Identity crisis

No mailborne anthrax attacks have been confirmed since 2001, yet there have been 20,000 suspicious powder-driven post office closures since then. Differentiating between a real threat and a hoax, and deploying the correct technology to deal with it, is paramount.

By Dr Robert Hahn, vice-president, Pitney Bowes Secure Mail Solutions, USA
"MOST IMPORTANT FACTOR IN MAILSTREAM SECURITY IS A WELL-TRAINED, EDUCATED MAIL HANDLING TEAM"

the US government. That elderly woman in Connecticut had no connection to any of the other victims, except that they all opened their mail—something virtually everyone does every day.

The anthrax issue has in some ways taken on a life of its own. There have been no reported cases of anthrax since November 2001, although there was a ricin incident that affected the US Senate in 2004. Yet there have been 20,000 suspicious powder-driven post office closures. The majority of these incidents have been hoaxes, while others were legitimate packages that had some kind of accidental leak or residue. One of the persistent myths about anthrax is that it is a powder that can be seen inside an envelope. "It needs to be thought of less as powder in an envelope and more like perfume in the air," explains Dr Douglas Quine, an anthrax expert with Pitney Bowes' advanced concepts and technology studio. "The spores fit very easily through the pores in a paper envelope. Once it's in a building, even if the powder is contained in a paper envelope, the building is contaminated," he adds.

To use an analogy, microscopic anthrax spores permeate the pores in a paper envelope as easily as people walk through New York City's Grand Central Station. The woman who died of anthrax poisoning in Oxford, CT was infected by mail that was never any closer than three envelopes away from one that contained the actual spores. The only way to be sure that mail is safe is to keep it quarantined in a containment system until it is tested.

Plastic is one way to contain anthrax. Pitney Bowes is developing a detection system that uses airtight plastic bags as the first line of defence. Bagging the mail is a safe approach for low-volume recipients of mail. If anthrax is detected inside the sealed bag, it is contained and can be disposed of properly. But for high-volume users, bagging the mail may not be practical. It may be easier to 'bag' the mail handlers instead. High-volume, high-risk mail recipients should consider investing in an offsite, self-contained, negative-pressure air room to keep the mail quarantined until proved safe.

In the USA, the responsibility for safeguarding more than 200 billion pieces of mail a year—and protecting 700,000-plus postal employees, about 38,000 postal facilities, 200,000-plus postal vehicles, postal assets and millions of postal customers—falls on the shoulders of US postal inspectors. Since the anthrax attacks, and in addition to the 2004 ricin scare, the inspectors have investigated more than 2,169 bomb threats and mail suspected of containing explosives. In 171 of these incidents, an actual hoax device simulating an explosive was found in the mail. Postal inspectors dedicated 46,285 workhours to such investigations, resulting in the prosecution of 151 suspects. The inspection service spent roughly US$5.2 million to conduct the investigations.

The real threat faced by most businesses is the lost worker productivity and downtime associated with these false alarms. How does one calculate the loss to a company if a 2,000-member employee campus is shut down for two to three days due to a false alarm? As with any other anti-terrorist activity, there is no silver bullet solution. A number of integrated approaches must be implemented. By having the right people and processes in place, these disruptions can be minimised.

The most important factor in mailstream security is a well-trained, educated mail handling team. Equipment alone cannot replace an aware, trained, mail centre staff; working in conjunction with security personnel, this is the best line of defence against an attack on a mail
centre. Being able to identify the sender of a particular mailpiece is an important safety consideration. None of the anthrax-tainted letters carried indicia from a postage meter, because the indicia are traceable and trackable to a specific device. Mail centre personnel should be aware of this and should be able to easily affirm that the mailpiece comes from a trusted source. Business leaders should conduct an audit of operational, safety and security requirements, and make sure that mail centre staff have coordinated processes, strategies and equipment appropriate to the level of risk.

