
Cumulative abnormal returns at 6 calendar months (-29%)

Link: www.nrf.com/Attachments.asp?id=12546

**4. “Transform. The Resilient Economy: Integrating Competitiveness and Security”,
Debra van Opstal, Council on Competitiveness, 2007**

InterCEP Highlight: Due to many factors, the level of risk has increased for societies and organizations. Furthermore, these risks are increasingly interrelated so that disruptions in one area can cascade and create disruptions in other areas.



InterCEP Highlight: Corporate resilience will be a competitive advantage in the 21st century. Some companies, such as Waste Management, have been able to profitably sell their own internal resilience solutions to others.

Key Points:

- “Globalization, technological complexity, interdependence, terrorism, climate and energy volatility, and pandemic potential are increasing the level of risk that societies and organizations now face. Risks also are increasingly interrelated; disruptions in one area can cascade in multiple directions.”
- “The ability to manage emerging risks, anticipate the interactions between different types of risk, and bounce back from disruption will be a competitive differentiator for companies and countries alike in the 21st century.”
- “The failure to manage risk on an enterprise basis takes a huge toll. The study [Deloitte Research. “Disarming the Value Killers.” Deloitte, February 2006] found that almost half of the 1000 largest global companies suffered declines in share prices of more than 20 percent in a one-month period between 1994 and 2003, relative to the Morgan Stanley Capital International (MSCI) World Index. 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.”
- Waste Management as an example of a resilient establishment: “After 9/11 and a break-in a few months later at a landfill in Cut and Shoot, Texas, that destroyed half a million dollars in heavy equipment, Waste Management began to investigate the benefits of a state-of-the-art security operations center. It found that its own security was inconsistent across its 2,000 facilities. Some facilities lacked alarms altogether, and other alarms were broken or not in use. So, the company created the Life Safety Control Center (LSCC) and deployed smart video and alarm technologies to monitor intrusions into secured areas, as well as to monitor for fire or workplace violence... And from a competitiveness point of view, Waste Management is demonstrating that good security can become a bottom-line benefit. Waste Management now actively markets these capabilities to other small- and medium-sized companies that would rather outsource these costs effectively than make the capital investments in their own monitoring centers. Despite the considerable capital costs, LSCC’s year-over-year productivity and financial return has increased—from \$490,000 in 2004 to more than \$5 million in 2006.”

Link: <http://www.compete.org/pdf/Transform.TheResilientEconomy.pdf>



5. “The Value of Resilience”, Council on Competitiveness, Council on Competitiveness, 2006

InterCEP Highlight: Corporate resilience is a contributor to profitability, shareholder value and competitiveness.

Key Points:

- “Resilience is a shareholder value issue.”
- “Almost half of the one thousand largest global companies failed to manage risk systematically and suffered declines in share prices of more than 20% in a one month period between 1994 and 2003. Roughly one-quarter took more than a year for their share prices to recover, and sometimes much longer (*Deloitte Research, 2005*).”
- “As the global footprint of firms expands, so too do the risks they face on a daily basis. Extended supply chains, technology interdependencies, IT vulnerabilities, mutating viruses, turbulent geo-politics, flat world economics and even weather phenomena all combine to make doing business --- well, a risky business.”
- “For firms, resilience in the face of increasing risk – the ability to avoid, deter, protect, respond, and adapt to market, technology and operational disruptions – is becoming a linchpin of profitability, shareholder value and competitiveness.”

Link: <http://www.compete-resilience.org/index.php?mp=5&doc=56>

6. “Navigating Risk — The Business Case for Security”, Thomas E. Cavanagh, The Conference Board (Purchase required), October 2006

InterCEP Highlight: Effective risk management and security can prevent business disruption. It can also lower costs, enhance corporate reputation value and improve overall business performance.

Key Points:

- “In order to gauge acceptance of the business case for security, the U.S. Department of Homeland Security (DHS) sponsored a survey of senior corporate decision makers that was undertaken by The Conference Board. The survey purposely did *not* include security directors, risk managers, or chief information security officers in the sample. Rather, the focus was on



determining support for security initiatives among executives whose responsibilities do not ordinarily include security functions.”

- “The companies that participated represent a cross section of the American business community. A total of 113 firms were in critical infrastructure industries as defined by the U.S. Department of homeland security, and 93 were in non-critical industries; the remaining seven could not be classified. ..51 respondents were companies with less than \$250 million in annual sales, 47 with sales between \$250 million and \$1 billion, 63 with sales between \$1 billion and \$5 billion, and 49 with sales of \$5 billion or more. There were 41 companies with less than 500 full-time equivalent employees, 63 with 500 to 2,499 employees, 50 with 2,500 to 9,999 employees, and 58 with 10,000 or more employees.”
- “Senior executives were asked which metrics they found especially helpful in determining the appropriate level of spending for security in their companies. In general, the most useful metrics were those which enable executives to determine how much a security problem would cost the firm in terms of liabilities or foregone business. The most helpful metrics were the cost of business interruption, cited by 64 percent of executives; vulnerability assessments (60 percent); and benchmarking against industry standards (49 percent). Another group of helpful metrics was explicitly related to insurance costs, such as the value of facilities (mentioned by 44 percent), the level of insurance premiums (39 percent), and the cost of previous security incidents (34 percent).”
- “In sum, enterprise risk management is becoming a vital element in the rebranding of security as a corporate function. Security needs to be seen as a source of value, and not just a cost center within the company. Security can avoid cost and prevent disruption of the business. It can also add intangible value to the brand by serving as a marker of performance excellence and a symbol of concern for the integrity of products and the safety of customers and employees. Employing the concepts and terminology of risk management can enable security executives to more effectively perform their jobs and, in so doing, improve the performance of their companies in the marketplace.”

Official Website:

<http://www.conference-board.org/publications/describe.cfm?id=1231>

Website with abstract:

<http://www.conference-board.org/publications/describe.cfm?id=1231>

Article summarizing key findings and stats:

<http://www.continuitycentral.com/news02885.htm>



7. “The Business of Resilience: Corporate Security for the 21st Century”, Rachel Briggs and Charlie Edwards, Demos, 2006

InterCEP Highlight: Security is a new source of competitive advantage impacting reputation, corporate governance, regulation, corporate social responsibility and information assurance.

Key Points:

- “The business of security has shifted from protecting companies from risks, to being the new source of competitive advantage . . .”
- “Many of the threats, such as terrorism, organized crime and information security, are asymmetric and networked, making them more difficult to manage. There is also greater appreciation of the interdependence between a company’s risk portfolio and the way it does business: certain types of behavior can enhance or undermine an organization’s ‘license to operate’, and in some cases this can generate risks that would not otherwise exist. As a result, security has a higher profile in the corporate world today than it did five years ago. Companies are looking for new ways to manage these risks and the portfolio of the security department has widened to include shared responsibility for things such as reputation, corporate governance and regulation, corporate social responsibility and information assurance.”

Link: http://www.securitymanagement.com/library/security_offensive1106.pdf

8. “Managing Risk to Increase Stakeholder Value”, Robert Bruce, The Chartered Institute of Management Accountants, November 2002

InterCEP Highlight: Business interruption involves the greatest uncertainty and the greatest possibility of catastrophic loss to the corporation of all other business risks.

InterCEP Highlight: Factors determining reputation and risk can change overtime. For example, the public tolerance for a rail crash is much lower today even though the frequency of crashes has not increased.



InterCEP Highlight: “Ultimately, demonstrably strong corporate governance is essential to preserving reputation, investor confidence, access to capital, employee satisfaction, customer loyalty, and long-term sustainability.”

Key Points:

- Several case studies from leading companies (such as Lehman Brothers and Microsoft) are provided to reinforce the importance of risk management.
- “Ultimately, demonstrably strong corporate governance is essential to preserving reputation, investor confidence, access to capital, employee satisfaction, customer loyalty, and long-term sustainability. Poor or inadequate governance, by contrast, will not maximise shareholder value, but it will attract the attention of those who see reforming governance as a means of increasing value.”
- Case study example (Kevin Hayes, International CFO, Lehman Brothers): “The issue of managing business interruption is one of the hardest to deal with because it offers greater uncertainty and the possibility of greater catastrophic loss than any other business risk... ‘Our experience is illustrative’, he said. ‘You can only imagine the disruption caused by having the majority of our US-based producers displaced from our 11 headquarters. However, we recovered very quickly – even on September 11 we were able to provide funding to others in the industry to ensure that the markets continued to operate. It was because of the measures we had in place, and others we improvised, that we were able to maintain connectivity to clients and were fully operational when the markets reopened.’”
- Case study example (Railtrack’s management of a rail crash): “It is also a question of always keeping abreast of changing attitudes. ‘The reactions of your different stakeholders change’, he said. ‘Public tolerance of a rail crash, quite rightly, is now much lower than it was twenty or thirty years ago. The frequency of crashes has not increased. It is the tolerance that has reduced’. Risk managers have to assess not just the reputation risk but how it changes over time.”

Link: http://www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC544-1BE04C5B/live/mgrisk_techguide_2002.pdf



9. “Protecting Value Study. Managing Business Risks 2003”, Factory Mutual Insurance Company and Financial Executives Research Foundation, Inc., Security Management Online

InterCEP Highlight: Risk management is an instrument that protects the ability of a firm to generate a positive return to its shareholders.

