

# SECURITY

A good loss-prevention and security program does many things. It minimizes loss, streamlines operations, gives employees peace of mind, and—perhaps most surprisingly—contributes to overall profitability. That's the experienced-based philosophy of Barry Brandman, president of Danbee Investigations in Midland Park, N.J.

Brandman's firm works with more than 600 major companies, providing a range of security and investigative services. One of the firm's particular areas of expertise is logistics and supply chain. Reflective of this, Brandman is a frequent guest speaker at organizations such as the Council of Logistics Management and the Warehousing Education and Research Council.

Supply chain security is foremost in the minds of U.S. companies today for many reasons—some obviously more painful to recount than others. But companies have to do more than think about the problem, says Brandman. They need to act in a smart and effective manner. Yesterday's solutions are no match for today's security challenges, he emphasizes. Supply chain managers have to meet the new challenges with a combination of management commitment, efficient procedures and processes, and advanced loss-prevention technology.

Brandman was interviewed recently by Supply Chain Management Review Editor Francis J. Quinn.

PHOTOS BY MARC ASNIN/CORBIS

**Q:** From a supply chain security perspective, what changed on 9/11?

**A:** I think the biggest lesson that we learned about security is that there's a difference between being good and being lucky.

To tie that into airline security, for example, prior to 9/11 we did not have a major act of terrorism—not because our security controls were so effective, but because we were lucky that nobody launched a strategic attack on us. A lot of corporations have taken that lesson to heart. They're re-examining their own corporate security programs to determine whether they have avoided problems because their programs are that good or because they've just been fortunate. Obviously, if you're lucky, it's only a matter of time before your luck may run out. So the bottom line is that cosmetic security is no security. Your security controls need to be meaningful, strategically designed, and diligently maintained. And if you're not doing that, then you are unnecessarily exposing your company to internal and external loss.

**Q:** What's the difference between cosmetic security and meaningful security?

**A:** I'll give you a couple of examples. We went into a company that sustained a significant inventory loss. In an attempt to determine where the missing product might have left the building, we decided to utilize the company's existing video system. They assured us that they had a very expensive closed-circuit TV system in place. But when our investigators went in, they found that the cameras watching the docks gave only very broad, distant images of the product. The problem was that we couldn't use the video to count pallets going out or coming in the dock doors.

Now had we designed that system, for example, we would have positioned the cameras in different locations, used different lenses, and different recording equipment. We would have designed the system so that everything that went through the shipping or receiving doors was clearly recorded.

# MATTERS

“ Companies with theft problems find that they very, very rarely go away on their own. ”

—Barry Brandman,  
President of Danbee  
Investigations



We would have been able to recreate reality, so that we could accurately count the number of pallets we saw going out the various doors, compare it to the manifests, and look for discrepancies. But because the existing video system was poorly designed, it turned out to have no value whatsoever. So the \$70,000 that they spent on that video system gave them no return when they really needed it.

Another example involves a company that had an internal problem with theft and deliberate destruction of company equipment and product. On top of that, they also had rampant substance abuse. Because they received no warnings via their open-door policy and in-house tip-line, they initially had difficulty believing that their problems were as bad as they really were. But the reality is that the concept of an open-door policy is fine for a lot of things, but it doesn't work for security-sensitive issues. Employees are reluctant to come forward and speak openly. So because the employees did not feel safe and secure in coming forward and knocking on the door of a manager or human resources or legal, they kept the information to themselves. And because they feared they could be identified, they didn't use the company tip-line. So the problems continued and worsened over time.

The extent of the problems was really brought to light once the company outsourced the open-door policy to us. Once the employees realized that they could call an outside company, and the people on the other end of the phone would not ask them their names and would not recognize their voices, suddenly we started getting calls. That enabled this company to identify the people who were responsible and put a stop to the loss and damage.

Now did this company have the right idea with an open-door policy and in-house tip-line? Yes. But was it effective? Just like with the video system, no. So there is a right way and a wrong way to set up and implement your loss prevention. Again, tie this into airline security. We had metal detectors, x-ray scanners, personnel, card access, alarm systems, and video cameras. But did we really have the right equipment and the right people in place? Absolutely not. So we had an illusion of security, and a false sense of security is no security whatsoever.

