As security officials struggle to protect their facilities from mail-borne terrorist threats, Jason Wakefield discusses the screening options available and argues now is the time to upgrade your antiquated X-ray system

YOU'VE GOT– DEADLY– MAIL

Before purchasing equipment that can detect suspect devices entering a building through the postal system, there are many variables that need to be taken into account. An X-ray machine is a step in the right direction, but this will not solve your problems overnight. Such devices merely form part of a number of security measures that need to be undertaken to give protection to the facility and the personnel employed within.

Firstly, the recommendation is that a thorough post room threat assessment is carried out. This will give you a better understanding of what is needed and why. A post room threat assessment should provide an understanding of the current processes and assess the equipment that is already in place to specifically combat any potential postal threats to your location. An understanding of what the current postal threats are and how they are delivered will help. The current threat can be in the form of chemical or biological agents in powder or liquid form, as well as explosives and items designed to inflict physical and psychological harm. The threat assessment should be carried out by a professional security person. The threat assessment should start at the point of entry where the post enters the building; this can include multiple locations, such as Royal Mail and courier deliveries into a loading bay, as well as items hand delivered through reception. If possible, all deliveries should be placed into one specified area.

The post room needs to be located as close as possible to the post delivery point. An assessment should be made to identify any services such as computer servers, electric, water, gas utilities and key personnel within your organisation within a potential blast area, so that any detonation would have minimal effect to the business and the area affected can be closed off with ease.

Threat information is forever changing, and a relationship with your local counter terrorist security advisor (CTSA) would be advisable to get the latest threat information. An overview of groups that may target your establishment should be identified, along with reasons why they would target your organisation; you should not rule out the lone activist, disgruntled employees or customers with a grudge.

©Getty Images

This writer recommends checking the MI5 website once a week to keep up to date with all current threats and to follow the countrywide alert status. Keeping a dossier on all recent mail attacks with current trends and methods used would also make a fantastic staff training tool.

A decision to scan mail onsite or offsite needs to be made early on in the decision making process, and there are pros and cons to both. Offsite scanning is an ideal option, because any risk to your building through mail delivery is alleviated as all the scanning is done at another location. The offsite location will ideally need to be at an undisclosed location to keep it as anonymous as possible. Some things to remember when setting up offsite scanning include: there will be a delay in receiving mail; greater expense will be incurred, as you need to pay for premises and a secure delivery vehicle to take the mail between the two locations; an X-ray machine will be required at the onsite location to screen hand delivered items.

Onsite screening is by far the most popular and cost effective alternative. The downside to onsite scanning is that, if a suspect package is identified, you run the risk of loss of business due to a possible evacuation; if a device was to detonate, the disruption would be on a larger scale than an explosion at the offsite location.

There are various different types of X-ray machine available, and from a variety of manufacturers, but essentially we can break these machines down to cabinets and conveyors. A conveyor machine is similar to what you see at any airport to scan your hand luggage. It is an effective scanner for when your flow of mail is constant and you have an amount of large packages entering your business.

The conveyors have some additional optional software options. Advanced detection software (ADS), for example, is an advanced algorithm software that works by identifying the atomic number in explosive substances and contraband. This then highlights to the operator explosives within a red box and contraband within a yellow box, thus making it easier for the X-ray machine user to identify potentially dangerous or banned substances. Similarly, threat image projection (TIP) software allows the automatic projection of a simulated, pre-defined banned item (such as a gun, knife, bomb, etc) into a real scanned item. The operator would need to hit the suspect button on the keyboard when a suspect item has been identified; this will then go towards the operator's TIP score. If after hitting the suspect button there is no TIP confirmation, the image on the screen is genuine. Reports on the X-ray machine operator's effectiveness can be generated for management use.

Cabinet X-ray scanners are the most popular machines for post room use, and are in use in embassies across the world. Cabinet X-ray scanners take up around the third of the footprint and cost up to 50 per cent less than a conveyor. Cabinet scanners are also extremely effective and easy to use. These are operated by opening the chamber door, placing the items to be scanned inside, and then using a push button operation to generate an image. Once the image has been generated you have operating software with advanced features to make the identification of suspect items easier. These advanced features include enhanced powder detection (EPD) to increase the chances of identifying powders such as anthrax or Ricin, as well as e-mail capability which allows users to send pictures of suspect packages to a third party for assessment. There is also zoom control, density alerts and three-point colour, which have all been designed to help the user identify what is inside the package they are scanning. If your organisation currently owns an X-ray machine that is more than eight years old, the chances are that this machine is not fit for purpose, obsolete and inadequate for dealing with the types of suspect devices that are currently being identified.

Training on the use of the X-ray machine and its enhancement tools should be completed upon the purchase of the machine, and refresher training is required every two years. It is also recommended that all operators attend an endorsed suspect package training course to give them further knowledge on the types of devices that can come through the postal system and what these look like under X-ray conditions. The training should also cover the types of devices that have been

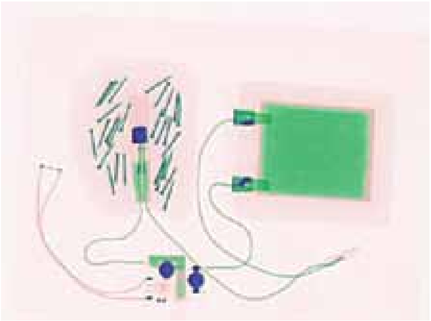
If your organisation owns an X-ray machine more than eight years old, the chances are it is not fit for purpose, obsolete and inadequate"

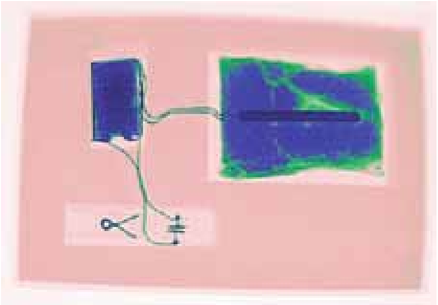
found in the postal system and the main components that go into these.

Full procedures, with procedures to be followed upon finding suspect devices, need to written, practiced and updated on a regular basis so operators and security staff are comfortable with what to do if a suspect device is found. There should be a separate action plan for the discovery of powder, which includes a decontamination plan in order to stop the spread of a potentially lethal powder. These procedures need to cover full escalation plans as well as safe routes and evacuation plans. All staff should know the action plans, so during sickness and holiday everyone will know the well-rehearsed procedures.

A senior person will need to take down the following vital information to hand over to the authorities: 1. What is it? 2. Where is it? 3. What does it look like? (Possibly a picture saved onto memory stick) 4. Who found it? 5. What time it was found? 6. Identify a safe route into the suspect package area.

Explosive devices and other suspect packages are found more often than most people think, and it is very easy to become complacent about the daily operation of the X-ray scanner and the training people get when using it. The scanner and its operators are the first line of defence against postal devices, and it is therefore imperative that the X-ray machine is able to see powders, fine wires and biological agents, and that the operators you have function as a highly trained team.





The use of cabinet-based X-ray systems to detect mail-borne threats must be combined with appropriate procedures should a positive result be returned

©Todd Research

Jason Wakefield is a threat assessment manager at Todd Research. He served with the British Army for more than ten years, during which time he gained extensive knowledge of IEDs and their components. Since leaving the army he has worked across the private security industry. His current role includes post room threat assessments for embassies, government and commercial customers.