Key Points:

- “Building on the findings of the 2002 Protecting Value Study, the 2003 study asked nearly 400 CFOs, treasurers and risk managers at the world’s largest corporations about business interruptions...”
- “Risk management is an investment because it is instrumental in protecting the future value of the company and mitigating exogenous events that could impact the ability of the company to generate a positive return to its shareholders.”
- “Overall, property hazards (e.g., fire/explosion, natural disasters, mechanical/electrical breakdown, terrorism/sabotage/theft, service disruption, supply shortage/strike and cybercrime) continue to collectively pose the greatest threat to earnings drivers, according to 59 percent of this year’s respondents.”
- “This year, two-thirds of respondents said that a major disruption to their top earnings driver either would cause a sustained hit to their firm’s earnings or actually threaten their business continuity.”
- “...85 percent of respondents indicated they view risk management as an investment. In particular, those who view risk management as an investment do so because they believe it protects their business continuity; as a result, they believe there is a realized return on investment. Conversely, those who view it as an expense do so because they see it as a necessary cost of doing business with no realized return.”

Link: http://www.securitymanagement.com/library/ProtectingValue_tech0703.pdf

10. “A Terrorist Attack Could Cost You More Than You Think”, Catherine A. Asaro, Beecher Carlson Holdings, Inc., 2005

InterCEP Highlight: Lack of effective planning may result in severe legal liability for the corporation, its directors and officers as well as threatening the continuation of the firm itself.



Key Points:

- “Corporations may find themselves facing liability in the event of a terrorist attack. The recent attacks in London serve as further notice that corporate preparedness remains a serious issue warranting immediate attention.”
- “Protecting employees, revenue, and assets are all components of a well thought out plan aimed at minimizing loss and liability. A corporation’s failure to identify its exposures and evaluate the impact of potential losses could be disruptive to the continuity of its business leaving its directors and officers open to severe legal and public criticism.”

Link: <http://www.beechercarlson.com/newBeecher/WhitePapers/TerroristAttack.pdf>

11. “Boardroom Briefing Business Continuity and Disaster Recovery”, Paper consists of several articles written by various authors, Directors & Boards Magazine, Spring 2006

InterCEP Highlight: The CEO is responsible for informing the Board of Directors about company risks. Business continuity planning addresses corporate governance responsibilities to customers and shareholders. Over a third of CFO’s see disaster preparedness and recovery as their largest vulnerability.

Key Points:

- The thirty six page publication by the Directors & Boards Magazine touches on several topics at the core of business continuity and disaster recovery. Attempts are made through several articles to present business case arguments for having a Business Continuity Plan.
- “With terrorist threats increasingly frequent and well-publicized, directors and officers will have a hard time claiming that corporate risk management did not need to include emergency preparedness.”
- “Implementing a business continuity plan also may have legal significance for a corporation. Because business continuity recognizes risk and mitigates it, the creation and implementation of such a plan may help a corporation discharge its corporate governance responsibilities to customers and shareholders alike.”
- “...business continuity is a strategic investment, and its dividends will be evident during an attack, and economically and legally, in the aftermath of a terrorist event. For example, when a cascading grid failure left tens of millions of people in the U.S. and Canada without electrical power in August 2003, corporations without business continuity plans suffered. Without electricity to run computers, commerce simply stopped. Not so for the New York brokerage firms that had



aggressively invested in business continuity after September 11. That preparedness, including installation of emergency generators and back-up trading systems, allowed commercial transactions to continue with minimal interruption. Considering the financial losses brokerage firms sustain from even an hour of missed trading, investments in business continuity paid for themselves many times over in that one event. Indeed, the 2003 blackout and the business continuity success stories within the financial services sector accelerated the NYSE's and the NASD's adoption of business continuity rules for the industry as a whole."

- "In a recent survey, 37 percent of chief financial officers perceived their firms to be most vulnerable in the area of disaster preparedness and recovery. The survey reflects the anxiety of many executives concerning the state of their company's business continuity plans. Why the concern? Because experts estimate that 50 percent of companies without business continuity plans go out of business within two years following a disaster."
- "72.9% of the respondents of a survey conducted by Directors & Boards in 2006 answered that they consider the CEO responsible for informing the board of risk issues at the company. Multiple responses were allowed."

Link: <http://www.directorsandboards.com/BoardroomBriefing6.pdf>

12. "Taking Risk on Board," Lloyd's of London, Lloyd's of London, 2005

InterCEP Highlight: A Moody's survey found that one in five companies had suffered significant damage from a failure to manage risk over the past year and over half had at least one near miss.

InterCEP Highlight: Boards are becoming aware of the connection between good risk management, better financial performance and stronger corporate reputation.

Key Points:

- The paper cites a survey carried out by the Economist Intelligence Unit in 2005. Examples of companies such as Rolls Royce and Novo Nordisk are given as role models in risk management.
- "Corporate scandals and the resulting tightening of regulation have caused roughly two thirds of the companies surveyed to reassess their risk management strategies...just 14% of board members are confident that their organisations' boards understand, and will respond correctly to, risks facing their foreign operations."

- “Overall, however, there is little doubt that the question of risk is climbing up the corporate agenda. According to Ken Bertsch, an analyst with Moody’s Investors Services, a rating agency: “Directors keenly feel the risks now just of being on boards,” thanks in part to Sarbanes-Oxley. Yet the fact that boards are more aware of risks than they were, say, three years ago does not mean that they agree on how best to identify and, where necessary, mitigate them. We found that during the past 12 months one in five of the companies surveyed had suffered significant damage from a failure to manage risk and over half (56%) had experienced at least one near miss. As many as 10% of respondents reported three near misses during the past year alone. And these are only the ones that companies will admit to.”
- “Under Sarbanes-Oxley, the directors of companies whose shares are listed in the US are not only required to set up independent audit committees to ensure that shareholders’ rights are protected; senior executives also have to certify their companies’ accounts. The penalties for lax or negligent governance, particularly if it leads to shareholders being defrauded, are severe. As Bertsch of Moody’s notes: “The reputations of directors are on the line, not just that of their companies.”
- “The fact that boards are only slowly becoming conscious of the connection between good risk management, better financial performance and stronger corporate reputation suggests that they need to focus more closely on the wider benefits of fully integrating risk management into corporate decision-making, and on the tools available to facilitate this process. Until they begin to do so, risk management is likely to continue to be seen by senior management as a constraint on their business rather than as a source of competitiveness.”

Link: <http://www.lloyds.com/NR/rdonlyres/48FC5495-1313-4616-AD83-AA2C1BA5C952/0/Takingriskonboard.pdf>

13. “Prospering in the Secure Economy”, William D. Eggers, Deloitte Touche Tohmatsu, 2005

InterCEP Highlight: To prosper, organizations must invest in compliance, processes and tools for security. They must also create value from relationships, processes and even products that enable security.

Key Points:

- “There’s no denying it, the terrorist attacks of September 11 changed the global economy. The result, 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 organisations 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.”

Link:

<http://www.deloitte.com/dtt/article/0,1002,sid%253D5628%2526cid%253D80288,00.html>

14. “Justifying the Contingency Plan”, John Watkins, Disaster Recovery Journal, 1997

InterCEP Highlight: The business impact of crises can run into the billions. The 1990 Wall Street Blackout and the 1992 Chicago flood are two examples.

Key Points:

- The article argues that initiating a Business Impact Analysis can have positive implications for the bottom line, especially in the event of a disaster.
- “...for any CEO or CFO who thinks contingency planning is a waste of money, two incidents clearly point out the necessity of a well thought out recovery plan: the August 13, 1990 Wall Street blackout and the April 13, 1992 downtown Chicago flood. In the Wall Street outage 28 firms relocated to hot sites, and in the Chicago flood that number was still higher: 33 firms. The Chicago Board of Trade, one of the world’s largest financial exchanges, closed down completely on the first day of the flood and affected all world financial markets because of the volume of uncleared trades. The most important fact for any executive to remember about both the New York and Chicago disasters is that the cost in dollars most frequently heard is “billions”. However, it will probably prove impossible to refine that estimate because corporations are reluctant to discuss their losses.”

Link: http://www.drj.com/new2dr/w2_011.htm

15. “Protecting Value in the Face of Mass Fatality Events”, Rory F Knight, Deborah J Pretty, Oxford Metrica, 9/29/2005

InterCEP Highlight: How a company responds to corporate catastrophes impacts a firm’s share price. This impact is doubled in the case of mass fatality events.

Key Points:

- “The aim of this briefing is to measure the shareholder value impact of mass fatality events and to identify the key determinants of value protection and



recovery. Mass fatality events are defined generally as those which produce more fatalities than can be handled using local resources. In this study, we include also those events which had the potential to result in mass fatality but, thankfully, did not. Events emanating from four prominent perils over the last five years are evaluated:

- Aviation disasters
- Fires and explosions
- Terrorist attacks
- Natural catastrophes

The tragic nature of mass fatality events brings a number of managerial behaviors into painfully sharp focus and there is much to learn from the different ways in which firms respond. A firm's share price reflects the consensus view of investors as to how management has performed under such pressure. For the research presented herein, these share price reactions are analysed extensively to reveal some core policy implications for senior management. The key conclusions are listed below."

