

# RISK Factor

Volume 2 Issue 1

April 2006

## Six Senses of Loss Prevention

By Vincent Volpi

*If you're still relying on hindsight and historical benchmarks, here are six reasons why you should become more visionary in your loss prevention methods.*

### In This Issue: Loss Prevention

- Loss Prevention Strategies
- Five Fatal Distractions
- Safety & Loss Prevention
- Post-Katrina Telecom

#### Plus:

- News Briefs
- Moves/Notes
- Event Calendar

**Risk Factor is now  
Online!**

Visit  
**ldwpublishing.com**  
and read our  
Risk Management  
Weblog!

The world changed September 11, 2001. I was working in NYC responsible for global loss prevention for one of the largest US brands. Prior to the World Trade Center attacks, I had suggested to my employer security measures including a strict control of building ingress and egress, a chemical and biological attack response plan, mail and parcel screening, sophisticated Information Technology countermeasures and a business recovery plan. I was initially regarded as an alarmist. Now, I'm a visionary and these are best practices.

This is risk management -- predicting the next threat and preparing for it.

The losses to your company in the event of an emergency can be direct or indirect. In the days after 9/11, for instance, both the US and world stock markets plummeted. The New York Stock Exchange, the American Stock Exchange and NASDAQ did not open that day, remaining closed until September 17. When the stock markets reopened after the longest closure since the Great Depression, the Dow Jones Industrial Average (DJIA) stock market index fell 684 points, or 7.1 percent, to 8920, its biggest-ever one-day point decline. By the end of the week, the DJIA had fallen 1369.7 points -- 14.3 percent -- its largest one-week point drop in history. US stocks lost \$1.2 trillion in value for the week even though the majority of the US companies impacted had sustained no tangible damage on 9/11. The crisis was one of confidence, both consumer and investor, and doubts in the ability of our government to protect us. This is the objective and real cost of terrorism and economic warfare.

Planning for the unexpected is the job of those who manage the risk.

Now politely known as Business Continuity Management, "Disaster Planning" is a major part of a company's overall security strategy. It establishes a protocol for responding to emergencies (both manmade and Acts of God) and provides for the continuation of business and general security of management, employees, customers and ultimately, investors.

*(Continued from page 1)*

The threats companies face today may sound like the spy thrillers of a decade ago, but any solid security plan for a major corporation should address at least six areas of potential exposure. Following are six senses of security and questions that your company should address in formulating an effective business continuity plan.

**Facilities Security:** Is your facility secure? Can you centrally lock down every entrance and exit if necessary? Is your system fail-safe or fail-secure? Can you identify who or what is coming and going from your facility? Is it compliant with local building codes and fire laws? Do you have an evacuation plan? Facilities security is the most basic aspect of loss prevention but one of the most overlooked. A word of caution, now that many companies are assuming a “bunker mentality” in the workplace, the problem sometimes becomes maintaining security along with an inviting, comfortable and pleasant work environment and culture. Striking a balance is essential.

**Theft, Safety and Sabotage:** Protecting against traditional threats of theft, unsafe working conditions and sabotage involve adding integrity to existing processes and raising awareness of existing staff. Securing the supply chain is the key to combating theft and sabotage. This starts with controlling raw materials (including technology and trademarks) and then production, transport, distribution, administration and point-of-sale processes. Training and communication is fundamental in identifying and preventing workplace risks, including violence against or between employees. The common denominators in dealing with all of these threats are good people, policies, procedures, oversight and accountability. We are rarely victimized when we hire the right employees and vendors who are ready, watchful and accountable.

**Chemical/Biological/Radiological Agents:** Say the word “anthrax” and most people panic. However, anthrax is a naturally occurring disease encountered in the soil from livestock. It has been around for eons but only recently weaponized. It is not the only lethal chemical (poisons, nerve gases etc.) or biological (bacteria, viruses, prions) weapons governments have designed to “protect” us. Weaponized biological and chemical agents are a major threat today because they are small, virtually undetectable and have the potential to exact major harm and terror. Radiation weapons are also now a major new threat, especially with the advent of the so-called, dirty bomb -- a conventional explosive packed with easily obtainable low-grade radioactive material designed to disperse radiation over a broad area and render it uninhabitable for decades. An effective Chemical/Biological/Radiation Response Program needs to address isolation of the biologically, chemically or radioactively contaminated area if interior, the shutdown of the building HVAC system, evacuation or non-evacuation of the facility if threat is exterior, and emergency supplies of essential equipment, foodstuffs, water and communications, in the event that quarantine becomes the safest option.

