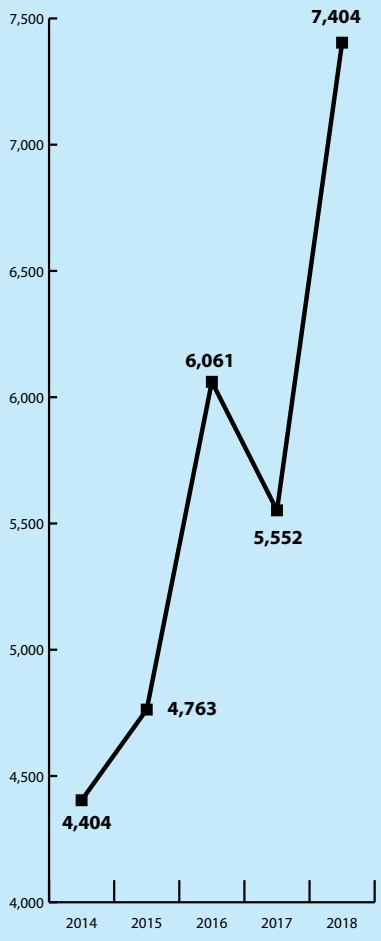
RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Why Mail Screening Must be an Integrated Part of Comprehensive Executive Protection Programs

BY CHRISTIAN WEST AND MARTIN NIELSEN
AS SOLUTION

SUSPICIOUS / UNATTENDED PACKAGE TRENDS



Graph from US Bomb Data Center Explosive Incidents Report 2018

Mail threats and vulnerabilities increasingly matter to executive protection professionals. At AS Solution we believe that we can now mitigate these risks for organizations and family residences with the help of new screening technology.

MAIL THREATS MATTER

Mail-borne threats, especially those due to explosives and biological and chemical agents, are real, deadly, and on the rise.

In 2018 alone the U.S. Bomb Data Center documented no fewer than 600 explosions related to parcels and letters. A quarter of these were directed at residential targets and resulted in 17 deaths and 64 hospitalizations.

In addition to lethal improvised explosive devices (IEDs) and incendiary devices, mail threats containing dangerous biological and chemical compounds are also increasing – as are white powder hoaxes.

Whether real or hoax, intended to do bodily harm, disrupt business, intimidate, or blackmail, mail threats are relatively easy to execute and difficult to trace back to the perpetrators. Given their potential impact and the widespread vulnerabilities of most organizations and families, we believe that mail screening will play an increasingly vital role in comprehensive executive protection (EP) programs in particular and in corporate security in general.

OF THE FIVE TYPES OF MAIL THREATS, TWO ARE MOST RELEVANT FOR EXECUTIVE PROTECTION

Government agencies such as the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) U.S. Bomb Data Center categorize mail threats into five types: chemical, biological, radiological, nuclear, and explosive – commonly referred to as “CBRNE”. While all threats must of course be considered, this piece will focus primarily on biological and explosives threats, as these are the most common and likely to occur in the settings in which we, as EP professionals, work.

As mentioned above, explosives in mail are disturbingly common, with about **1.6 occurring every day** in the U.S. alone on average. Many of these are pipe bombs – relatively simple to make but deadly. Explosives are easier to detect visually than powders due to their density and appearance.

Two of the most well-known biological threats are anthrax and ricin. Both are extremely toxic substances that are lethal in even minute quantities when inhaled in powder form (anthrax) or ingested or injected into the body (ricin and anthrax). Anthrax spores in powder form sent in anonymous letters killed five persons in 2001, injured 17, and revealed just how vulnerable we are to this deadly threat. Ricin-laced letters have been sent to Presidents Obama and Trump and other officials – and just recently to California prisons. Although anthrax and ricin are not simple to make in their concentrated, pure forms that are deadly, skilled chemists with the proper means and motivation can do it. A wide range of copycat hoaxes show how easy it is to wreak havoc, close offices, and create an environment of fear by sending innocuous white powders (baby powder, soap powder, sugar, flour…) to businesses, media outlets and residences.