**Q.** Have theft and disruptive incidents increased in recent years?

**A.** It's difficult to track because most companies don't report them. Companies are not anxious to air their security problems out in public. So a lot of what we learn is told to us in confidence; a lot of what's discussed in the industry is anecdotal. But some general statistics and surveys are available. I think that cargo crime right now, statistically, is

“ If you don't have senior management support for loss prevention, then you're always going to have an uphill struggle. ”

about \$10 billion a year. That number has gone up dramatically for the last five successive years. From talking with other experts in the industry and from studies I have seen, it's clear that the problems are growing and getting worse.

Some part of this is being fueled by our criminal justice system. The reality is that the system simply does not take economic crime seriously. The penalties handed out for economic crime, in some cases, are disturbing and, in other cases, are absolutely outlandish. And, by the way, that's one of the reasons that some professional crime organizations have shifted from drug smuggling to logistics theft. The penalties for getting caught bringing in kilos of cocaine are probably five times as severe as getting caught hijacking a truck or breaking into a warehouse. They are a slap on the wrist compared to what they are for drug trafficking. So a lot of these organized crime organizations have shifted from drugs to freight because the risk is a lot less, and the penalties are nowhere as severe.

With respect to how security problems can grow, it's important to remember that theft is addictive. Companies with theft problems find that they very, very rarely go away on their own. It's just as uncommon for a theft problem to stay at the same level over a long period of time. Theft is an economic cancer and, very much like cancer, has a tendency to grow if it's left unchecked and not treated aggressively.

**Q.** What types of products are most susceptible to theft or supply chain disruption?

**A.** Anything that has intrinsic value can potentially be stolen because there's always someone out there willing to pay for it. Some people think that if their company doesn't deal in gold dust or diamonds, they don't have to worry about theft. But the reality is that dishonest people will steal what they touch if they can find an outlet to convert that product into cash. That's how these individuals look at inventory today. They don't see cases of goods; they see cases of cash that can be converted into net profit. And every dollar they make goes right into their pocket. They don't pay taxes on it, state or federal. Whoever said crime doesn't pay obviously lived in a different century because it not only pays, but it pays very handsomely.

**Q.** What are some of the supply chain impacts of a security-related disruption like theft?

**A.** There are several—some obvious and some not so obvious. Obviously, you have the cost of the loss of the goods, which is a big problem. But you have indirect costs as well. If you operate on a 10-percent gross profit and you lose \$100,000 worth of goods, you need to do \$1-million worth of sales just to break even to replace the expense of the lost goods. Plus, you have to factor in some subliminal costs that are not so apparent, such as the time and labor involved in

reordering, re-receiving, restocking, remanifesting, and reshipping those goods. When people estimate their losses, they tend to look at the shrinkage numbers and don't bring into that formula the ancillary costs, which are very important.

Another ramification of inventory loss with consumable goods is that you don't know for certain whether or not the product's been tampered with when it hits the market. If it has and somebody, hypothetically, has introduced ground glass, a biological agent, a chemical agent, whatever, and they've caused people to become ill or even worse, the public's not going to know that those goods were tampered with when they were in someone else's hands. They're going to look at the company name on the label and hold that company responsible both ethically and legally.

There is also the issue of brand integrity. Do you want your product being sold for 50 to 70 percent off its legitimate value? When your goods are stolen, you have no control over who will end up reselling them and at what price.

If the theft involves a component used to make a finished product, then there's another impact. For example, if you're building a computer and you don't have all of your components in stock because some have disappeared, you can't complete the assembly of the finished product. Obviously, that's a huge productivity issue, especially with many firms going to just-in-time (JIT) inventory systems.

**Q.** Are there certain recurring problems that suggest supply chain people are not looking at security in the right way?