The chemical /biological response program my staff and I developed for the Manhattan-based global brand owner was a model program that not many (if any) companies had at the time. Post 9/11, the New York Police Department approached us for a copy, which was subsequently used as a model in New York City’s Emergency Management Plan.

**Suspicious Packages and Bomb Threats:** Does your company have a plan for identifying and dealing with suspicious packages? Would every one of your employees know whom to contact, how to handle or not handle the package and how to react in front of your customers and their colleagues? Would your employees be able to protect everyone involved without inducing mass panic? Do you have a bomb threat and reaction plan? Do you know when to search, how to search and when to evacuate? The basic elements of these plans are simple to develop. However, if you wait until the event occurs, you may be considered negligent, put employees at risk and/or allow business interruption or serious damage to your assets.

**Internet and Related Threats:** Do you have authentication servers, intrusion alerts, user authentication, updated firewalls, virus and spyware definitions, and controlled access (including physical) to sensitive data? Do you use encryption? Do you monitor employee Internet (including file-sharing) activity and track footprints in the system? Do you limit supervisory access to your IT, control vendors, close “back doors” and other supervisory-access tools and vet users? To address Internet threats you need to do all this and more and this typically involves a close partnership between IT, LP and IT providers.

**Information Security:** The US is a world leader in intellectual property (IP) development - leading the way

(Continued from page 2)

in software and IT, engineering and chemical design, medical and pharmaceutical products, entertainment, luxury goods branding, consumer goods, inventions and more. It's not faster hands that deliver business advantages, its better ideas. According to a recent NBC Universal study, the intellectual property industries – computer software, entertainment, publishing -- are the most important growth drivers in the current US economy, contributing nearly 40 percent of the growth achieved by all US private industry and nearly 60 percent of the growth of US exportable products and services. The IP industries are crucial to the future growth of the US economy; gross domestic product ten-year growth estimates would be approximately 30 percent lower than current predictions without the contributions of these industries. Whether or not your company is in an industry deemed an IP industry, you have intellectual property. It may be your strategies, plans, methods; it goes beyond just your brand and your intellectual property is able asset.

**The technology that makes us more productive also makes us more vulnerable.**

### IS 101

Our ideas are often made through our technology, which also makes them more vulnerable to theft. Information security (IS), which is the protection of intellectual property and trade secrets, like customer lists and corporate strategies, should be a partnership between IT, IT providers, LP and the departments that produce the IP in your company. A basic IS plan has three major components: securing the machines or the devices that hold the information – the IT system; protecting the physical space that houses these systems; and guarding against corporate espionage or negligence -- the human factor.

To protect your IP technologically, you need to take the steps suggested above for Internet and related threats. Physical security concepts predominantly address access control and tracking workplace activities that include surveillance and cyber-surveillance.

Controlling the human element is not as easy. The technology that makes us more productive also makes us more vulnerable. Incredible amounts of data can be exported with a pocket-sized USB drive or via the Internet in an encrypted file transfer. You also can't prevent competitors from stealing your employees and the IP they take with them in their heads. And, increasingly, companies outsource work to consultants. Guarding against these very real human elements takes many forms. I have encountered numerous threats to corporate security including an employee caught trying to export a database of client information before leaving (detected though File Transfer monitoring), unscrupulous vendors "shopping production and samples" at factories who were stealing design specifications (uncovered when unauthorized products entered the distribution chain and were traced back to the source) and key employees violating non-competition and non-disclosure agreements (proved through a counter-espionage investigation and reverse engineering of products at issue).

The best way to control the human factor is to make sure you hire good, loyal employees and take care of them. No one ever left a company because they were happy and well paid. Also, obviously, limiting access to information on a need-to-know basis, monitoring information use and transfer and making all employees with access to sensitive information sign fidelity agreements with enforceable restrictive covenants and penalties, helps to deter unfair and illegal competition.

All companies must recognize we are functioning in an increasingly dangerous, global economic environment. We need to expect the unexpected. History has proven that it can and does happen. The most effective way to assure you are maintaining your obligation to your employees, customers and stockholders is to hire an expert consultant who understands and can evaluate existing and emerging threats in the industry, environments and cultures in which your business functions. This assures that cost-effective best practices are identified and implemented. Combined with regular compliance reviews, solid business continuity planning will make your company a hard target, while increasing profitability by protecting the bottom line and adding value for your stockholders in uncertain times.