Powders can be difficult to detect visually using conventional technologies. They are small in size and can be confused with the large amounts of dust common in mail centers.

ALL PHYSICAL MAIL STREAMS ARE VULNERABLE TO MAIL THREATS

Although electronic mail continues to chip away at the number of snail-mail letters we send each other, postal carriers and couriers deliver an ever-increasing volume of goods we purchase online.

By 2021, worldwide ecommerce sales are expected to reach almost $5 trillion, or 17.5% of all retail sales. That's a lot of parcels and small packages moving around, and the trend is only expected to continue upwards.

While convenient for consumers and companies, the huge flow of post and package deliveries to homes and businesses represent a growing security vulnerability. Because anyone can send mail via these streams anonymously, the risk of detection is low for those who wish to do harm. Furthermore, carriers do only very limited screening in these streams. According to the U.S. Bomb Data Center, incidents regarding explosives in packages and parcels increased 99% from 2017 to 2018. Furthermore, the rise in outsourced "last mile" delivery introduces even greater vulnerabilities in the chain of custody. It is now common for parcels to arrive in unmarked cars and vans dropped at the front door or reception by private individuals.

Interoffice or intra-campus mail are often-overlooked vulnerabilities. Even though the organization might do some kind of screening "at the gates", once inside, such screening is rare. Envelopes and packages are often transported internally in open containers, making it easy for malicious visitors or disgruntled employees to end-run most mailroom screening procedures and introduce mail threats directly into the internal delivery stream.

UNDERSTANDING THE RISKS DUE TO BIOLOGICAL AND EXPLOSIVES IN MAIL AND PARCELS

Bodily harm is obviously the most serious risk due to mail-borne biologicals and explosives, but these threats expose organizations to other types of risk – and potential costs – as well:

- Financial costs: Companies incur significant expenses when forced to deal with mail threats, often closing the affected facilities for days while investigations take place and even longer if remediation is necessary.
- Psychological costs: Organizational morale and productivity suffer when staff doubt the organization's ability to protect them and are worried about their safety at work.
- Reputational costs: The negative PR resulting from mail attacks can impact sales and the company's capacity to attract and retain the best employees.

The psychological and reputational costs are real, albeit difficult to calculate. The financial costs due to facility evacuations and closures, however, are more straightforward. Depending on the circumstances, expenses related to such shutdowns can far outweigh the costs of mail screening.

THE LOCATION OF MAIL SCREENING FACILITIES MATTERS

As we outline above, the bad news is that mail threats are deadly and on the rise, putting both organizations and families at risk. The good news is that mail threats are possible to mitigate with mail screening.

For both organizations and residences, the location of mail screening facilities matters. Here is how some of the options compare, in descending order of security:

- **Off-site screening –** In high-risk situations, it's best to do mail screening (and screen all deliveries, including those for canteens, office supplies, etc.) offsite in dedicated, isolated facilities.

- **Isolated on-campus or on-residence screening –** This option is not as secure as off-site screening, but it is in most cases better than those described below. These screening facilities are located within the security perimeter but separate from other buildings. Importantly, their HVAC systems are also separate in order to keep any air-borne threats isolated and away from the rest of the organization or residence.
- **Non-isolated on-campus or on-residence screening –** Such facilities are attached to a building, preferably with direct access from outside so unchecked mail doesn't have to be transported through working or living spaces. Ideally, internal transportation of mail should take place under negative pressure to contain any contaminants; there should be separate HVAC which should be able to be shut down quickly if necessary; and walls between the mail screening facility and the rest of the building should be hardened to withstand explosives.

We do not have any statistics, but we suspect that with the exception of government offices and major corporations, most companies and private residences do not have any special location for mail screening. And as we shall see below, nor do they have any appropriate technology, procedures, or trained personnel.

