



Leadership in Manufacturing

Whether or not it gets painful is up to you.



[SUBSCRIBE](#)

[SEARCH](#)

[FEEDBACK](#)

- [DAILY NEWS](#)
- [ARTICLES](#)
- [COLUMNS](#)
- [ARCHIVES](#)
- [RESEARCH](#)
- [PRODUCTS](#)
- [BUSINESS TOOLS](#)
- [READER SERVICE](#)
- [SUBSCRIPTIONS](#)
- [MEDIA KIT](#)
- [EVENTS](#)

Articles - Publication Date 9.1.2004

## 5 Threats That Could Sink Your Company

These five threats could sink any company, including yours: Intellectual Property, Product Liability, Workplace Violence, Supply Chain, Business Continuity.

By [Tonya Vinas](#) and [Jill Jusko](#)



An industrial equipment manufacturer believes someone has stolen electronic copies of its designs. It hires an IT security firm to investigate, and indeed discovers the designs have been stolen via a breach in its IT systems. The firm tightens up its security but doesn't recover its lost sales. The FBI is now prosecuting the thieves.

Another manufacturer notices knockoffs -- albeit high-quality knockoffs -- of its patented product coming out of China. Considering the pros and cons of pursuing an injunction within the complex framework of global politics and economics, the manufacturer instead decides to license the Chinese manufacturer.

And in Roanoke, Ill., on July 13 of this summer, a storm with winds of 80 miles-per-hour and hail as big as softballs spawned a hurricane that leveled a plant belonging to Parsons Manufacturing. Production workers managed to escape to nearby shelters, but the plant was leveled. Gone. Nothing left.

These three stories are true. The injuries carried the potential to kill the companies. The first two companies recovered, bruised but smarter. It's not yet known if Parsons, a 29-year-old metal fabricator, will rebuild its 225,000-square-foot plant.

Today's manufacturing executives face heightened threats from traditional disasters, such as tornadoes, as well as ones not imagined just a decade ago, such as the large-scale terrorist attack the United States suffered on Sept. 11, 2001. Not only are the types of potentially fatal threats against companies increasing, but also the number of threats themselves is rising.

-  [E-Mail Article](#)
-  [Printer-Friendly](#)
-  [Reply To This Article](#)

**"Employees your biggest liability. Any you bring an employee or you're adding risk."**

**-- Jason Mor Background Information Services Inc**

- FROM THIS ISSUE**
- [All Systems Grow](#)
  - [The Next Preside The Record](#)
  - [The Next Preside The Record](#)

ADVERTISEMENT

PeopleSoft Manufacturing  
The ONLY complete  
**DEMAND-DRIVEN** solution

---

>> [READ AN AMR WHITE PAPER ON DEMAND-DRIVEN MANUFACTURING](#)

PeopleSoft®  
Manufacturing

"We're seeing an explosion in the reporting of security breaches," says Bryan Sartin, director of technology solutions at Ubizen, a Belgium-based IT security assessment and consulting firm with U.S. headquarters in Reston, Va. "Whether it's a large virus outbreak or IT people coming across a Web server that's been hacked, the number is increasing."

**IndustryWeek** looks at five areas where manufacturing companies are most vulnerable and makes suggestions on: shielding intellectual property and crucial data; protecting against product liability; keeping employees safe; securing your supply chain; and planning for business continuity.

While it may seem the world is a chaotic, threatening place to do business these days, those things that make it so also have opened doors to immense cost savings and growing revenues for many manufacturers. The agile manufacturer will be able to weigh the benefits and risks of such factors as capital equipment purchases, site location, supplier agreements and other day-in, day-out decisions. No decision should be made without considering risk, especially a risk that has the potential to sink a company.

## Intellectual Property

### *Do Unto Yourself, Then Others*

When it comes to intellectual property (IP) protection, Charles H. Mottier, who has 25 years of experience dealing with the issue, says manufacturers should follow a basic two-pronged strategy.

"Manufacturers should work to protect their own rights and products, and work not to infringe the rights of others," says Mottier, a partner with the Chicago-based law firm Leydig, Voit & Mayer Ltd.

Like The Golden Rule -- do unto others as you would have done unto you -- Mottier's rule seems simple, but in the day-to-day world it can be complex.

For instance, Mottier says, a supply chain easily can be disrupted by an accusation of IP theft. If a company's supplier has been so accused, and is hit with an injunction, the pipeline of supply stops -- and it doesn't matter that the customer has nothing to do with the alleged theft. Another example: The further globalization of manufacturing means large U.S.-based companies must engage in some IP transfer overseas, but models of best practices are still evolving.

Mottier says manufacturers can fall victim to having their patent rights violated or their trade secrets revealed. (Other areas of IP threats include copyright and trademark right violations.) This mostly happens in the consumer products industry (purses, shoes, small appliances) and at lower-tier parts manufacturers.

