

# Secure your mail center

How to achieve security in your mailstream operation without losing efficiency

By Dr. Robert F. Hahn II

Five and a half years after the post-9/11 anthrax scare, mailstream security continues to be a serious issue. The recent spate of letter bombs in London and pipe bombs shipped to people in the Midwest shows that the mailstream is continuing to be used as a weapon. In addition, we've seen terrorism and activism taken to extremes, with people willing to use toxic agents, chemical weapons and radioactive dirty bombs. The aim frequently is anarchic disruption of your organization's operations. To the dismay of all of us, hoaxes are equally effective.

Certain sectors are more prone to receiving suspicious letters and parcels than others. Government has an incident rate that's 155% above the average. Finance and banking are 137% above the average and high technology is 91% greater than average. But even if you're not in an industry with a high potential to be a target, cross-contamination, which was an exacerbating factor in 2001, is a threat to us all. The office buildings or industrial parks your facilities are situated in may also be close to some prime targets.

It is important to secure your mailstream operation, first and foremost, for the health and welfare of your employees and customers. We should always remember that safe mail

handling is a corporate benefit that gives people peace of mind, shows that you care about them and that you will do whatever it takes to ensure their well-being.

Securing your mailstream operation is also important from an economic point of view. Depending on your business, the cost of a disruption caused by a breach in mail security can be huge. The figure can vary from less than \$50,000 to more than \$5 million per hour. If that last number sounds high, think about financial services organizations whose operations are transactional in nature. Shutting down a trading floor for concerns about contamination will have catastrophic impact on the revenue stream. Then there's the cost of clean-up. Depending upon the nature of the contaminant, these costs can be substantial. Entire automated systems may need to be scrapped. It often costs less to replace a facility entirely than to clean it up.

Recognizing the seriousness of all these issues, it is still important to remember we need to keep our operations functioning effectively. Here are some things you can do to achieve security in your mailstream operation without losing efficiency.

**1** Do all initial acceptance of your mail off-site, away from your main facility. Isolating your incoming mail operation

from your place of business is the single most effective thing you can do to avoid disruption from either a hoax or an actual threat.

**2** Have X-ray screening or explosive detection screening installed. X-ray systems will alert you to the presence of powders as well as bombs.

**3** Provide some kind of containment. There are pre-fabricated enclosures that can accommodate all your incoming mail processing systems. Their negative pressure capability prevents contaminants that have become airborne from spreading.

**4** Train your mail center personnel on visual recognition of suspicious mail and packages. This includes looking for things like no return address, restrictive markings such as "Personal," addresses to title only, strange odors and discolorations.

**5** Establish response procedures to various incidents and rehearse them. What do you do with each kind of suspect mailpiece (e.g., do you cover an explosive package or not?) What do you do in the facility (e.g., do you shut down the air ventilation or not?) Which emergency responders do you contact and in what sequence (e.g., FBI, USPS postal inspection services, doctors). When and how will you alert employees?

**6** Conduct mailstream security audits. These are formal reviews in which you document all the ways someone might get something into the mailstream. A valuable benefit of these security audits is the fact they will also reduce theft. Knowing where your security holes are tells you where your theft vulnerabilities are, too.

**7** Conduct background checks on employees. Like maintenance workers, mail center employees can impact a company's security every day. Yet because these jobs are low in the organization and often have a high turnover rate, time is not taken to do the thorough background checks these positions warrant. Take the time. Do the checks.

**8** Create documented processes and workflows for your mailstream operation. This is a continuous improvement procedure that can make your security operation more time-efficient and cost-effective. And in the event of a disruption, you will know where to pick up the process.

**9** Put into place a system for mail tracking and accountability. Always know where the mail is going and be able to confirm that it got there.

**10** Make safe mail a corporate policy. Set up rules for mail handling throughout the organization, not just in the mail center. Make sure everyone is aware of the procedures and follows them.

Here are the things that are especially helpful in keeping your operation running smoothly. First, have a continuity plan. This is your backup plan for your operation when normal procedures get disrupted. Be able to re-route your mail on the fly. Understand the impact of shifting to an alternative mailstream flow. Most important, make sure your redundant capabilities really are redundant, so security standards aren't compromised just when you need them most — in the wake of a disruption.

Next, bring in as much containment capability as you can. This can be a substantial

upfront expense, but it will pay huge dividends in preventing a security breach from making an impact on business operations. Finally, use Six Sigma to identify the location of the best site for each step in the mailstream workflow. This ensures maximum efficiency for the entire process.

The mail center is a strategic point of defense for your company. Putting in place processes and procedures for more secure mail handling and distribution is inexpensive compared to the cost of having a real threat or a hoax shut down operations. The fact is, with intelligent planning and the right deployment of technology, you can achieve mailstream security without sacrificing your day-to-day effectiveness.

*Robert F. Hahn II, Ph.D., is Vice President, Strategic Development, Government Mailstream, Security and Document Solutions, at Pitney Bowes Management Services. For more information, please contact him via email [Robert.Hahn@pb.com](mailto:Robert.Hahn@pb.com). ●*