**A.** Supply chain people need to begin by understanding the value of prevention and not reaction. We often like to use the term loss prevention, as opposed to security. The connotation of security is someone sitting behind a desk waiting for the phone to ring to be apprised of the fact that you've had a major breach. That is not the smartest, most

cost-effective way to protect your company. It makes far more sense in terms of time, money, resources, and aggravation to dedicate your efforts to preventing problems from happening. There's a reason that some of the smartest, most successful companies focus their efforts on preventing problems rather than responding to them after they take place.



**“ Successful loss prevention will not only save you money but also increase morale because your good people want to work in a theft-free, drug-free environment. ”**

Now, if you want to go into some specifics of where companies are missing the boat, I think they're spending their security dollars in areas that don't give them a maximum return on investment. And it's not that these companies don't have budgets appropriated. Instead, it's *how* those dollars are being utilized that is not really generating income on their bottom line. This surprises a lot of people, but we don't necessarily come in and ask them to spend more money on security. In some cases, we'll work with their existing budgets; in other cases, we'll actually reduce those budgets significantly by using the money in a smarter way.

**Case in point:** For a major manufacturer with numerous manufacturing and distribution centers throughout the country, we were able to save \$380,000 a year from their security budget by eliminating unnecessary manpower and then substituting the manpower with more strategic policies and procedures while integrating certain types of security electronics. Not only did the company's shrink

numbers dramatically improve, but they were able to put almost \$400,000 of what used to be an expense item on the security budget right back onto the bottom line. Between the reduction in losses and the reduction in the security budget, they were able to gain more than a half-million dollars a year in newfound profitability. So a company needs to look at what they're spending and ask themselves this question: Are we investing our money in the best possible ways? Is security contributing to our bottom line, or is security an expense item on our income statement? If it's an expense item, then you're not doing something right.

**Q.** What are some of the traits of companies that have good supply chain security?

**A.** Two things come to mind, and this is by no means a complete list. First is the buy-in and support of top management. One of the best companies in the country in terms of inventory loss and other types of business-related crime is a big publicly traded company whose CEO is so supportive of the loss-prevention function that he actually takes the time to read reports generated by his loss-prevention people and outside consultants. When you have a CEO or a senior vice president that pays that kind of attention to loss prevention, that's going to permeate throughout the entire organization. That is a company with tremendous opportunity for loss prevention to impact their bottom line.

Now conversely, if you don't have senior management support for loss prevention, then you're always going to have an uphill struggle. You will be spending your time trying to convince people why they should support your efforts and buy into the program. You shouldn't have to waste your time doing that. You need to be able to focus your energy on just getting the needed results. In short, there is absolutely no substitute for the unequivocal support and backing of senior management.

Second, companies that successfully protect their corporate assets also don't go into denial, and they don't rationalize. They keep careful quantitative track over their assets. And when their numbers are not right, they don't try to bury the problem or blame it on a faulty MIS (management information system) or some other operational excuse. They're quick to say, "We might have a problem, so let's investigate and find out whether or not we really do. Let's not wait six months and vacillate before we leap into action."

**Q.** You've talked about the threat of Internet or cyber theft. What forms can these disruptions take within the supply chain?

**A.** One of the big concerns here is the theft of proprietary information—customer lists, P&L (profit and loss) statements, marketing plans, and so on. You obviously don't want that information ending up in your competitor's hands. Another concern is an attempt at sabotage where somebody shuts down your ability to operate on a day-to-day basis by closing down your network. An example would be the deliberate planting of a virus or a worm that causes your system to crash and come to a complete stop. If you ask a group of people how difficult it was for them the last time their network went down for an hour, you get those knowing smiles, and everybody starts nodding their head. Now if I ask them what their lives would be like if someone deliberately

crashed their system for a week, everybody goes, "Whoa!" Logistics is driven by computers. Your ability to communicate with your customers, to communicate internally, to track your product, to get your product selected, loaded, inventoried, priced, manifested ... nobody does these things manually anymore. So if somebody were successful in taking down your system or corrupting it or giving you permanent data loss, you could lose literally millions of dollars.