- "Mass fatality events have double the impact on shareholder value than corporate catastrophes in general."
- "As with non-fatal reputation crises for firms, the key determinant of value recovery relates to the ability of senior management to demonstrate strong leadership and to communicate at all times with honesty and transparency."
- "For mass fatality events particularly, the sensitivity and compassion with which the Chief Executive responds to victims' families, and the logistical care and efficiency with which response teams carry out their work, become paramount. There is a 40% value premium associated with the engagement of such specialist services."

Link: <http://www.oxfordmetrica.com/pdf/OMMassFatalitiesBriefing.pdf>

16. "Mobilizing Corporate Resources to Disasters: Toward a Program for Action", William Raisch, Matt Statler & Peter Burgi, International Center for Enterprise Preparedness, New York University, 24 January 2007

InterCEP Highlight: When firms support government and NGO disaster efforts, they serve their own interests as well as the interests of the community by promoting economic resilience.



Key Points:

- **“The Rewards of Corporate Resiliency:** There are clear financial and strategic rewards for enterprises that develop resiliency programs. They include:
 - Increased productivity and innovation, often supported by more effective internal communications, streamlined processes, more adaptive workplaces, better workflows and increased employee morale.
 - Protected revenue flows as a result of plans to protect key assets – Inventory, property/plant, equipment and intellectual property – as well as sustain core operations.
 - Expanded customer base and increased customer retention, as both individual consumers and organizations place an increasing focus on safety, security and preparedness.
 - Lower operating expenses as a result of lower insurance and legal costs, less theft, reduced employee turnover and more competition among suppliers.
 - Reduced cost of capital as both equity and debt markets (including key rating agencies) increasingly evaluate corporate preparedness and resiliency.
 - Stronger reputation, as a result of both the application and communication of resilience.
 - Better regulatory compliance and governance both internally and in terms of external review.”
- “...when a well-prepared business effectively responds to a local disaster, it may minimize employee injury and substantially lessen economic damage to business property as well as community infrastructure. This in turn lessens the response requirements of governments and NGOs. It helps protect jobs, tax revenues, supplier income streams, investor returns and the well-being of its customers. The business aids in overall recovery by not becoming a victim itself. Corporate self-interest ultimately serves the interests of the broader community.”

Link:

<http://www.nyu.edu/intercep/events/Mobilizing%20Corporate%20Resources%201.25.2007.pdf>

17. “Insurance Incentives for Corporate Preparedness”, William G. Raisch – Director & Matt Statler Ph.D. – Associate Director, International Center for Enterprise Preparedness, New York University, 10/17/2006

InterCEP Highlight: When made known to insurance companies, a corporate preparedness program can result in relatively lower insurance premiums and better policy terms.



Key Points:

- “Having an effective corporate emergency preparedness programs can result in relatively lower insurance costs and better policy terms for companies. This can be an important financial consideration in evaluating investment in corporate preparedness and may not be widely known.”
- “Avoidance or mitigation generally results in lower financial losses to both to the insurance policy holder and the insurance company which insures it.”
- “...if a corporation undertakes emergency preparedness activities, it will most likely receive relatively better policy terms (including better premium pricing and deductible levels) than it would if it did not prepare. And in some high risk situations, the presence of an effective corporate preparedness program determines whether or not the company will be offered insurance at all.”
- “...insurance companies generally do not provide comprehensive guidance as to what from their perspective constitutes the basic elements an appropriate preparedness program and thus what they will assess. Nonetheless, it was confirmed with leading insurance companies that all key elements of the consensus-based preparedness standard, ANSI-NFPA 1600 (also known as the National Preparedness Standard) are generally reflected in the underwriting processes of the leading insurance companies. These elements may however be dispersed throughout the underwriting process.”
- “There is a dual benefit to corporate preparedness in this regard. In general, both insurance companies and insured businesses experience losses in the aftermath of any disaster or major emergency. Business policy holders are responsible for the cost of any losses up to their deductible as well as beyond the limits of the coverage, while insurance companies are responsible for any losses between the deductible and the limits of the policy. Businesses are also responsible for the wider losses that extend well beyond that which can be insured or easily quantified (e.g., loss of market share, reputational loss, etc.). Therefore, both policy holders and insurance companies benefit when preparedness measures are undertaken and these measures ultimately limit the size of the loss due to an emergency.”

Link:

<http://www.nyu.edu/intercep/Insurance%20Incentives%20for%20Corporate%20Preparedness%2017%20Oct%2006.pdf>



18. “The Legal Obligation for Corporate Preparedness”, Bill Raisch, M.B.A. – Director & Matt Statler, Ph.D. – Associate Director New York University International Center for Enterprise Preparedness, Denis Binder, S.J.D., Professor of Law, Chapman University, New York University International Center for Enterprise Preparedness, October 16, 2006

InterCEP Highlight: Corporations risk substantial legal liability if they do not put in place appropriate emergency preparedness programs.

Key Points:

- “Corporations are vulnerable to significant legal liability if they do not undertake emergency preparedness efforts. This liability can result from several sources including common law negligence, specific legislation/regulations and contractual obligations.”
- “The corporation faces a diversity of risks in its day-to-day operations: Whether the source is natural or human, the number of ways an accident can occur, a facility fail, or system malfunction is probably infinite.”
- “Litigation Can Drain Financial and Executive Resources: Unlike generations past, America had become a much more litigious society. The aftermath of any major disaster, such as Hurricane Katrina, 9/11, or the Loma Prieta and Northridge earthquakes in California, will include extensive litigation, both over issues of liability and insurance coverage. The costs of litigation and diversion of executive resources away from management can be enormous.”

Link:

<http://www.nyu.edu/intercep/Legal%20Case%20for%20Preparedness%2016%20oct%2006.pdf>

19. “Crediting Preparedness”, William G. Raisch – Director & Matt Statler, Ph.D. – Associate Director, International Center for Enterprise Preparedness, New York University, 8/2/2006

InterCEP Highlight: A firm’s level of preparedness can clearly impact its ability to repay debt and deliver value to shareholders. Rating agencies are beginning to recognize this.

Key Points:

- “Businesses operate in an increasingly uncertain global environment with growing operational risks from a diversity of sources ranging from technology failures and supply chain interruptions to natural disasters and pandemics. A



- business' capacity to manage these risks has become an increasingly important component of its financial condition. In the interest of enabling more informed financial decisions by both investors and creditors, rating agencies should include an assessment of corporate preparedness in the rating process.”
- “Effective management response and corporate preparedness programs can significantly mitigate the impact of operational risk events and affect corporate recovery.”
 - “There are significant developments in securities regulation, among insurance industry rating agencies, and among private sector companies that demonstrate the relevance of preparedness to a firm's capacity to repay debt and deliver value to stakeholders.”
 - “Specific and higher profile inclusion of corporate preparedness in rating agency underwriting processes would yield multiple benefits.
 - First, by acknowledging the importance of preparedness for operational risks, it would provide creditors and investors with more comprehensive and accurate assessment of creditworthiness;
 - Second, it would allow investors and creditors to identify those industry-leading firms that have already learned lessons from 9/11, Katrina and other catastrophic events, and proactively undertaken key preparedness measures;
 - And finally, by introducing a competitive dimension to preparedness through specific acknowledgement in the underwriting process, it would provide an incentive for firms to develop more robust preparedness programs and consequently improve the overall resilience of the global marketplace.”
 - “A compelling illustration of the impact of organizational preparedness can be found in recent research by FM Global, the major property and casualty insurance firm. The firm acknowledges that business interruption insurance is the last line of defense against business interruption, and that the first and most important step is a holistic risk management program that includes all aspects of the organization. FM Global provides site-specific, scientifically-based loss prevention recommendations as part of its coverage. In the aftermath of last year's hurricanes, FM Global compared the loss history of those of its policyholders which implemented its loss prevention recommendations versus those that still had recommendations to complete. They found that those policyholders that fully implemented the preparedness recommendations had on average 75% to 85% lower dollar losses than those policyholders which did not implement such measures. As to the cost of physical improvements and preparedness, the research indicated a remarkable return on investment. In the case of Hurricane Katrina, across 476 locations with a total of \$42 billion in insured property exposed to the hurricane's impact, FM Global clients collectively spent \$2.3 million to prevent a projected \$480 million in loss, with cost of those improvements averaging only \$7,400 per facility. That equals a 208 to 1 payback – or in other words,



for every \$1 spent on targeted preparedness measures, \$208 in resources were saved in one single event.” Link to InterCEP’s Case Study:

<http://www.nyu.edu/intercep/events/20061009-256.html>

- “InterCEP has additionally gathered anecdotal data suggesting that within this competitive environment, some industry-leading firms are already embracing 'all-hazards preparedness' as a point of strategic differentiation and advantage. Preparedness programs in some cases are seen as adding agility to respond to changes in the business environment. Additionally, other firms have found that their customers value the perception of safety and security that results from effective corporate preparedness, especially in the commercial office space and retail environments.”

Link:

<http://www.nyu.edu/intercep/research/pubs/Crediting%20Preparedness%208.2.06.pdf>

20. “Can Your Business Survive A Natural Disaster?”, Alfa Insurance, Alfa Insurance, 2007

InterCEP Highlight: History shows that business continuity planning can be critical for business survival in the aftermath of a disaster

Key Points:

- “Of all businesses that close down following a disaster, more than 30 percent never reopen again.”

