



On-Demand Thought Leadership For Homeland Defense & CyberSecurity Professionals

<http://www.homelanddefenseweek.com/Blogmain/TheListeningPost/Counterterrorism/040207.html>

The Need or Facility-Level Mail Screening

Why Government Agencies Remain At Risk for Mail Bound Threats and the Advanced Strategies That Can Help Protect

By Don Shanks

Special to Homeland Defense Week

April 2, 2007

This past January, the Palm Beach County Courthouse in Florida was evacuated after mailroom employees were exposed to the chemical tellurium, which spilled from a partially opened envelope. Although no one was seriously harmed, the event spread widespread fear.

Live media coverage of the building's evacuation and the massive decontamination of those exposed put the disruption of services and the anxiety experienced by facility personnel and visitors in the limelight. The event's impact was felt the following day, when the building was again evacuated in reaction to an unidentified powder found on a jury notice inside the courthouse.

This serves as a clear sign that – five years after the 2001 anthrax attacks – the majority of federal, state and local government facilities remain at risk. Ongoing efforts by government agencies, the USPS and private carriers to educate mail handling teams have improved the situation. However, many facilities, especially those with large high-volume mailrooms, remain at risk. Clearly, improvements are needed, but there are a lot of questions to consider in designing the best strategy.

Disruption or Best Friend? The Debate over Mail Screening

Unfortunately, there is a general reluctance to implement comprehensive facility-level screening programs. While the reasons vary from facility to facility, common concerns include the impact of comprehensive screening on delivery times, misconceptions regarding existing in-route screening procedures by the postal service or private

vendors, concerns over addressee/sender privacy and the potential impact on the mail handling budget.

Balancing the Risk

Developing mail-screening protocols that successfully meet security goals without significant impact on delivery times is considered very challenging. Mailroom facilities are set up to receive, sort and deliver mail, but few are designed to support aggressive screening techniques.

It is important to consider the scale of impact when assessing delivery delays. For instance, which has the potential to be more costly and disruptive: Implementing screening protocols that cause a brief delay in mail delivery, or not implementing a screening program and losing the entire facility for several months or years while it is being decontaminated? The answer is obvious – and while mail security programs are designed to cut down delivery delays, they clearly outweigh any office closures, massive disruptions of business and potential harm to employees.

Handling with Care – and Sensitivity

As screening protocols are developed, facility managers and mail room supervisors must address privacy concerns associated with the various procedures. There will be times when it becomes necessary to open suspect letters or parcels. The only way to mitigate this issue is through clearly defined, and agreed to, operational procedures. These will have two pathways:

- Emergent threats: normally identified by x-ray, chemical/biological sensor or physical attributes.
- Routine operations: normally triggered by an attribute such as being addressed to or from a specific individual, organization or location.

Under either circumstance, procedural safeguards must ensure the privacy concerns of the addressee (for example, having surveillance cameras in the screening area to monitor employees opening such mail) – and the safety of the facility and its occupants exceed individual privacy concerns.

Relying on Carriers for Safety?

There is a common misconception that the USPS and private carriers (such as FedEx or UPS) conduct comprehensive screening procedures as mail passes through their handling facilities.

While highly effective in delivering operational safeguards, their screening programs are not sufficient in the face of today's emerging biological and chemical threats – and only identify basic threats to handling facilities, resources and personnel.

Making it Worth the Investment

The cost-benefit analysis for facility mail screening is simple: Mail screening programs save lives and safeguard facilities. It may be years before a mailroom detects a valid threat, but it only takes one event to justify the expense. It's vital to factor in the costs associated with closing a federal building or courthouse, the costs of providing immediate and long-term care to hundreds of employees and visitors and costs of locating and funding temporary facilities during primary facility decontamination and refurbishment. These far exceed the financial investments of setting up and maintaining a quality-screening program.

Facility-Based Screening: The Next-Level for Risk Reduction

Chemical, biological and radiation detection equipment at mail handling facilities is designed to sample the overall environment versus individual letters or packages. To increase protection, many high-profile federal and state agencies are taking mail screening to the next level by establishing rigorous facility-based inspection processes.

These advanced steps require hard-nosed expertise. Developing minimal impact, cost-effective screening programs at the facility level can only be delivered by outside sources trained specifically this highly specialized work.

Bringing in consultants and contractors can help keep workflow on track by clearly identifying those organizations or individuals within the facility that are most vulnerable. Isolating the risk helps maintain overall workflow, while providing increased security. Additionally, mailroom workflow analysis will identify which screening elements – such as x-ray, chemical, radiation, and biological threat screening (closed or open envelope), hand sorting and hand screening, if necessary – will best serve the daily security needs of the facility.

These highly trained individuals know the threats and how strategies and execution are evolving. They can suggest the best procedural and technical approaches to protect workers and facilities at all times.

Another Layer of Protection: Educating Employees

Knowledge and awareness remain the most cost-effective tools in mail-screening. X-ray machines and chemical sensors cannot detect every threat. Educating mailroom employees on threat response procedures, and lessons learned from other national facilities is the starting point for all comprehensive-screening operations. Organizations must understand the risk profile for facilities and train for the worst-case scenario.

Guarding against chemical, biological, radiological and explosive threats continues to be a major challenge. An evaluation of threats and the potential impact clearly shows the need to develop and maintain an effective screening program.

About The Author

Don Shanks, Vice President of Engineering for SoBran Inc. can be reached at 703-352-1344; dshanks@sobran-inc.com