That's the high-tech form of sabotage today. And it could be done by somebody sitting 1,000 miles away in a basement or by someone inside your company on the third floor in a corner office.

**Q.** What role is technology playing in loss prevention today?

**A.** Technology is a big part of programs we're setting up. One example is how we are helping clients protect against the growing threat of organized crime rings posing as legitimate truckers. The criminals are sending their people up to the company's dispatch office with bogus carrier identification and are being given loaded containers of product. They then drive out of the yard never to be seen again. On our advice, clients now are mandating that all

outside trucking companies that they use to deliver their high-value goods must take digital photographs of their drivers. Before a pickup takes place, the carrier is required to electronically transmit that driver's photograph along with a confidential pickup number. My client will then download that data. When the driver

comes in and says, "I'm here to pick up a load of \$780,000 worth of your product," they'll say, "Fine, do you have a company ID? Okay. Do you have a manifest? Okay, thank you. Now please come to the window because we want to take your digital picture, and we're going to compare your face in the window to the face we have on our computer screen and see if it matches. And by the way, we're videorecording the transaction as well."

Now if you are a bogus driver, you're not going to get possession of that container. And if somehow you do because the dispatcher was careless and failed to match up your face to the face on the digital photograph, then we can electronically transmit that driver's image to every law enforcement agency within 100 square miles in less than 60 seconds flat. So basically we've taken security technology, married it with best practices, and come up with an almost fool-proof way of preventing bogus drivers from absconding with loaded containers.

Digital videorecording is an important technology. Note that I said videorecording not videotaping because there are no tapes involved. To safeguard our clients' server rooms or high-

"The supply chain obviously is one of the most significant targets for rogue governments and terrorist cells that are hostile to the United States."

value areas, for example, we will set up digital video cameras that automatically begin recording onto a hard drive as soon as they pick up the presence of anybody or anything that changes the pixelization in the field of view. When coupled with biometric access and intrusion-detection technology, it becomes exceedingly difficult for anyone to gain unauthorized access to these areas without the company knowing who it was. This type of security is also a powerful deterrent.

**Q.** You've encouraged supply chain managers and their companies to embrace the new security trade initiatives such as C-TPAT (Customs-Trade Partnership Against Terrorism). Why is that so important?

**A.** To begin with, we as a nation have to do everything possible to prevent another act of terrorism from being perpetrated on American soil. The supply chain is obviously one of the most significant targets for rogue governments and terrorist cells that are hostile to the United States. Given the number of inbound shipments that we bring in daily and the number that can be physically inspected, Customs has a very, very difficult job to do. In fact, it's almost impossible. I think the government has recognized that, which is why they look at this program as an important partnership with the business community.

So the first benefit of participating in C-TPAT is to help ensure that we never have a weapon of mass destruction detonated in the United States. Let's work down from there. Companies that implement good supply chain security practices not only dramatically reduce the odds of a weapon of mass destruction being smuggled into one of their containers or cartons but also dramatically reduce the odds of their product being contaminated. And if you're in industries like health and beauty aids, consumable goods, pharmaceuticals, and so on, you want to make sure that your product is absolutely sterile and free from contamination.

Effective loss-prevention measures also dramatically reduce the odds of your product being stolen. So many of the same safeguards that will protect against a weapon of mass destruction from being smuggled in will also safeguard the integrity of your product.

Another reason to participate is that many companies in the United States have outsourced their finished goods production or are bringing in parts for JIT-type manufacturing. Rather than stockpiling six months' worth of inventory on their shelves, they're saving a tremendous amount of money by only stockpiling two or three weeks' worth of inventory and, in some cases, even less. Obviously, they are very much dependent on keeping the supply chains flowing—on getting that product received at the port of importation and then either trucked or trained over to their facility. If you do not have C-TPAT certification, you will not get your goods in nearly as fast as those companies that are certified. In essence, C-TPAT is going to result in an EZ lane, just like you're on the Garden State Parkway. If you don't have an EZ Pass, it's probably going to take you twice as

long sometimes three times as long to get through the cash toll booth. In simple terms, that's a good analogy to make at our major ports now. Why in the world would you want to take three days to have your container unloaded if you can get it unloaded in one day?