Link: <http://www.alfains.com/business/BusinessDisasterarticle.htm>

21. “Computing the Cost of Downtime — Building a Business Case for Disaster Recovery”, nFrame, nFrame

InterCEP Highlight: “40 percent of companies that suffer a major business disruption go out of business within two years because they are unable to recover from the long-term affects.”

Key Points:

- “According to KPMG, a global network of professional services firms that provides audit, tax and business advisory services, 40 percent of companies that suffer a major business disruption go out of business within two years because they are unable to recover from the long-term affects. Given the potentially fatal impact of a business systems interruption, it’s absolutely



critical for companies to carefully define and implement plans that mitigate risk.”

Link: <http://www.nframe.com/PDF/ComputingtheCostsofDowntime.pdf>

BUSINESS FUNCTIONS

INFORMATION TECHNOLOGY

22. “Data Protection and Disaster Recovery”, Walt Hinton, Managed Storage International, 2000

InterCEP Highlight: The loss of important business data can result in significant losses in terms of both existing and future business as well as liabilities to customers, investors and legal authorities. IT downtime costs can range from \$1 million to over \$6 million annually.

Key Points:

- The white paper argues that loss of critical data due to any crises can be a costly affair for companies.
- “The costs associated with losing important data can include the potential loss of existing and new business, the potential loss of customer confidence, and potential liabilities to customers and investors. Failure to produce certain data in response to an audit or subpoena may also carry legal consequences.”
- Sample of Hourly Costs of Downtime by industry:
 - Brokerage Operations \$6,450,000
 - Energy \$2,817,846
 - Financial Institutions \$1,495,134
 - Information Technology \$1,344,461
 - Insurance \$1,202,444
 - Pharmaceuticals \$1,082,252

(Hourly costs of downtime experienced by each industry given on pg. 6 of the report)

- “...but remember that vulnerability to data unavailability and loss isn’t just limited to immediate monetary impact: it also includes such things as loss of customer confidence, liability, and lost current and future business.”

Link: <http://www.msiservice.com/uploads/1084916515.pdf>



23. “Testimony delivered by Louis Rosenthal, Executive Vice President, LaSalle Bank Corporation on June 1, 2004 to the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, United States Congress” (also found under Banking), Statement of Louis F. Rosenthal Executive Vice President Lasalle Bank Corporation, BITS Financial Services Roundtable, June 2, 2004

InterCEP Highlight: There are increasing attacks on the IT systems of financial institutions with many resulting in financial loss.

Key Points:

- “Information security is a complex challenge. Among industry sectors, the financial sector is particularly aware of the challenge, in part because customer trust is so vital to the stability of financial services and the strength of the nation’s economy. At the same time, we are a favorite target of criminals operating in cyberspace and of terrorists, as was made clear on 9/11. The Deloitte Global Security Survey 2004 finds that the majority of global financial institutions have seen an attack on their IT systems within the last year, and that many of those breaches resulted in financial loss. Eighty-three percent of respondents reported their systems had been compromised in 2003, versus 39 percent in 2002.”

Link: <http://www.bitsinfo.org/downloads/Testimony/rosenthaltestimony.pdf>

24. “Business Continuity: New risks, new imperatives and a new approach”, IBM Global Services, IBM, 1999

InterCEP Highlight: The financial impact of a major IT system outage can be enormous. Impacts include immediate loss of revenue, reduction in customer base as well as intangible damages such as lower morale and productivity, increased employee stress, delays in key project timelines, diverted resources, regulatory scrutiny and a tainted public image for both the corporations and responsible executives.

Key Points:

- “Many senior executives and business managers consider business continuity the responsibility of the IT department. However, it is no longer sufficient or practical to vest the responsibility exclusively in one group. Web-based and distributed computing have made business processes too complex and decentralized. What’s more, a company’s reputation, customer base and, of course, revenue and profits



are at stake. All executives, managers and employees must therefore participate in the development, implementation and ongoing support of continuity assessment and planning.”

- “According to a report published by Strategic Research Corporation, a Santa Barbara, California, market research and consulting firm, the financial impact of a major system outage can be enormous: US\$6.5 million per hour in the case of a brokerage operation; US\$2.6 million per hour for a credit-card sales authorization system; or a mere US\$14,500 per hour in automated teller machine (ATM) fees if an ATM system is offline.”
- “In this climate, executives responsible for company performance now find their personal reputations at risk. Routinely, companies that suffer online business disruptions for any reason make headlines the next day, with individuals singled out by the press. Moreover, corporate directors and officers can be liable for the consequences of business interruption or loss of business-critical information.”
- “For example, the New York-based research firm FIND/SVP calculates the average financial loss per hour of disk array downtime at US\$29,301 in the securities industry, US\$26,761 for manufacturing, US\$17,093 for banking and US\$9,435 for transportation. More difficult to calculate are the intangible damages a company can suffer: lower morale and productivity, increased employee stress, delays in key project timelines, diverted resources, regulatory scrutiny and a tainted public image.”

Link: <http://www.moregroupinc.com/IBM%20BC%20White%20Paper.pdf>

25. “Medium businesses lose \$867,000 a year to network downtime”, Infonetics Research, Inc, Infonetics Research, Inc., 2006

InterCEP Highlight: Medium-sized businesses lose nearly \$1 million annually in network downtime.

Key Points:

- “In a new study on network downtime, Infonetics Research found that medium businesses (101 to 1,000 employees) are losing an average of 1% of their annual revenue, or \$867,000, to downtime.”
- “The study, *The Costs of Downtime: North American Medium Businesses 2006* says that companies experience an average of nearly 140 hours of downtime every year, with 56% of that caused by pure outages. Many medium businesses have a hard time closely tracking downtime caused by service degradation because they don’t have the proper network management tools to observe and quantify service degradations.”



- “There isn’t a single problem area that organizations need to focus on, which would be a simpler fix,” said Jeff Wilson, principal analyst at Infonetics Research. “Every decision is critical, from hardware selection, to product setup and from employee training to SLAs with service providers. Human error is the most troubling, because fixes for human error are elusive and require process changes and retraining, which can take a long time and be very expensive.”
- “Infonetics conducted the study to understand the causes and calculate the cost of outages and service degradations in terms of lost revenue and productivity. They studied seven sources of downtime: network products, security products, cables/connectors, servers, applications, service providers, and e-commerce; and the four common causes: hardware problems, software problems, human error, and service provider error.”

Link: <http://www.infonetics.com/resources/purple.shtml?upna06.dwn.nr.shtml>

26. “Business Continuity Planning: Your Insurance Policy Against Disaster Disruption,” Cablevision Systems Corporation, Cablevision Systems Corporation, 2006

InterCEP Highlight: 43 percent of companies impacted by a severe crisis never reopen. 29 percent of those that do reopen fail within two years.

Key Points:

- “How prepared is your business to operate through a disaster? That is the essence of Business Continuity (BC). It’s more than simply how to get back in business after a disaster. BC covers the processes and procedures your organization has in place so that it can operate continuously through any kind of disruption.”
- “What you’re insuring against is nothing less than the possible survival of your business. The American Red Cross estimates that as many as 40 percent of small businesses that experience a disaster never reopen. According to a study by Datapro Research Company, 43 percent of companies hit by severe crises never open their doors again. Worse yet, the crises have a rippling effect, which causes another 29 percent to fail within two years. While small and mid-sized businesses often have the most to lose in a disaster, they are often the least prepared.”

Link: <http://www.optimumlightpath.com/mediaassets/businesscontinuitywhitepaper.pdf>



27. “Downtime costs European businesses £300k per hour on average”, Global Switch, Global Switch, 09 May 2007

InterCEP Highlight: European businesses lose an average of £300,000 per hour to IT downtime.

Key Points:

- “Global Switch has released findings from a pan-European survey, revealing that IT downtime costs European businesses on average £300,000 per hour.”
- “50 percent of business service providers claim that one hour of downtime could incur costs of between £501,000 and £1 million. Financial institutions follow close behind, with 23% predicting costs of between £51,000 and £100,000 and a further 18% estimating costs in the region of £101,000 to £500,000.”

Link: <http://www.globalswitch.com/news/newsarticle/itemId/i65768095>

28. “Business Continuity Business Brief”, Hitachi, Hitachi Data Systems Corporation, 2004

InterCEP Highlight: “Your data really is your business.” IT downtime can result in lost revenue, adverse headlines, lower employee productivity and decline in company valuation. Lost revenue estimates run from \$1 million to over \$ 6 million per hour.

Key Points:

- “Meta Group estimates lost revenue from downtime at an average of US\$1 million/hour. Contingency Planning Research says losses go as high as US\$6.45 million/hour for retail brokerages. Beyond the loss of revenue, there are adverse headlines and the potential impact on company valuation to consider, not to mention lower employee productivity caused by sporadic outages. It adds up to this: Your data really is your business.”

Link: http://www.hds.com/pdf/business_continuity_brief_463_01.pdf



SUPPLY CHAIN MANAGEMENT

29. “The Effect of Supply Chain Disruptions on Long-term Shareholder Value, Profitability, and Share Price Volatility”, Kevin Hendricks and Vinod Singhal, The Logistics Institute, June 2005

InterCEP Highlight: Supply chain disruptions have substantial impacts on firms including 33 to 40% lower stock returns relative to their benchmarks, 13.5% increase in share price volatility, 107% drop in operating income, 7% lower sales growth, and 11% increase in costs.