*Vincent Volpi is the CEO of PICA Corporation, a Columbus-based private investigations firm specializing in security issues. The company website can be found at [www.pica.net](http://www.pica.net)*

## **Fatal Distractions: Five Steps to Ensure Your Workers' Safety**

*by Carl Potter and Deb Potter*

Workplace injuries cost over \$50 billion annually, according to the National Safety Council, so they're a major drain on profits across industries. When co-workers, family or members of our community are hurt or killed at work, the loss can be devastating.

Accident investigations usually reveal that injuries occur when something or someone distracts a worker on the job. He or she then hurries, takes a shortcut or decides not to follow safe work procedures, often resulting in significant personal injury as well as destruction of equipment and property.

On the bright side, you *can* eliminate most workplace injuries from your company. Managers and supervisors have a significant impact on worker safety and have a moral and legal obligation to provide a safe workplace. By identifying employee distractions and knowing what you can do, you can help workers avoid the devastation of an injury or fatality in *your* workplace. Consider these five fatal distractions and how to avoid them.

### **The Distraction of Production**

Employees face a tough dilemma when they feel pressured to complete work but don't feel as if they have enough time. Often, they'll take shortcuts so they can finish their assigned tasks in time. These shortcuts are fertile ground for accidents. To alleviate this distraction, consider the following: If your employees complain that they cannot get the work done in the time allowed, stop the job and listen to their concerns. You may need to allow more time or add more resources to the job. Also, collaborate with your employees to come up with plans that allow them to get the work done safely.

### **The Distraction of Time**

The distraction of time occurs when the clock determines workers' decisions about whether to do a job safely or to complete it by a deadline. Some companies have policies that limit overtime pay. When these policies are inflexible and the production requirements are stringent, employees and supervisors feel bound to the clock. This also occurs when workers decide that they want to finish the work during a certain timeframe, perhaps because they do not want to work overtime or they have other work that they want to move on to. To alleviate this distraction, ensure your employees know that no job is so important that they should take short-cuts in order to complete the work in a timely manner. Talk to your employees frequently about how working safely actually *saves* time. Discuss how much time an injury involves with investigations, lost work time and reports, not to mention the impact on worker morale.

### **The Distraction of Management**

Management can have a positive or negative impact on employee safety. When managers, supervisors and employees do not share common beliefs about the importance of safety, inconsistent communications result. Research shows that employees pay attention to whatever management pays attention to. If employees constantly hear about the need to reduce costs, increase production and improve quality while hearing little or nothing about safety, they will focus, like management, on everything *except* safety. To alleviate this distraction, be a positive influence by spending time every week with workers to show your interest in them. Ask your workers specific questions about their safety and health concerns.

### **The Distraction of Money**

Workers believe that the budget drives all corporate decisions. They may be right. If employees receive less training than they should have, and aging equipment is not maintained or replaced because budgets are tight, the number of recordable injuries goes up. To alleviate this distraction, review your budget to make sure you have funding for unexpected safety issues. Give workers, even in the lowest levels of your organization, the authority to tap into these funds when necessary.

*(continued on page 5)*

*(Continued from page 4)*

### **The Distraction of Personal Issues**

Employees often bring to work their off-the-job stress from family issues, financial concerns or other personal problems. Without realizing it, stressed and preoccupied employees can put themselves and others at risk of injuries. You may find it difficult to recognize when an employee is distracted by such matters, so take time to get to know all of the workers around you and pay attention to individual responses, reactions and attitudes. To alleviate this distraction, also consider the following: When you suspect that employees are distracted by personal issues, take them aside to discuss it. If necessary, temporarily reassign a worried worker who performs work that requires concentration. Assure employees who are having personal crises that you have their best interests in mind and that your goal is to return them to normal duties as soon as possible.

### **Think Safety for a Successful Future**

As a manager or supervisor, you can have a tremendous influence on employee safety. You simply need to make a focused effort to include safety into every aspect of your role. By adopting and demonstrating a personal commitment to workers' safety, communicating the importance of safety relative to production and quality, and recognizing when employees are distracted on the job, you can have a very positive impact on your organization's safety performance.

*Carl Potter, CSP, CMC and Deb Potter, PhD are advocates of a zero-injury workplace. They are speakers, authors and consultants to industry. Contact them at Potter and Associates International, Inc. 800-259-6209 or [www.potterandassociates.com](http://www.potterandassociates.com).*

## **Telecom Loss Control Post-Katrina**

*By John Savageau*

In the aftermath of Hurricane Katrina, there were stories of young people driving vans down to the Gulf Coast, setting up a portable generator, linking a wireless bridge to a "friendly" ISP to provide email and VoIP telephone access to neighborhoods cut off from the world. If a 19-year-old high school graduate with a portable generator can get global communications installed within hours after a natural disaster, then shouldn't we consider this model as a permanent solution?