Now think about what would happen if we go to a high-security alert and clamp down on imports and close our borders, as we did on 9/11. When those borders open up, there's a real good chance that the C-TPAT imports are going to get first preference coming into this country. You don't want your product to be number 222 in line for clearance when you see the C-TPAT containers moving in like clockwork. The question to ask is, what is the cost of your goods *not getting* into your hands? There's a reason why some of the most successful companies participate with C-TPAT.

**Q.** Is there anything to be fearful about or intimidated by the C-TPAT certification process?

**A.** I understand the concern some companies have about the government coming in and looking over their shoulders at how they operate their businesses. But I truly believe that the spirit of C-TPAT is that the government wants to work with trade in a mutually cooperative, productive, and beneficial way. This is not a gotcha-type program. The government is not looking to come in and disrupt a company's ability to conduct business. Instead, they're really looking to partner with trade. The government realizes that this approach will reduce the odds of a terrorist act taking place successfully here, while at the same time enabling Customs to do its job in a much more productive manner.

Customs needs to profile high-risk shipments coming into the United States. With the millions and millions of conveyances that come in every year, there's no way to inspect every container. It's impossible to inspect even 25 percent of them. The only way Customs can do its job is to identify high-risk vs. low-risk containers. That's really, in a large part, what C-TPAT is all about.

**Q.** Could you talk a little more about the tie-in between security and profitability you mentioned earlier?

**A.** If we can go into a company and show them that whatever they spend on us, we can return it to them dollar for dollar—and in some cases actually give them more—that's a very persuasive argument. And that goes back to the concept I mentioned before about how successful security contributes to bottom-line profitability. Successful loss prevention will save you money in numerous ways: It will allow your company to operate more efficiently; it will minimize the odds of your product being deliberately contaminated or sabotaged; it will prevent delays and gaps in moving the product to market or to your assembly facilities; and it will not jeopardize your customer good will. And it will increase morale because your good people want to work in a theft-free, drug-free environment. Ultimately every dollar you

*Continued on page 45.*

lose comes right off your bottom line. Consequently, this means that every dollar that you can take off your loss category and put back onto your bottom line is pure 100-percent profit. If you understand these economics, it's easy to justify the importance of loss prevention.

The problem is that some security programs have become antiquated or stale, and they haven't been able to quantitatively prove their contribution to profitability. And when a company gets into hard economic times and starts thinking about cuts, they're going to look at those entities on their balance sheet that contribute to the bottom line vs. those that are an expense item. The expense items, obviously, are going to be the first targets to go.

You can never become complacent. Understand that security problems today are different than they were 10 or 15 years ago. If you're relying on the same safeguards you had 10 or 15 years ago, there's an excellent chance that your program is not using the smartest, most-effective practices. You need to look for constant improvement and always measure your results. Basically, it comes down to staying innovative and being results-oriented.

**Q.** What should supply chain professionals be doing right now to enhance security in their organizations?

**A.** The first step is to take an "MRI" of your asset-protection program. If you have the internal

professionals with the expertise to do a vulnerability assessment, fine. If not, go to an outside company to have it done. You need to identify where your supply chain may be vulnerable, where your program is weak, where you're lacking needed safeguards, where you need to make improvements. You also should identify your strengths so that you can build upon them. Then start identifying what action needs to be taken, the costs and benefits of those actions, and the timetables involved.

The next step is to put together a loss-prevention program, which will vary depending on the type of company. In a small company, this may consist of setting up an outside hotline program, doing background investigations of people hired into security-sensitive positions, periodically conducting on-site audits of your facility, and providing management training to your people.

In a bigger company, the program obviously would consist of much more, depending on the size and nature of your business. But that's a difficult question to answer and paint with a broad brush. You really need to break it down by company size, considering such factors as number of facilities and employees, type of product, and history of security problems.

But the bottom line for companies of any size is that loss prevention is good business—and it doesn't necessarily have to cost you money. When done right, it can make you money. That's really the key.