Key Points:

- “The evidence presented in this report makes a compelling case that ignoring the risk of supply chain disruptions can have serious negative economic consequences. Based on a sample of more than 800 supply chain disruption announcements, the evidence indicates that firms that suffer supply chain disruptions experience 33 to 40% lower stock returns relative to their benchmarks, 13.5% increase in share price volatility, 107% drop in operating income, 7% lower sales growth, and 11% increase in costs. By any yardstick these are very significant economic losses. More importantly, firms do not quickly recover from these losses.”
- The average effect of disruptions in the year leading to the disruption is:
 - 107 percent drop in operating income
 - 114 percent drop in return on sales
 - 93 percent drop in return on assets
 - 14 percent growth in inventoriesThese negative performance metrics often continue for two years after the disruption announcement.
- “The evidence presented in this report is based on an analysis of more than 800 supply chain disruptions that were publicly announced during 1989-2000. These announcements appeared in the Wall Street Journal and/or the Dow Jones News Service, and were about publicly traded companies that experienced production or shipping delays.”

Link: http://www.loginstitute.ca/pdf/singhal_scm_report.pdf



30. “An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm”, Hendricks, Kevin B, Singhal, Vinod R, Production and Operations Management, November 2004

InterCEP Highlight: Firms that experienced bad supply chain disruptions experienced stock returns approaching -40%

Key Points:

- “This paper investigates the long-term stock price effects and equity risk effects of supply chain disruptions based on a sample of 827 disruption announcements made during 1989-2000. Stock price effects are examined starting one year before through two years after the disruption announcement date. Over this time period the average abnormal stock returns of firms that experienced disruptions is nearly -40%. Much of this underperformance is observed in the year before the announcement, the day of the announcement, and the year after the announcement. Furthermore, the evidence indicates that firms do not quickly recover from the negative effects of disruptions. The equity risk of the firm also increases significantly around the announcement date. The equity risk in the year after the announcement is 13.50% higher when compared to the equity risk in the year before the announcement.”

Link: http://findarticles.com/p/articles/mi_qa3796/is_200504/ai_n13637019

31. “Association between Supply Chain Glitches and Operating Performance”, Kevin B. Hendricks and Vinod R. Singhal, Management Science (Journal), May 2005

InterCEP Highlight: Supply chain glitches lower sales growth (-6.92%), increase growth in costs (+10.66%), and result in a high growth in inventories (+13.88%). Furthermore, these negative effects linger.

Key Points:

- “This paper empirically documents the association between supply chain glitches and operating performance. The results are based on a sample of 885 glitches announced by publicly traded firms. Changes in various operating performance metrics for the sample firms are compared against a sample of control firms of similar size and from similar industries. In the year leading up to the announcement, the control-adjusted mean percent changes in operating income, return on sales, and return on assets for the sample firms are -107%, -114%, and

–92%, respectively. During this same period, the control-adjusted changes in the level of return on sales and return on assets are –13.78% and –2.32%, respectively. Relative to controls, firms that experience glitches report on average 6.92% lower sales growth, 10.66% higher growth in cost, and 13.88% higher growth in inventories. More importantly, firms do not quickly recover from the negative economic consequences of glitches. During the two-year time period after the glitch announcement, operating income, sales, total costs, and inventories do not improve.

- “...it does not matter who caused the glitch, what the reason was for the glitch, or what industry a firm belongs to—glitches are associated with negative operating performance across the board.”

Link: <http://mansci.journal.informs.org/cgi/reprint/51/5/695>

32. “Quantifying the Impact of Supply Chain Glitches on Shareholder Value”, Vinod R. Singhal, SAP (www.sap.com), 2003

InterCEP Highlight: Supply chain disruptions can “torpedo shareholder value” resulting in losses up to 25%. Adaptive supply chains can reduce the problem and conserve shareholder value.

Key Points:

- “Most managers intuitively believe that there is a strong link between a company’s supply chain performance and its shareholder value. Now this intuition can be backed with hard facts. Results from a research study show that supply chain glitches torpedo shareholder value. After adjusting for industry and market movements, the total shareholder value loss associated with a glitch can be as high as 25 percent. Irrespective of who is responsible for the glitch or what caused the glitch, shareholders of companies that experience glitches pay dearly. Glitches are bad news, regardless of the company’s size, industry, and growth prospects. Building adaptive supply chains with the capability to respond to glitches can help reduce the problem and conserve shareholder value.”
- “The evidence presented here is based on estimating the loss in shareholder value from 838 supply chain glitches that were made known publicly by the news media from 1989 through 2001. These news stories appeared in the *Wall Street Journal* or the *Dow Jones News Service* and were about publicly traded companies that experienced production delays or shipping delays.”
- “...the average destruction in shareholder value ranges from \$129 million to \$145 million per major glitch. The total loss in shareholder value for companies experiencing the 838 glitches is estimated to be between \$107 billion and \$120



billion – counting only the loss on the day the glitches were made public in the news. By any standards, this represents a significant loss of shareholder wealth.”

Link:

http://www.sap.com/solutions/business-suite/scm/pdf/BWP_Quantify.pdf

**33. “Innovators in Supply Chain Security: Better Security Drives Business Value”,
Barchi Peleg-Gillai, Gauri Bhat and Lesley Sept, Stanford University, July 2006**

InterCEP Highlight: Disruptions in supply chains can occur for a diversity of reasons including natural disasters, product contamination and adulteration, shortages, border closings, strikes by ports and terrorism.

InterCEP Highlight: Investments in supply chain security can provide significant business value including, improvements in product safety, inventory management, supply chain visibility, product handling, customs clearance, speed, resilience, customer satisfaction and other process improvements.

Key Points:

- “Following terrorist attacks in recent years, firms have been taking multiple steps—either voluntarily or to meet mandated government regulations—to ensure safe transit of their goods across international borders. In parallel, natural disasters such as Hurricane Katrina, as well as many other unforeseen events such as product contamination and adulteration, shortages, border closings and strikes by ports, made firms more aware of the vulnerability of their supply chains, and encouraged them to seek ways to reduce risks of such unforeseeable situations and increase stability along their supply chain.”
- “The study was based on inputs from 11 manufacturers and 3 Logistics Service Providers (LSPs) that are considered “innovators” in supply chain security, and clearly demonstrated that investments in supply chain security can provide business value.”
- “Some of the more significant benefits participating manufacturers reported included the following:
 - 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 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).”

Link:

http://www.nam.org/s_nam/bin.asp?CID=202515&DID=237208&DOC=FILE.PDF

34. “Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management”, Hau L. Lee and Seungjin Whang, Graduate School of Business, Stanford University, Stanford, July 6, 2003

InterCEP Highlight: Higher supply chain security can be achieved at lower cost by proper management and operational design.

Key Points:

- “Governments and industry have all responded with proposals to create more confidence in supply chain security, while maintaining smooth flows of goods and services in a global supply chain. One of the most effective strategies may be to apply the lessons of successful quality improvement programs. In this paper, we describe how the principles of total quality management can actually be used to design and operate processes to assure supply chain security. The central theme of the quality movement – that higher quality can be attained at lower cost by proper management and operational design – is also applicable in supply chain security. By using the right management approach, new technology, and re-engineered operational processes, we can also achieve higher supply chain security at lower cost. We will demonstrate how this can be done with a quantitative model of a specific case example.”

Link: <http://bctim.wustl.edu/calendar/mediafiles/SecurityQuality.pdf>



35. “The New Supply Chain Challenge: Risk Management in a Global Economy” (requires site registration), Ruud Bosman, Factory Mutual Insurance Company, 2006

InterCEP Highlight: A survey of more than 600 financial executives identified supply chain risk as having the greatest potential to disrupt the “top revenue driver.”

Key Points:

- “The worrisome news here is not just that some corporations fail to recognize how new business paradigms have changed their risk profile. Rather, it is that even among those that do, too many accept it under the mistaken belief they can’t do anything about it. Still others, fail to plan for the unthinkable—the devastating hurricane, the shocking terrorist attack, or the collapse of an important supplier in the wake of political upheaval or accounting fraud. Conversely, some companies fail to appreciate the dramatic consequences that even a seemingly minor supply chain disruption can trigger.”
- “In fact, a recent FM Global study of more than 600 financial executives around the world found that respondents identified supply chain risk, more than any other, as having the greatest potential to disrupt their top revenue driver.”
- “By implementing a holistic, enterprise-wide supply chain risk management program, companies also can uphold their commitment to providing strong corporate governance on behalf of shareholders, which ultimately boosts shareholder value. Companies that don’t are, in a very real sense, working without a safety net. In today’s high-risk world, that’s never a smart idea.”

Link: <http://www.fmglobal.com/pdfs/ChainSupply.pdf>

36. “Supply Chain Management under the Threat of International Terrorism”, Yossi Sheffi, Massachusetts Institute of Technology, 2001

InterCEP Highlight: Resilience strategies not only work in maintaining business continuity but can yield cost savings through better forecasting, smoother operations, downsized warehousing and lower administrative overhead.



