

**March: Biodefense // Guest column**

## **Understanding – and minimizing – today’s prevalent CBRNE threats**

**// by Matthew Sweatt**

27 March 2008

**Today’s response structures are too narrow in focus; while being prepared for a small pox attack is great, what would happen if another bio-toxin were used? Most billion-dollar detection equipment today only looks for anthrax, allowing today’s emerging threats easily to penetrate most systems**

To most eyes, today’s biochemical landscape appears as it has in the past. No new chemical or biological threats have been developed; just variations in the delivery methods of known threats. If one thinks the overall threat levels have subsided, however, they cannot be more wrong -- and are placing themselves in a very vulnerable position.

The scale of today’s threats is heavier than ever before. Many terror cells are actively seeking to purchase or develop CBRNE weaponry. Anthrax, smallpox, pneumonic plague, cholera, and botulism remain the most researched toxins by agencies, as they are the most developed, weaponized toxins known. The United States has issued orders for the manufacturing of nearly one-hundred million vaccinations for smallpox, and hopes to have enough to treat everyone in America if smallpox were to be used as a weapon.

We are making strides in understanding CBRNE risks, but as a nation we are far from proper preparedness. Even though the United States has begun stockpiling smallpox vaccines, and the U. S. Postal Service (USPS) has purchased billion-dollar detection equipment, an adequate preventive approach is still lacking. Today’s response structures are too narrow in focus. While being prepared for a small pox attack is great, what would happen if another bio-toxin were used? Most billion-dollar detection equipment today only looks for anthrax, allowing today’s emerging threats easily to penetrate most systems.

Many Americans falsely believe there has not been any terrorist activity since the anthrax attacks of 2001-2002. From ricin found in the White House mail in November 2003, to the multiple package bombings in the United Kingdom in 2007, mail-borne threats have continued to torment government and commercial organizations across the world.

In my experience, I have seen many real threats and hoaxes, yet everyone still has an “it won’t happen to me” attitude. When businesses are asked whether they believe they are at risk to mail- or parcel-borne contaminants, most believe they are not; and if they were, irradiation of mail entering their facilities eliminates all risk. Irradiation does not neutralize chemical, radiological, nuclear, and explosive threats; it is only helpful against biological threats.

Furthermore, most Americans believe that their mail is irradiated, but this is not accurate, either. Only certain zip codes are irradiated and no major commercial carriers routinely irradiate their mail stream. At last check, only 15-20 zip codes -- all associated with government agencies -- are being irradiated on a regular basis by the Postal Service. This means that with 20 zip codes out of approximately 48,000 zip codes in America, the USPS is irradiating only about 0.0004 percent of mail delivered annually.

The myths of irradiation killing all threats have made individuals complacent about their level of protection, and have put them at risk. The recent discovery of ricin in a Las Vegas motel room has proven the fact that dangerous threats still exist, and preparation must be made to protect government, corporate and civilian property and life.

### **Mail stream vulnerability**

The mail stream is extremely vulnerable to CBRNE attacks for many reasons. More than 500 billion pieces of mail are delivered annually in America between the USPS and commercial carriers. It is impossible for a facility to detect all types of threats that could exist. Furthermore, anybody can send individuals or their businesses mail anomalously.

Since 2001, more than 20,000 post office closings have been attributed to powder threats -- a number that does not take in account the plethora of business days, and costs, lost to similar threats.

Also, since 2004, more than 40,000 white powder hoaxes have been investigated, with the massive results often not fully recognized. Thousands of businesses were shut down, and many employees were left with heavy psychological damage. Owing to its frequency -- and scope -- it is impossible to calculate the lost revenue of businesses due to CBRNE hoax threats.

Just because people may not hear about things happening does not mean they are. Remember, 40,000 hoaxes are being investigated yet many more incidents are not reported. Most organizations do not report incidents; in fact, many do everything they can to ensure sure that information is not leaked, for fear of negative public perception or alarm.

I have done numerous CBRNE risk assessments. I have seen anthrax and ricin, and I have watched people take contaminated mail and walk it around a building. In speaking to companies, they always tell me that they are not adequately prepared. Mail stream vulnerability is not a new thing; mail was used as a weapon far before 2001, the Unabomber is an example that dates back to the late 1970s. Everyone always asks how to stop attacks from happening, and the answer is that you can not stop them from happening; you can only be prepared when they do. Is it even possible to search every piece of mail for every kind of contaminant?

The answer is a definitive no. Companies need to take a more proactive approach in the protection of their facilities. When accessing mail stream vulnerability, they also

have to consider the protection of their infrastructure as well as CBRNE threat defense. If the building itself is unsecured, there is no point in having a secure mail stream.

### **Protecting business operations**

Protecting any company's facilities and mail stream all starts with highly trained personnel. Having educated individuals aware of the dangers that may arise is far more valuable than any piece of equipment a company may utilize to mitigate risk. Other safe facility practices include:

- Continuous emergency response training
- Conducting infrastructure and risk assessments
- Developing emergency response plans
- Detailed standard operating procedures (SOP's)
- Preventing access to heating, ventilation and air conditioning (HVAC) intakes
- Attempting to isolate the HVAC on mail rooms with an emergency shut off
- Preventing public access to roof, stairways, and mechanical areas
- Utilizing surveillance equipment
- Key card access
- Simulating CBRNE events and response

Also, companies need to assess their own risk. Organizational characteristics commonly associated with high levels of vulnerability include the following:

- International firms
- Government related
- Frequently in the news
- Financial institutions
- Involved in something unpopular to some (animal testing, oil, military support)

### **Locking out threats: Effective mail room strategies**

The most important practice to secure the organization's mail is to combine a design and mail strategy with a proper training structure. This could include using automation solutions such as scanning; isolating mail streams from facilities; wearing special protective equipment; using modular containment, high efficient vacuums with charcoal and High-Efficiency Particulate Air (HEPA) filter; and initiating laboratory analysis.

Corporations and government facilities must assess the impact that a hoax threat or actual contaminant would have on their facility. It actually costs more to remediate a building after being contaminated by anthrax than it would be to level and rebuild the structure. It may be in the best interest of companies to have their mail processed off-site by professionals, as the cost of this work is inconsequential considering lost labor hours or remediation if contamination occurred. Other key practices which should be integral to any safe mail policy should include:

- CBRNE detection equipment

- o X-ray machines
- o Radiation detectors
- o Chemical/Biological sniffers
- Digitalization
- o Scanning and electronic delivery of mail
- o Photographs of unexpected packages
- Modular Containment
- o Isolation of mail flows
- o Easily decontaminated
- Emergency response planning
- Disaster recovery planning

Businesses today have a myriad of choices when it comes to mailroom, infrastructure, and personnel protection. It all depends on what a business feels is adequate, and what they are willing to spend. Yet in this time of escalating CBRNE awareness, businesses should be prepared if the unthinkable were to happen – and that starts with an effective mailroom strategy. As the old adage says; an ounce of prevention is worth a pound of cure.

*Matthew Sweatt is a CBRNE Engineering Executive and leads SoBran Incorporated's CBRNE Center of Excellence Manager; he is also the acting coordinator and architect of SoBran Incorporated's CBRNE Critical Infrastructure Protection (CIP) response*