To help New Orleans and the rest of the region recover, we need to deliver high-performance communications to every addressable home and business. We need to do it fast, and we need to do it under a reasonable budget. Buying telephone switches and copper lines, digging up the streets for either conduits and manholes, or planting telephone poles every 100 feet just doesn't make sense. The quicker and more cost-effective alternative is to take advantage of high-performance wireless technologies that are only restricted by the end user having electricity and the potential for a line of sight to a wireless transmitter.

In illustrating what can be done, let's take a look at a project that at first glance appears impossible. It takes place in the middle of the desert -- 500 miles from the nearest real city. The objective is to install a telecom network covering an area of about 150 square kilometers and make communications function at the same level as a city-based industrial campus. We must design a technologically advanced and flexible solution that meets or exceeds everybody's expectations ahead of schedule and under budget. Simple. Right?

In the middle of the desert we incorporate wireless bridging to connect major locations, VoIP to take advantage of lower startup and operating costs for both internal and external communications, a VSAT link to the home office, and then gateways for network connectivity and voice transit/termination. Using a numbering plan provided by the upstream VoIP provider, we have now created an extension of the office PBX located 3,000 miles away.

### **Science Fiction?**

The only lines in this scenario that aren't wireless are LAN connections, and they are really only useful to connect file servers to the LAN/WLAN or VoIP phones to the LAN. Anyone using a wireless PDA with a

(Continued from page 5)

softphone or WiFi handset would be completely wireless. Sound like science fiction? Surprise. This took place in 2002, more than three years ago in the middle of the Gobi Desert.

Shift to Seoul, South Korea at present day. Walking along the street, we see a lot of phone booths. Fun- There are no wires connected to these booths, and we see a little antenna sticking up from the top of each one. Wireless DSL.

Shift back to the hurricane-ravaged Gulf Coast. New communications systems are being installed and old developments are being demolished as part of the post-storm reconstruction effort. The new telecom tool bag includes Verizon Broadband Wireless, SBC broadband, DirecTV and a number of enterprising start-up companies, all capable of providing a Gobi Desert-style wireless hub. Any one of them could deliver a service equal to or better than those formerly riding on top of the old copper infrastructure.

### **Cost-effective Capacity**

What about capacity concerns with wireless? According to GigaBeam.com, we can sling up to 10 gigabytes per second through the air -- a pretty healthy bridge. That 10 Gbps is good for up to a mile, and the distance increases dramatically for lower speeds: 1 Gbps, a couple of miles, and other capacities around 512 megabytes per second, about 30 miles.

The truth is that in addition to being a lot less expensive, wireless actually can provide much higher capacity than existing copper cable. Plus, most people do not care if their communications and entertainment comes from Comcast, DirecTV, SBC, Verizon or Time Warner. They simply want the most advanced services available, regardless if it is over fiber, copper or through the air. They must have 450 TV channels, Internet that provides whatever content they desire with no delay and an effective way to communicate with any point in the world.

No solution is disaster proof. A backhoe, car accident, or any one of a thousand other variables can work to bring down a traditional telephone line as easily as a wireless connection. With a wireless network, recovery time is now as simple as restoring and aligning the antennas. Rather than months, service is back up in days.

As a society we need to prepare ourselves for the upcoming quantum shift in technology-enabled communications and entertainment. As business decision-makers we need to keep a close eye on the first movers and be prepared to go forward, either through R&D or M&A.

For New Orleans? Let's forget this traditional copper telephone line nonsense. Let's aggressively exploit wireless technologies and meet the needs of the community and businesses as quickly, efficiently and cost-effectively as possible. Really.

***John Savageau**, who has extensive telecommunications disaster recovery experience throughout the world, is senior vice president of operations at CRG West.*

### **Notes**

**NAMIC** is now offering e-learning publications for the agriculture risk inspection and underwriting areas. The **2006 NAMIC Farm Underwriting Guide** and the **2006 NAMIC Farm Inspection and Loss Prevention Manual** are available at <http://learn.namic.org>

**Risk and Insurance Management Society, Inc. (RIMS)** and **American Institute for Chartered Property Casualty Underwriters** and the **Insurance Institute of America (AICPCU/AII)** have launched a joint project to sell the Institutes' publications online. ARM study materials can be ordered at the RIMSTORE section of the RIMS website: [www.rims.org](http://www.rims.org)

**Horace Mann Educators Corporation** will offer scholarships totaling \$30,000 to help educators continue their education. [www.horacemann.com](http://www.horacemann.com)

## What's Cooking? Safety, Loss Prevention and the Bottom Line

By Robert Wellman

How do you increase your costs of risk? Untrained (or under-trained) workers, unguarded or inadequately protected production equipment, unsanitary working conditions and inattentive management are an excellent recipe. The recipe for financial loss is just as easy to follow: do not detect hazards, implement loss prevention measures, establish claim cost containment methods or identify root causes of loss. Ultimately, following either recipe will lead to impaired operating results.