Key Points:

- “On the morning of September 11th, 2001, the United States and the Western world entered into a new era – one in which large scale terrorist acts are to be expected. The impacts of the new era will challenge supply chain managers to adjust relations with suppliers and customers, contend with transportation difficulties and amend inventory management strategies. This paper looks at the twin corporate challenges of (i) preparing to deal with the aftermath of terrorist attacks and (ii) operating under heightened security. The first challenge involves setting certain operational redundancies. The second means less reliable lead times and less certain demand scenarios. In addition, the paper looks at how companies should organize to meet those challenges efficiently and suggests a new public-private partnership. While the paper is focused on the US, it has worldwide implications.”
- “For example Solomon Smith Barney, the financial services firm, had 7,000 workers in the World Trade Center, all of whom, fortunately, got out in time. The company was up and running within 12 hours using a backup New Jersey site and invoking a set of emergency backup processes.”
- Benefits of Shipment visibility: “Shipment data visibility allows manufacturers to avoid plant shut down due to part shortages and allows retailers to avoid turning customers away due to unavailability of goods since such problems can be corrected early... The cost savings associated with better forecasting and smoother operations include not only lower inventory carrying costs, and the avoidance of expedited shipments; it also means that warehousing facilities can be downsized and a significant amount of administrative overhead associated with unscheduled activities can be avoided.”

Link:

<http://web.mit.edu/sheffi/www/selectedMedia/genMedia.supplyChainManagementUnderTheThreatOfInternationalTerrorism.pdf>

37. “Building the Resilient Enterprise”, Yossi Sheffi & James B. Rice Jr., MIT Sloan Management Review, Fall 2005

InterCEP Highlight: Investing in resilience can have many “day to day” benefits for the corporation in addition to more dramatic impacts when disruptions do occur including clear competitive advantages which can boost earnings.

- The article asserts that nearsighted supply chain practices such as just in time inventory management endanger companies’ profits and survivability in the



aftermath of a disaster. Furthermore, investing in resilience may cost time and money but the additional outcome of the analyses can have many “day to day” benefits.

- “In some cases, a company can foresee and prepare for disruption, minimizing its effects. Warnings range from the 30-minute tornado alert General Motors Corp. received in Oklahoma on May 8, 2003 to the several months of deteriorating labor negotiations at West Coast ports that preceded the October 2002 lockout. In other cases, such as 9/11, there is little or no warning.”
- Examples are provided such as: In 1999 Dell increased third quarter earnings by 41% and Apple lost sales due to a semiconductor shortage that affected both companies. The shortage was a result of an earthquake that halted semiconductor production in Taiwan. Dell adjusted to the shortage in a more flexible manner than Apple to an event neither company could have foreseen.

Link: http://web.mit.edu/sheffi/www/selectedMedia/smr_vol47No1.pdf

38. “Building a Resilient Organization”, Yossi Sheffi, MIT, December 2006

InterCEP Highlight: Supply chain disruptions create shortages similar to demand spikes caused by market supply/demand imbalances. Thus, resilient enterprises can often react more quickly (than their competitors) to changing market demand, winning market share and customer loyalty.

Key Points:

- “A company can suffer a serious business interruption not only when one of its own facilities, distribution channels, or work force is disrupted, but also when any one of the elements in its supply chain or, more expansively, its ecosystem, is disrupted. The damage to the Philips plant was about \$40 million, which was mostly covered by insurance. The damage to Ericsson was orders of magnitude larger – the loss of its handset manufacturing business.”
- “...government actions have to be regarded as part of the disruption. For example, if a container will explode in a US port, it is likely that the Government may close all ports causing significant economic damage. If this seems far - fetched, one only has to examine the congressional actions in the 2006 Dubai Ports fiasco, where ignorance and narrow interests succeeded in hurting the security interests of the US in order to “score” politically.
- “...increasing supply chain flexibility can help a company not only withstand significant disruptions but also better respond to demand fluctuations and therefore be a stronger competitor. The notion of flexibility is based on



- interchangeability – developing the ability to interchange elements in the supply network quickly...”
- “The rewards for building a resilient organization are substantial. Not only will the enterprise be “hardened” to withstand disruption of all kinds, but it will be more competitive day - to - day. The reason is that supply disruptions create shortages which are not dissimilar to the demand spikes caused by supply/demand imbalances. Resilient enterprises can thus react to changing market demand ahead of their competitors. Furthermore, resilient enterprises can look at disruptions as opportunities rather than problems. In most cases large - scale disruptions affect a whole industry or an entire region. In such situations the resilient enterprise is likely to bounce back ahead of its competition, winning market share and customer loyalty.”

Link:

http://web.mit.edu/sheffi/www/selectedMedia/wpd_building_a_resilient_organization_rev20061226.pdf

39. “Risky Business: Failing to Assess Supply Chain Continuity”, Chael Porier & Brian Zawada, Disaster Resource Guide, 2007

InterCEP Highlight: The timely receipt of goods and services from sources outside your organization are critical to ongoing revenue generation.

Key Points:

- “Following a disaster or business interruption, the organizations that survive will be those with a defined strategy in place, have accurately anticipated and planned for contingencies, and understand the cost metrics associated with their strategy. Organizations relying on the timely receipt of goods and services to continue revenue generating production view supply chain continuity as a critical business continuity management component.”
- “All in all, the business continuity process that focuses exclusively on internal operations fails to manage many of the risks leading to business interruption.”

Link: http://www.disaster-resource.com/articles/03p_032.shtml



40. “Managing Disruptions to Supply Chains”, Lawrence V. Snyder, Zuo-Jun Max Shen, *The Bridge* (National Academy of Engineering), winter 2006

InterCEP Highlight: Supply chain disruption events can have significant physical costs (e.g. damage to facilities, inventory, electronic networks, infrastructure) and subsequent losses due to downtime, wages for employees who cannot work and loss of customer goodwill. Significant declines in sales growth, stock returns and shareholder wealth can be expected for two or more years following the event.

Key Points:

- “Supply chain disruptions can have significant physical costs (e.g., damage to facilities, inventory, electronic networks, and infrastructure) and subsequent losses due to downtime. A recent study (Kembel, 2000) estimates the cost of downtime (in terms of lost revenue) for several on-line industries that cannot function if their computers are down. For example, the cost of one hour of downtime for Ebay is estimated at \$225,000, for Amazon.com, \$180,000, and for brokerage companies \$6,450,000. Note that these numbers do not include the cost of paying employees who cannot work because of an outage (Patterson, 2002) or the cost of losing customers’ good will. Moreover, a company that experiences a supply chain disruption can expect to face significant declines in sales growth, stock returns, and shareholder wealth for two years or more following the incident (Hendricks and Singhal, 2003, 2005a, 2005b). The huge costs of disruptions show that business continuity is vital to business success, and many companies are actively pursuing strategies to ensure operational continuity and quick recovery from disruptions.”
- “One important area for future research is the development of analytical tools for understanding the interdependence of risks faced by a supply chain. A single event (e.g., an economic downturn or a bird-flu pandemic) might cause multiple types of disruptions (e.g., a shortage of raw materials and absenteeism among the firm’s own workforce), and these risks may be subtly related. In other words, the supply chain’s total risk may not be a simple sum of its parts.”

Link: <http://www.lehigh.edu/~lvs2/Papers/SnyderShenBridge.pdf>



VERTICAL INDUSTRIES

FINANCIAL SERVICES

41. “Using Loss Data to Quantify Operational Risk”, Patrick de Fontnouvelle, Virginia DeJesus-Rueff, John Jordan, Eric Rosengren, Federal Reserve Bank of Boston, April 2003

InterCEP Highlight: For large international banks, the capital charge for operational risk will often exceed the charge for market risk.

Key Points:

- “Management and quantification of operational risk has been impeded by the lack of internal or external data on operational losses. We consider newly available data collected from public information sources, and show how such data can be used to quantify operational risk for large internationally active banks. We find that operational losses are an important source of risk for such banks, and that the capital charge for operational risk will often exceed the charge for market risk. Although operational risk capital will vary depending on the size and scope of a bank’s activities, our results are consistent with the 2-7 billion dollars in capital some large internationally active banks are currently allocating for operational risk.”
- “Financial institutions have experienced more than 100 operational loss events exceeding \$100 million over the past decade. Examples include the \$691 million rogue trading loss at Allfirst Financial, the \$484 million settlement due to misleading sales practices at Household Finance, and the estimated \$140 million losses stemming from the 9/11 attack at the Bank of New York. Recent settlements related to questionable business practices have further heightened interest in the management of operational risk at financial institutions.”

Link: <http://www.bis.org/bcbs/events/wkshop0303/p04deforose.pdf>

42. “Moody’s Analytical Framework for Operational Risk Management of Banks”, Brendon Young, Moody’s Investors Service (Global Credit Research), January 2003

InterCEP Highlight: Moody’s asserts that operational risks will affect credit ratings, share prices and organizational reputation. Therefore, analysts will increasingly include it their assessments of management, their strategy and the expected long-term performance of banks.

Key Points:

- “Moody's believes that the assessment of operational risk is becoming increasingly central to the fundamental analysis of a rated bank. Put simply, operational risk management improves the quality and stability of earnings, thereby enhancing the competitive position of the bank and facilitating its long-term survival.”
- “The control of operational risk is fundamentally concerned with good management, which involves a tenacious process of vigilance and continuous improvement. This is a value-adding activity that impacts, either directly or indirectly, on bottom-line performance. It must, therefore, be a key consideration for any business. Since operational risk will affect credit ratings, share prices, and organisational reputation, analysts will increasingly include it in their assessment of the management, their strategy and the expected long-term performance of the business.”