In addition to employee training, the possible countermeasures that organisations can implement to improve mail centre security include relocating the incoming mail function to isolate it from other departments, automating the function to reduce the incidence of manual handling, and improving the screening of incoming mail and packages through the use of video, x-ray and even specially trained dogs.

Some firms at a higher level of perceived risk are implementing additional safety measures, which include the mandatory use of protective clothing and equipment for personnel, the creation of secure and self-contained workstations for opening mail, and the use of high-efficiency vacuums and air filtration systems. For example, in response to the 2001 attacks, which shut down the Congressional postal centre, the House of Representatives piloted a digital mail system that allows first-class mail to be scanned offsite and delivered to members in electronic form in order to reduce the House’s vulnerability through the mail. The Hill, a congressional magazine, reports that the programme began with 30 House offices in 2002 and was expected to expand to 75 offices by the end of November 2003, according to House Administration Committee Chairman Robert Ney (R-Ohio).

Keeping the physical mail offsite is an important part of this strategy. The cost of cleaning up an anthrax-contaminated facility is about the same as the cost of tearing down the facility and rebuilding it completely. Clean-up at the two USPS facilities that were infected in 2001 cost more than US$130 million and took two years. The cost of outsourcing mail screening to trained professionals for one year is less than the cost of a large business being shut down for two days due to an incident, real or otherwise.

In the unlikely event that actual biohazards are detected at an offsite mail facility, they are contained in a vacuum-sealed room that is far cheaper to clean than a whole building. The mail handlers inside are trained professionals who understand the procedures for remediation and know what steps to take to minimise the threat to themselves and the operation.

An array of products and technologies are available to help bolster mail centre security. These range from commonplace strategies such as metered mail and address management software to help verify the origin and authenticity of individual mailpieces, through to advanced technologies such as email alerts with attached digital images of unexpected packages or the remote opening and digital delivery of messages, and on to premium solutions, which can include extreme measures to isolate and contain potential biohazards, as well as the ongoing use of clearing or biohazard detection devices. Every product or technology related to mail centre security may not be appropriate for or needed by every organisation, and a solution must be tailored to fit individual needs. Every organisation needs to strike a balance and take sensible safety precautions. When mail-processing personnel use awareness, common sense, and effective, documented procedures, mail safety and security is possible.

These clippings are sampled from a two-day period in a random week in September 2005... and represent a fairly typical week to those who track these incidents. At the very least, educating executives, managers, mail handlers and the general public as to the myths and realities that have circulated since the anthrax attacks in 2001 will help boost security.

**Suspicious Mail Causes Panic and Evacuation on College Campus**

Bridgewater State College, MA – A suspicious package was delivered to the Administration Office of BSC Wednesday, causing an evacuation and panic throughout the afternoon. The package was partially open, wet, and emitting a foul smell when it was received by an employee. The employee also said a gas-like substance appeared to release from the 5x8 sized envelope. It was brought to the mailroom, and was immediately deemed a suspicious parcel.

(Campus News, 22/9/2005)

**Suspicious Powder Sent to Nevada Congressman’s Campaign Office**

Reno, NV – Work at Congressman Jim Gibbons’ campaign office in Reno was put on hold Monday after the discovery of a powdery substance. The incident happened just before 17:00 at the office on Arlington and Liberty Streets after workers discovered a letter containing an unknown powder.

The building was quickly evacuated while the HAZMAT team tested the powder. Fortunately, it turned out to be harmless.

(KRNV News, 22/9/2005)

**Canada Post Evacuated After Powder Found**

Ottawa – An Emergency Services squadron, including the Ottawa Police, responded to a call of a suspicious powder at the Canada Post office 1424 Caledon Place at 10:15 am on Friday. A mail worker on the second floor who was moving some bins dropped one, which released a white powder. The man began having trouble breathing and EMS crews were called while part of the building was evacuated. The man was treated by paramedics and is expected to be fine. HAZMAT crews took a sample of the substance and determined it to be talcum powder.

(Ottawa Citizen, 23/9/2005)