MAIL SCREENING TECHNOLOGY AND EXECUTIVE PROTECTION

A wide variety of technologies mitigate mail threats. All have their advantages and disadvantages regarding substance detection, operator safety, operator training, throughput, complexity, and cost.

Visual inspection, for example, can detect the most common mail threats effectively if slowly, but depends on a human operator to open and examine every individual parcel or piece of mail, directly exposing him or her to threats from all types of substances.

At the other end of the complexity spectrum are high-throughput automated systems utilizing various different types of sensors and identification technologies to detect or identify a wide range of CBRNE threats. While complex and costly, these systems make sense for corporate campuses and government facilities with significant risk profiles and large delivery volumes.

Until recently, executive protection programs, not least at the residential level, have lacked technology suitable for mail screening. Automated sensor systems that protect principals at the office rarely do so at home. X-ray scanners have been used in some residential security programs, and while they are good for spotting explosives, they are ineffective in detecting other substances, such as powders and liquids. It's an unfortunate fact that visual inspections, with all their risks for the household staff, executive protection agents, or principals opening the mail, have probably been the most common "technology" used for mail screening in residential contexts.

Fortunately, this situation has recently changed. New millimeter wave technology, or mmWave, using ultra-short wavelengths and operating in the spectrum between 30 and 600 GHz, coupled with new imaging systems and software, are now capable of detecting the most common mail threats including chemical, biological, explosive and suspicious powders. The leading systems also contain an integrated radiation detector, providing capabilities image or detect most types of CBRNE threats. We have tested the solution developed by RaySecur, for example, and found it suitable for residential programs as well as organizations that want better mail security, but are not ready to invest in high-volume automated sensor solutions.

Threat Detection:

SUBSTANCE	MMWAVE TECHNOLOGY	VISUAL INSPECTION	AUTOMATED SENSOR SYSTEMS	K9 TEAMS	X-RAY SCANNERS
CHEMICAL	X	X	X		
BIOLOGICAL	X	X	X		
RADIOLOGICAL	X		X		
NUCLEAR			X		
EXPLOSIVES	X	X	X	X	X
SUSPICIOUS POWDERS	X	X			

THE NEED FOR SOLID PROCEDURES AND WELL-TRAINED STAFF

- Of course, technology on its own is not enough. Executive protection teams need reliable people and procedures, too, in order to carry out mail screening effectively and safely.
- In addition to determining the best possible location and isolation of the mail screening facility, as we discussed above, executive protection managers also need to establish standard operating procedures regarding:
- Training of staff
- Personal protection equipment for staff
- Incident response procedures – what to do if you find something (you don't want to run through the residence or office carrying a suspicious package, exposing more to the threat).
- Evacuation plans
- Internal and external communications

WE BELIEVE MORE CLIENTS WILL SOON INCLUDE MAIL SCANNING AS PART OF COMPREHENSIVE EXECUTIVE PROTECTION PROGRAMS

Given the increasing incidence of mail threats coupled with increasing vulnerabilities to the mail and package distribution system and the latest mitigation technologies, we believe more clients will soon include mail scanning as part of comprehensive executive protection programs.

The security and peace of mind benefits are high, and the incremental costs of adding effective screening to new or existing protective programs are low. That's why we are now offering mail scanning as standard in new SOWs and talking to existing clients about adding this important component to their programs.

THIS FIRST APPEARED AS A BLOG POST ON THE ASSOLUTION.COM SITE ON SEPTEMBER 2, 2019.

Christian West
Founder and CEO
of AS Solution.

Martin Nielsen
Executive Protection
Operations & Executive Projects
Director of AS Solution.

AS SOLUTION™
An Allied Universal® Company

WWW.ASSOLUTION.COM

RAYSECUR™
SAFE ACCESSIBLE DETECTION

www.raysecur.com | 617-855-9938 | info@raysecur.com