Link: <http://www.gloriamundi.org/picsresources/maf.pdf>

43. “The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers”, J. David Cummins and Christopher M. Lewis, Wharton School and the Hartford Insurance Group, December 23, 2004

InterCEP Highlight: For banks and insurance companies, operational risk events generally result in a larger market value loss than the actual operational loss. The market may see such losses as signals of poor management quality and operational controls and thus reduced expectations of future cash flows.

Key Points:

- “This paper conducts an event study analysis of the impact of operational risk events on the market values of banks and insurance companies, using the OpVar database. We focus on financial institutions because of the increased market and regulatory scrutiny of operational losses in these industries. The analysis covers all publicly reported banking and insurance operational risk events affecting publicly traded U.S. institutions from 1978-2003 that caused operational losses of at least \$10 million – a total of 403 bank events and 89 insurance company events. The results reveal a strong, statistically significant negative stock price reaction to announcements of operational loss events. On average, the market value response is larger for insurers than for banks. Moreover, the market value loss significantly exceeds the amount of the operational loss reported, implying that such losses



- convey adverse implications about future cash flows. Losses are proportionately larger for institutions with higher Tobin's Q ratios, implying that operational loss events are more costly in market value terms for firms with strong growth prospects.”
- “Additionally, operational loss events may serve as signals of poor management quality and operational controls, leading the market to reduce expectations of future cash flows.”

Link: <http://www.gloriamundi.org/picsresources/jcclrw.pdf>

44. “Competitiveness and Security: Financial Services Sector Study”, BITS and the Santa Fe Group, Council on Competitiveness, 2006

InterCEP Highlight: Increasingly the financial services industry has taken a strategic approach to corporate resilience and security, integrating it into all significant business decisions. The result has been competitive benefits including, increased efficiencies, cost savings, loss avoidance, productivity enhancements, reputation protection, regulatory compliance, and direct revenue opportunities.

InterCEP Highlight: “Institutions with certain levels and kinds of security investments are also likely to have better bond ratings, lower insurance costs, and few or no punitive actions from regulators. As Basel II is implemented, there will also be benefits from lower capital requirements based on technology risk management.”

Key Points:

- “This study provides insight into the financial services industry’s perspective on security and business models. It addresses the questions: What synergies exist between security and competitiveness in the financial services industry, and what are best practices for achieving those benefits? Competitiveness includes strategic benefits from cost savings, productivity enhancements and revenue opportunities.”
- “The study examines the concept that productivity and revenue potential are enhanced by a strategic approach to security. Security has historically been viewed as a cost of doing business, but, increasingly, financial services firms are integrating security choices into all significant business decisions. The industry is realizing that corporate business strategies need to incorporate security on an enterprise-wide basis. Strategies need to be coordinated, top-to-bottom and end-



- to-end, for the greatest competitive benefits, which include increased efficiencies, cost savings, loss avoidance, productivity enhancements, reputation protection, regulatory compliance, and direct revenue opportunities.”
- “Recent events and trends illustrate another dimension to security: cross-sector vulnerabilities and interdependencies. Security issues cannot be dealt with in a vacuum. The resilience, productivity and competitiveness of the Nation’s economy requires increasing attention to interdependencies between sectors, particularly in times of crisis. Telecommunications, energy, information technology and transportation are particularly important to the financial services sector.”
 - “The extent to which the insurance industry takes investments in security into consideration also reflects evolving business attitudes. The insurance industry is beginning to value investments in cyber security. Premiums should ultimately reflect this valuation. The notion is that by reducing risk, a firm likewise reduces costs.”
 - “In December of 2003, BITS surveyed its members on the costs of addressing software vulnerabilities, including managing software patches. We found that: Software vulnerabilities are approaching a cost of \$1 billion annually to the financial services industry.”

Link: <http://www.compete-resilience.org/upload/Financial-Services2.pdf>

45. “Testimony delivered by Louis Rosenthal, Executive Vice President, LaSalle Bank Corporation on June 1, 2004 to the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, United States Congress” (also found under Information Technology), Statement of Louis F. Rosenthal Executive Vice President Lasalle Bank Corporation, BITS Financial Services Roundtable, June 2, 2004

InterCEP Highlight: Among the majority of global financial institutions, cyber attacks are increasing with many resulting in financial loss.

Key Points:

- “Information security is a complex challenge. Among industry sectors, the financial sector is particularly aware of the challenge, in part because customer trust is so vital to the stability of financial services and the strength of the nation’s economy. At the same time, we are a favorite target of criminals operating in cyberspace and of terrorists, as was made clear on 9/11. The Deloitte Global Security Survey 2004 finds that the majority of global financial institutions have seen an attack on their IT systems within the last year, and that many of those



breaches resulted in financial loss. Eighty-three percent of respondents reported their systems had been compromised in 2003, versus 39 percent in 2002.”

Link: <http://www.bitsinfo.org/downloads/Testimony/rosenthaltestimony.pdf>

CHEMICAL

46. “Achieving Competitiveness and Security: Creating a Business Case for Security in the Chemical Sector”, Report prepared by TIAX LLC, Council on Competitiveness, 10/13/2006

InterCEP Highlight: In the chemical sector, effective security strategies support industry leadership/corporate reputation, reliable and sustainable operations and new product/service opportunities.

Key Points:

- “A major challenge for companies in the post-9/11 world is developing integrated security systems while remaining economically competitive in a globalized marketplace. The chemical sector’s reliance on physical assets and intellectual property make security a high priority compared to other industries. Yet many companies have an outdated security model, focusing on “guards, gates and guns” instead of integrating security with long-term strategic business planning.”
- “Security strategies, effectively implemented, support the following desirable business outcomes:
 - Industry leadership (corporate reputation)
 - "Security is the same as environmental performance," "when products and prices are the same" [customers] go with "the leader in the industry."
 - Reliable and sustainable operations
 - Security "gives us the confidence that we'll be able to operate and sustain our operation."
 - New product and/or service opportunities
 - “We see a large business opportunity for them to sell our security information management software system”

Link: <http://www.compete-resilience.org/upload/Chemical3.pdf>



ENERGY

47. “Creating a Business Case for Security in Electric Power and Natural Gas Industries”, M.C. Wilhelm Associates LLC, Council on Competitiveness, 10/13/2006

InterCEP Highlight: In the energy sector, integrated security generates cost savings (increased productivity, reduced losses, more efficient use of capital). In addition, new revenue streams can be created.

Key Points:

- “A major challenge for companies in the post-9/11 world is developing integrated security systems while remaining economically competitive in a globalized marketplace. Few industries are as vulnerable to terrorist attack as electric power and natural gas. Technological advances continue to make us more dependent on the energy sector, thus making security for its infrastructure more critical than ever.”
- “The business case for security revolves around 2 areas, both leading to increased cash flows and a positive ROI.”
- “First, cost savings are generated by exploring the synergies that security has with other business units and the strategic goals of the firm.”
 - “Increased productivity – Security that improves efficiency in productivity.”
 - “Reduced losses – In case of a security breach, a robust security strategy will reduce potential losses.”
 - “More efficient use of capital – At some point, as more and more money is spent on traditional investments, they become less effective. Spending money on more advanced security investments may be less costly and more efficient.”
- “Second, new revenue streams are created by exploring the value that security can generate with external stakeholders.”

Link: <http://www.compete-resilience.org/upload/EPNG3.pdf>

48. “Creating a Business Case for Security in the Oil Industry”, M.C. Wilhelm Associates LLC, Council on Competitiveness, 10/13/2006

InterCEP Highlight: The business case for security in the oil industry revolves around two areas (cost savings and new revenue streams) both leading to increased cash flows and a positive ROI.



Key Points:

- “The Council on Competitiveness has created the Competitiveness and Security Initiative to establish a business case for security. Like quality in the 1980s and safety in the 1990s, security can be embedded in core business processes in ways that create business benefits and positive economic outcomes: greater productivity, increased reliability and customer confidence, and savings in areas like risk management and insurance.”
- “The security function within the oil industry includes not only protection, but also risk mitigation. Given the global nature of the industry, it is not possible to maintain oil supply by focusing only on U.S. assets. Over 50% of oil used by the U.S. comes from overseas. Further, security risks overseas are typically more challenging.”
- “The business case for security revolves around two areas, both leading to increased cash flows and a positive ROI.”
- “First, Cost savings are generated by exploring synergies that security has with other business units and strategic goals of the firm.
 - Increased productivity: improve organizational efficiency
 - Reduced losses: decrease both the frequency and the impact of security and other events.”
 - “More efficient use of capital: invest in more efficient solutions rather than traditional security (guards, gates, and guns)”
- “Second, new revenue streams are created by exploring the value that security can generate with external stakeholders.
 - Business: enable business activities that fundamentally depend on security
 - Customer: develop security-related products and services
 - Competitive: leverage security capabilities to gain competitive advantage”

Link: <http://www.compete-resilience.org/upload/Oil3.pdf>

49. “Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout”, Adam Rose, Gbadebo Oladosu, Shu-Yi Liao, Carnegie Mellon Electricity Industry Center, October 14, 2005

InterCEP Highlight: The model-based simulation of a two week blackout in Los Angeles underscores the value of resilience with an 86 percent reduction in business interruption loss based upon adoptive resilience strategies.



