SafeMail®

EASY TO MAKE
AND HARD TO SPOT

"Mail threats are so common today they don't make the news unless they reach a high-profile target. If you wait to screen until mail terrorism threatens your company, it's too late."

Amos-Leon' Otis, SoBran Founder and CEO

Mail terrorism has experienced an uptick in high profile incidents this year.

In Texas, a serial bomber used the mail to send package bombs. President Donald Trump's family received letters filled with white powder. In the United Kingdom, Prince Harry and his then fiancée Megan Markle were victims of an anthrax scare.

Most mail threats, however, aren't reported and don't appear in the media. Our research indicates that at least **one in four organizations has been the recipient of a mail threat** this year alone.

If you are associated with controversial issues or experienced recent layoffs, your risk of an attack is elevated. It's important to remember, however, that mail threats can occur at any time, for any type of organization. They may include dangerous substances or explosives or they may simply be designed to frighten an organization. Even a hoax threat can shut down operations for hours if not days or more.

"*Homemade bombs are easy to make and hard to trace.*"

Wall Street Journal

To assess how organizations are protecting themselves from mail terrorism, SoBran, Inc. conducts an annual survey of security and mailroom professionals responsible for the safety and security of their organization. In this year's survey approximately 40% of respondents work in government or as contractors and consultants to government agencies and the rest in private industry.

Most organizations don't take adequate security precautions

Approximately half (56.5%) of survey respondents report that the organization they work for screens at least some of the mail they receive. A much smaller number—35%—say all mail is actively screened on a consistent basis.

Those companies that do screen typically only conduct visual inspection (69%) and X-ray screening (60%). If a letter or package shows obvious signs of a mail threat, such as leakage, protruding wires, or unusual weight, smells or sounds, it may be caught with this type of light screening. X-rays may flag bombs, sharp objects or other high density materials such as metals found in IEDs (Improvised Explosive Devices) or PIES (Power Source, Initiator, Explosives and Switches) that can be used to make a bomb.
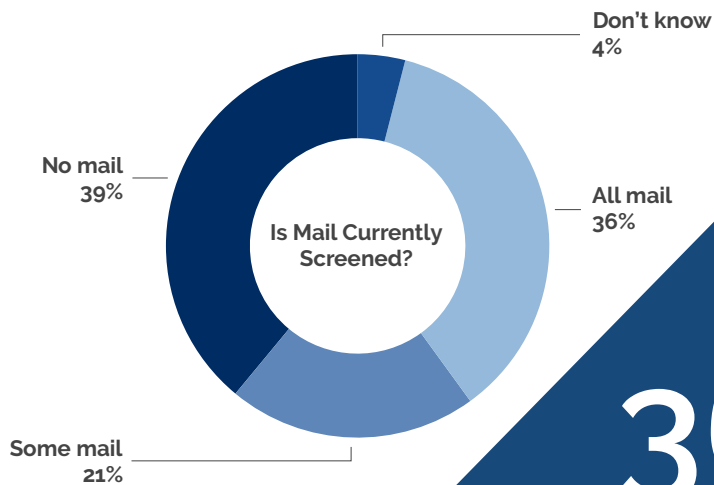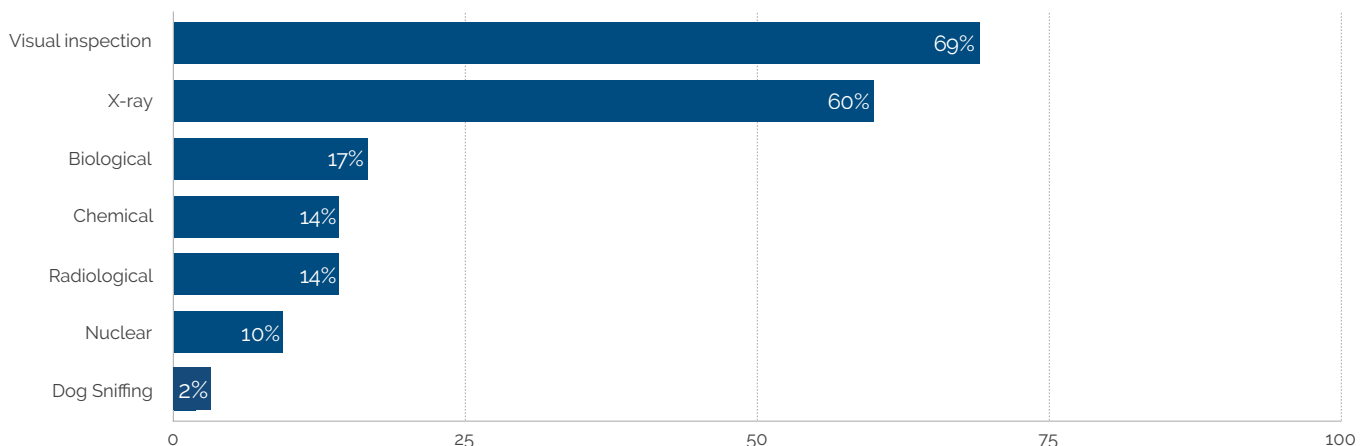
Unfortunately, limiting screening to visual inspection or X-ray leaves organizations vulnerable to the most dangerous type of mail threats, including chemical, biological, nuclear or radiological threats.