Safer workplaces will improve the bottom line, guaranteed. Take advantage of all loss prevention services available from safety consultants, insurer loss control specialists and multiple technical resources. The ultimate goals for your operation management are:

- Reduced incident frequency and severity rates
- Healthier employees, customers and facilities
- Safer operations, products and services
- Improved profits through reduced risk costs

### Convince the Chief Cook

Loss prevention begins with one vital step: enlist 100% support from the chief executive. Whether s/he is the president, mayor, managing partner or chairperson, their belief in and support of your goals are the most important ingredients. Each of your next steps will be easier but no less important:

- Assess your operating structure and work flows
- Establish performance standards
- Identify and analyze specific job hazards
- Reduce or eliminate loss sources
- Establish measurable safety objectives
- Identify loss trends and benchmark results
- Create an environment in which loss prevention is valued, and
- Celebrate the impact loss prevention will have on operating results

By taking the time to identify loss drivers, achieve a safer workplace and improve bottom-line results, everyone wins. Reducing total costs of risk starts with understanding your operations and analyzing your loss controls. Creating customized solutions for specific operating hazards or unsafe practices will pay enormous dividends. Through careful allocation of risk management resources, focusing on specific problems will lead to fewer and less severe losses. Reduced loss costs will increase the bottom line. Follow this recipe and your risk management program will be a success...starting today!

*Robert Wellman is Managing Director and Head Chef of Wellman & Company, an independent risk and insurance consulting firm in Cleveland, Ohio. He can be reached at [rcwellmanjr@aol.com](mailto:rcwellmanjr@aol.com)*

### Coming in the May Issue:

- Updates on RMIS Systems
  - Post-Katrina Claims
  - Port Safety

**Don't Miss a Single Issue—Subscribe Today @ [www.ldwpublishing.com](http://www.ldwpublishing.com)**

LDW Publishing  
1465 Tullamore Lane  
Phoenixville, PA 19460  
www.ldwpublishing.com

---

## **Conference Calendar**

**April 23-27, 2006** RIMS Annual Conference and Exhibition, Hawai'i Convention Center, Honolulu, Hawaii. Online registration available at [www.rims.org](http://www.rims.org)

**May 8-12, 2006** Global Derivatives and Risk Management 2006, Le Meridien Montparnasse, Paris. New workshops include: interest rate derivatives, equity & credit derivatives, volatility, and credit derivatives. Register online at <http://www.icbi-uk.com/globalderivatives/>

**May 22-24, 2006** ACORD/LOMA Insurance Systems Forum, Mandalay Bay, Las Vegas, Nev. This year's theme: "Reimagine Your Business." To register, visit [www.acordlomaforum.org](http://www.acordlomaforum.org)

**June 4-7, 2006** 21st Annual CFO and Risk Management Conference & Expo, Hotel del Coronado, Coronado, Calif. Sponsored by Western Independent Bankers, San Francisco, Calif. For more information, visit [www.wib.org/cfo\\_conf.htm](http://www.wib.org/cfo_conf.htm)

**June 6, 2006** IASA Annual Educational Conference & Business Show, Sheraton Copley Place Hotel, Boston. IASA's Executive Education Program presents two executive roundtable events designed specifically for Chief Financial Officers and Chief Information Officers. [www.iasa.org](http://www.iasa.org)

**RISK FACTOR** is published monthly by LDW Publishing, Valley Forge, Pa.

### **Editorial staff:**

**Lori D. Widmer**  
Publisher

**Barbara F. Davis**  
Contributing Editor

**Kevin M. Quinley, CPCU,  
ARM**  
Contributing Writer

Mailing address:  
1465 Tullamore  
Phoenixville, Pa. 19460

Website:  
[www.ldwpublishing.com](http://www.ldwpublishing.com)

For subscription and all general information, call 610-933-7980 or email: [ldwpublishing@comcast.net](mailto:ldwpublishing@comcast.net)

*Copyright 2006 LDW Publishing. All rights reserved. Reproduction in whole or in part without written permission is prohibited.*