Key Points:

- “This paper summarizes the development and application of a computable general disequilibrium model to estimate the business interruption impacts of the terrorist attack on the electricity power system serving Los Angeles County. The model has been especially designed to incorporate engineering and spatial aspects of the electric power system in the context of the regional economy, to reflect the several types of disequilibria that an electric power disruption will bring about, to include the various inherent and adaptive resilience responses at the individual, market, and economy-wide levels, and to capture both partial and general equilibrium effects. The simulation of a two-week total electricity blackout in LA County amounts to a business interruption loss of \$20.5 billion without any resilience adjustment and \$2.8 billion with the inclusion of several types of resilience, most prominently the rescheduling (recapture) of production after electric service is restored. The results indicate that inherent aspects of the electricity economy relationship (e.g., interfuel substitution) and adaptive behavioral responses (e.g., conservation, on-site electricity generation) can reduce the potential disruption impacts by 86 percent.”
- “In short, companies have started to realize that they participate in a greater ecosystem—and that their IT systems are only as resilient as the firms that they rely on to stay in business” (Corcoran, 2003; p. 28).

This is the link to the working draft, not to be quoted:

http://wpweb2.tepper.cmu.edu/ceic/SeminarPDFs/R_O_L_Bus_Int10_14.pdf

AVIATION

50. “Assessing the Impact of the September 11 Terrorist Attacks on U.S. Airline Demand”, Harumi Ito and Darin Lee, Brown University, Department of Economics

InterCEP Highlight: September 11th illustrated the capability of terrorism to impact an industry. The U.S. airline industry experienced both a negative transitory shock of over 30% and an ongoing negative demand shock amounting to roughly 7.4% of pre- September 11th demand.

Key Points:

- “This paper assesses the impact of the September 11th terrorist attacks and its after-effects on U.S. airline demand. Using monthly time-series data from 1986-2003, we find that September 11th resulted in both a negative transitory shock of



over 30% and an ongoing negative demand shock amounting to roughly 7.4% of pre-September 11th demand. This ongoing demand shock has yet to dissipate (as of November 2003) and cannot be explained by economic, seasonal, or other factors.”

Link:

http://www.brown.edu/Departments/Economics/Papers/2003/2003-16_paper.pdf

REGIONAL ECONOMIC RESLIENCE AND THE IMPACTS OF CATASTROPHES

51. “Florida Case Study: Economic Impacts of Business Closures in Hurricane Prone Counties”, Robert P. Hartwig, Insurance Information Institute, June 2002

InterCEP Highlight: Economic losses due to hurricanes can be staggering. Insurance generally covers only a portion of the losses experienced by businesses and in some cases insurance coverage may not be triggered due to lack of physical damage.

Key Points:

- “The purpose of this paper is to analyze the potential economic impacts resulting from damage or destruction of businesses following a major hurricane strike in Florida. The focus is on non-property losses suffered by businesses. Specifically, we examine losses in terms of the impact on the number of business establishments forced to close under various loss scenarios and the direct impacts on job and payroll loss, revenue loss and fiscal impact to the state in terms of decreased sales tax receipts. Various mitigation strategies adopted in Florida in the post-Hurricane Andrew era are also surveyed.”
- “Andrew struck south Florida in August 1992 with 140 mile-per-hour winds and produced insured losses of \$15.5 billion—about \$20 billion in current (2001) dollars. Economic losses were estimated at \$26 billion (\$34 billion in current dollars). Andrew’s reign as the most expensive insurance disaster in history ended, of course, with the terrorist attack of September 11, 2001.”
- “It is worth noting that some businesses may have business interruption coverage sufficient to compensate them for lost profits (i.e., net income—not revenues) and extra expenses they incur for some limited period following a disaster. However, because such coverage generally responds only when the business itself sustains direct physical loss or damage (or because authorities have closed off the area), the coverage may not be triggered in many circumstances.”



- Example of losses incurred in one county due to Hurricane Andrew at assumed 10% loss: Dade County: 4,918 (Establishment Loss), \$7,656,606,141 (Sales Loss) \$163,657,176 (Tax Loss), \$1,595,688,765 (Payroll Loss), 60,072 (Job Loss) \$9,415,952,082 (Total Dollar Losses)

Link: http://server.iii.org/yy_obj_data/binary/627581_1_0/hurricane.pdf

52. “Impact of Low-Intensity Hurricanes on Regional Economic Activity”, Robert T. Burrus, Jr., Christopher F. Dumas, Claude H. Farrell, and William W. Hall, Jr., American Society of Civil Engineers (requires subscription or purchase), August 2002

InterCEP Highlight: Lower impact/non-catastrophic events (such as low intensity hurricanes) can be more frequent than high impact events and have cumulative business interruption impact equal to that of a high impact event (such as a high intensity hurricane).

Key Points:

- Although low-intensity hurricanes cause far less structural damage than high-intensity hurricanes, these weaker hurricanes do impact regional economic activity through "business interruption." Because the strike frequencies of low-intensity hurricanes are orders of magnitude greater than those of stronger storms, the cumulative impact of frequent "business interruption" may be significant. Using Chamber of Commerce survey data, we estimate industry-specific business interruption losses for three low-intensity hurricanes striking the Wilmington, N.C., region. The average, per-storm regional impacts of business interruption, including direct, indirect, and induced impacts, are equivalent to between 0.8 and 1.23% of annual regional output, between 1.11 and 1.63% of regional employment, and between 1.21 and 1.81% of annual indirect business taxes. While these per-storm losses may appear small, the high strike frequencies of low-intensity hurricanes produce a cumulative (in expectation) impact equivalent to a high-intensity hurricane strike causing approximately \$3.7 billion in damage.
- “Business interruption has been found to have a significant impact on business losses following natural disasters (Webb et al. 2000). As the regional impacts of low-intensity storms arise mainly through business interruption rather than through structural damage, these impacts are not offset by large inflows of extra regional funds. The lack of offsetting reconstruction activity and the relatively high strike frequency of low-intensity storms raise the possibility that low-



intensity hurricanes may have a significant impact on regional economies over time.”

Link:

http://www.asce.org/files/pdf/hurricane/Structural_Performance_and_Damage_assessment/Impact_of_Low_Intensity_Hurricanes_on_Regional_Economic_Activity.pdf

53. “Effects of the 2001 Nisqually Earthquake on Small Businesses in Washington State”, Jacqueline Meszaros, and Mark Fiegener, Economic Development Administration, U.S. Department of Commerce Seattle Regional Office, October 2002

InterCEP Highlight: A relatively mild earthquake can result in significant losses especially to small businesses including losses in revenue, distracted and absent employees, building damage and inventory damage.

Key Points:

- “The 2001 Nisqually earthquake was a large magnitude (6.8 Mw) quake that yielded relatively mild ground shaking. Yet it was the costliest natural disaster in Washington State history. The fact that a relatively mild earthquake can yield such significant losses may be the most important lesson Nisqually has to offer.”
- “The most common disruptions from the quake were human and yielded hard-to-estimate indirect costs to businesses. Sixty percent of all small businesses reported that employees were distracted and unable to work for a period after the shaking stopped. In thirty percent of firms, at least some employees left work entirely to check on their homes and families.”
- “In the region a whole, excluding the most heavily damaged neighborhoods, approximately 20% of small businesses had direct physical losses. Sixteen percent lost less than \$100 but 4% of the region’s firms had losses amounting to 1% or more of their annual revenue. Losses were most commonly self-financed. Even the firms with the largest losses were more likely to self-finance than to receive insurance or other aid.”
- “Building damage was the most common and most costly form of direct loss in the quake. Large losses also resulted from damage to inventory and/or to data and records. Retail businesses were the most likely to suffer both building damage and inventory damage. Retail also reported the largest drops in revenue in the quarter following the quake.”

Link: <http://www.crew.org/Papers/nisquallysmallbusiness.pdf>



**54. “Business Losses, Transportation Damage and the Northridge Earthquake”,
Marlon G. Boarnet, Department of Urban and Regional Planning and Institute for
Transportation Studies., August 1996**

InterCEP Highlight: Loss of or restrictions in area transportation capacity can result in significant business losses.

Key Points:

- “The January 17, 1994 Northridge Earthquake damaged four major freeways in the Los Angeles area, creating the prospect of gridlock in the nation’s prototypical automobile city. This paper examines the effect of the transportation damage on business activity. Using survey responses from 559 firms in the Los Angeles area, this paper gives information on the extent and magnitude of the business losses that can be attributed to the transportation disruptions. Despite the fact that the freeway damage was repaired exceptionally quickly, 43% of the firms that reported any earthquake loss stated that some portion of that loss was due to transportation damage. For the firms that attributed some loss to transportation damage, the average response was that 39% of their earthquake related business losses were due to the disruptions in the transportation system. Comparing information on these and other survey responses yields several policy recommendations, which are summarized at the end of the paper.”
- “Despite the very quick response to the transportation disruptions caused by the Northridge earthquake, the economic losses from those disruptions were substantial. This should reinforce the importance of planning both to minimize transportation damage in future earthquakes, and to respond quickly when such damage occurs.”

Link: <http://www.uctc.net/papers/341.pdf>