"It would be unlikely that an unauthorized car would enter the United States, for instance. It's more likely that a part to that car would."

Because parts are one of the most active IP-theft areas in manufacturing, Mottier recommends that manufacturers include in their supplier agreements, language that requires the supplier to work to supply a "non-infringing" part if it is hit with an IP-related injunction.

When dealing with overseas manufacturing, Mottier recommends aggressively reviewing and obtaining patent protection for products and then thoroughly reviewing potential partners before establishing relationships.

"I've seen instances where there was not a high-level of due diligence, and

the results were disastrous," Mottier says. "There are certainly Chinese manufacturers with integrity and [who] deliver good products. It's finding them that's the issue."

Being the victim of IP theft can mean lost sales for a manufacturer as well as effort, time and money in correcting the violation; but violating another company's rights -- whether knowingly or not -- also can harm a manufacturer in the way of lost revenue from a stoppage (injunction) or payment of damages. Some states have laws that could make an IP violation a criminal act as well. -- Tonya Vinas

## **Product Liability**

### *Design, Guard, Warn*

The bottom line on product liability is that manufacturers have a duty to design products that are not defective. The definition of "duty," however, is ever-evolving.

For instance, says Sheila Kerwin, an attorney with Minneapolis-based Hallenland Lewis Nilan Sepkins and Johnson, says the states are beginning to require manufacturers to take on "post-sale duties" for products. This means that they must notify customers when they improve the safety of a product that's already been sold, usually through recalls, retrofits or notices. This increased duty means more recording and maintenance of customer data -- and perhaps an assessment of how well your company is prepared to face product liability lawsuits.

"It's a double-edged sword for manufacturers," says Cynthia Arends, an associate attorney at the same firm, commenting on the post-sales duty trend. "Once your product is in the market . . . one, you may have a legal duty imposed that you have to do this [a recall or a retrofit], and you may just feel that you need to notify your customers and make a correction. While you may want to do this thing, which is a good thing, you also are admitting that there was a problem with the earlier product. This is something that will take manufacturers a bit of analysis -- legal and engineering analysis -- to determine the best course of action . . . What companies have to realize is that all of the documents they are preparing for that recall process undoubtedly will be involved in litigation."

For this reason and for overall preparedness, Kerwin and Arends recommend having a document retention policy, which would spell out what goes into documents and which documents are kept, and which are destroyed.

Kerwin says juries in product liability cases will look closely at engineering notes and other internal documents, for instance. "It's really good to talk to the engineers and tell them not to list 'unsafe' in their notes," she says.

Another trend affecting product liability is a shortening of time-to-market cycle coupled with increased regulation, which has made medical devices a ripe area for product liability.

"Any time you have very quickly changing regulations or industry standards, that's going to be a hot area," Kerwin says.

Of course, the best way to avoid product liability issues is to avoid putting defective products in the market. Kerwin refers to the "Design, Guard, Warn" hierarchy on this point: If you foresee a risk, design it out of the product; if you can't design it out, guard against it; and if you can't put a guard on it, list specific warnings on the product. -- Tonya Vinas

## Workplace Violence

### *Protect Employees And Yourself*

Background screenings would not have stopped 9/11," states Jason Morris of Background Information Services Inc. But they "absolutely" make for a safer workplace, says the president and co-founder of the Beachwood, Ohio, firm that provides pre-employment screening and background checks. "Employees are your biggest liability. Any time you bring an employee on, you're adding risk."

Workplace violence is a growing issue, says Shannon Shinaberry, an attorney in the labor and employment department at Cleveland-based law firm McDonald Hopkins Co. LPA. Employers have an obligation to address that risk, he says.

"There are laws called, for example, negligent hiring [and] negligent retention, where the employer can be responsible for violence that its employees commit," states Shinaberry.

He suggests a three-stage approach to protecting workers that addresses pre-employment, employment and termination.

During pre-employment, "Are you doing background checks? Are you doing screening? That's obviously the first step in being able to screen out people who are potential problems," Shinaberry says.

In the course of conducting background checks, Morris says his company finds that 9% to 11% of the persons under investigation have criminal records, while work and employment verifications uncover discrepancies 56% of the time.

Secondly, says Shinaberry, create protection within the workplace. "Have a workplace violence policy that everybody is aware of and everybody understands. A policy that prohibits any weapons being brought into the facility and even a policy that makes it known that if you have lockers or areas that employees use, they should not consider those to be private -- that the employer reserves the right to be able to search those," the attorney says.

Train supervisors to recognize the signs of potential workplace violence, Shinaberry says, and then make it clear "who they need to come to if they recognize these problems potentially developing." The policy should state how management responds to a developing issue once it is reported. The policy also should address terminations "to make sure that you eliminate the potential for violence against co-workers and against the people in management who are delivering the news."

A step-by-step workplace violence policy eliminates confusion, Shinaberry says. "[It] allows you in a very precarious situation to address it appropriately and immediately." -- Jill Jusko

## Supply Chain

### *Minimize Opportunities To Disrupt Flow*

The supply chain is all about the flow of goods from the point of origin to the ultimate point of destination, states Scott Elliff, president of Capital Consulting & Management Inc. (CCMI), Charlottesville, Va. "The more

opportunities you have for disruptions of any kind . . . all those things disrupt the flow of merchandise."

Earlier this year, Elliff's firm developed a "supply chain executive agenda," which urged companies to develop more comprehensive supply-chain security plans to keep product moving in the event of disaster anywhere along the chain.

Simply carrying extra inventory is not the solution. "That is often the first, knee-jerk reaction that a lot of people have," he notes. "History has shown you can never really have enough of the right inventory at the right time to cover those sorts of issues."

Instead focus efforts on other practices that can make a difference. For example, Elliff says, manufacturers must get familiar with U.S. Customs regulations and be prepared to comply with them. The federal government has added or bolstered programs to strengthen supply-chain security at the borders. Manufacturers -- or their suppliers -- who fail to comply run the risk of delaying the movement of goods.

Additionally, consider developing an alternative sourcing option. "If you are sourcing all of a particular component from one place, and you don't have a secondary supplier identified, then you don't have much recourse if there is an issue associated with that supply line."

To the extent that they can, Elliff advises manufacturers to develop commonality of components. "If each individual product is all unique components, then you've got a lot of risk if there is any issue," notes Elliff. Common components, or components that share enough common traits to qualify as emergency sources, mitigate risk if suppliers don't deliver.

On a grander scale, it may be time to simply reassess sourcing and production locations as a whole. Manufacturers with at least some U.S. production should consider developing "surge" capacity, otherwise known as extra capacity that could be drawn upon -- at least temporarily -- if other production locations were unable to deliver, the consultant says. Additionally, he says, consider whether the manufacturing equation has changed to the degree that it no longer makes sense to source halfway around the globe. "Maybe Mexico makes relatively more sense than it used to," he suggests. "It's a land route closer to the U.S. It has higher labor costs than Asia but . . . a much shorter cycle time."

"The idea is to think about the whole globe in the potential set of sources more systematically," he says. -- Jill Jusko

## **Business Continuity: Succession Planning**

### *Make It Formal, Make It Fluid*

Whether a CEO's departure is planned, as in a retirement, or unplanned, as in an unexpected death, "the concept behind succession planning remains the same," says Keith Greene, director of organizational programs at the Society for Human Resource Management, Alexandria, Va. "And that is to prepare the organization for a smooth transition and continuity."

He points to fast-food chain McDonald's Corp. as a textbook example of a well-executed succession. When former CEO Jim Cantalupo died suddenly earlier this year, his successor was named the same day. "It's very clear that McDonald's had a formalized succession plan in place, and when their CEO died suddenly, they invoked it immediately. It's not like they had to dig something up or dig it out. It was there."

He adds, "I think McDonalds' bottom line was helped by such a smooth transition under horrible circumstances."

Greene believes succession plans should be formalized. "It should be written and it should be fluid, so it needs to be reviewed probably twice a year to make sure it's current and still accurate."

The plan should include every member of senior management, he says. They must be involved not only in its creation, but also each of their positions also should be addressed. Additionally, "some organizations -- even outside of senior management -- have very, very key positions that they need to ensure succession for," Greene notes. "Sometimes it's a technical person. What if that person leaves? You have to have a plan in place to protect the organization."

Business consultant Paul Rich believes a successful succession plan includes fostering an organizational culture that nurtures potential heirs apparent. "[If I'm CEO] I'm trying to develop people in my company that have and can grow and learn leadership qualities. And my job is to make sure that within the company there are one or two or three people who would have the ability to jump into the CEO's shoes."

That is accomplished via training and mentoring, says Rich, principal with the Seigel Rich Division of Rothstein Kass certified public accountants.

A caveat to any succession plan, says Greene, is that an organization "is going to do its due diligence to ensure that the best person is put in the job. And that could include an external search to complement an internal search."  
-- Jill Jusko



[Rate This Article](#)

#### **[Subscribe To Inside Track:](#)**

**IndustryWeek's** Inside Track offers a free weekly update - specifically for the busy executive. Delivered right to your email account are highlights of and links to key articles, newswires and columns from some of the leading thinkers in manufacturing management. [Sign up today.](#)



**ONLY PEOPLESOFT**  
gives you every advantage at every level.

[>> READ AN AMR WHITE PAPER ON DEMAND-DRIVEN MANUFACTURING](#)

**PeopleSoft.**  
Manufacturing

[SUBSCRIBE](#)

[SEARCH](#)

[FEEDBACK](#)



Copyright© 1998-2004 [Penton Media, Inc.](#) All rights reserved.  
[Penton Media's Privacy Policy](#)

Technical questions or bug reports  
E-mail [webmaster@industryweek.com](mailto:webmaster@industryweek.com)