A much smaller group of respondents uses more specialized screening techniques such as biological screening (16.7%), chemical screening (14.3%), radiological detection (14.3%), nuclear detection (9.5%) and dog sniffing (2.4%).

Exposing employees to harm

The majority of survey respondents (62%) say they handle mail screening on their own, using internal staff rather than third parties. Sixty percent (60%) screen on their business premises in the same location where general employees work, rather than in an isolated location, safely removed from daily business operations.

Is Mail Currently Screened?

- Don't know 4%
- No mail 39%
- All mail 36%
- Some mail 21%

36%

of all respondents say all mail is screened on a consistent basis.

How do you screen your mail?

Visual inspection	69%
X-ray	60%
Biological	17%
Chemical	14%
Radiological	14%
Nuclear	10%
Dog Sniffing	2%

(0   25   50   75   100)

"The ease and relative anonymity of sending and the specificity of receiving have been exploited to turn the postal service into a vector for violence."

The Atlantic Magazine

64%

are not very confident in screening techniques

Lack of confidence

Virtually all respondents say they are at least as concerned about mail security as they were a year ago. One third (33%) are more concerned than they were this time last year.

Despite the concern, the majority (64%) are not very confident that their current screening techniques will detect dangerous biological or chemical threats.

Only 11% of respondents say they have taken action to increase their level of mail security in the past year while the vast majority (75%) have kept the level of screening the same in the past year.

Challenges to effective security

According to the mail security professionals, a number of challenges stand in the way of improving or simply maintaining mail security strategies.

Many challenges reported by survey respondents point to the importance of gaining management support for mail screening programs. Without support it is difficult for mail screening professionals to procure budget for their programs that is needed to purchase sophisticated equipment and hire or train expert staff.
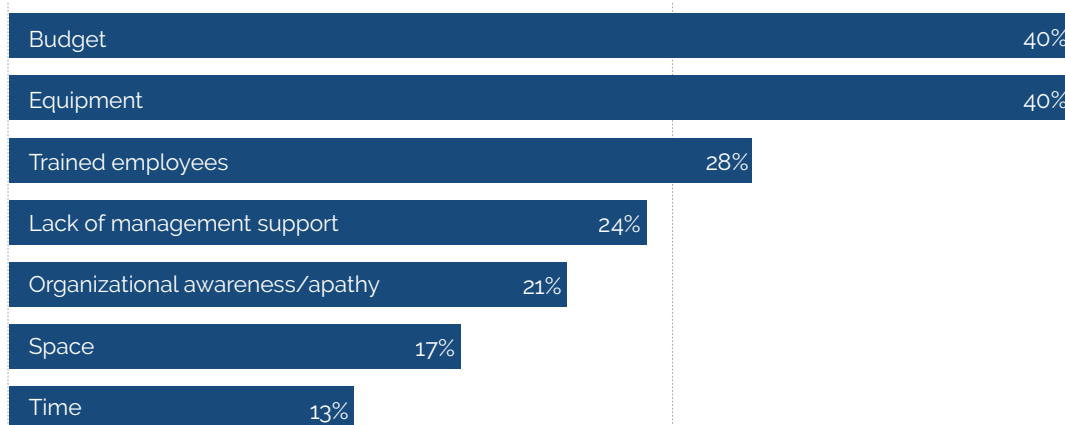
How can you protect your workforce?

The primary investment respondents plan to make is an increase in training. Over half (55%) are planning to increase training efforts.

What challenges do you face to improving mail security?

Challenge	Percentage
Budget	40%
Equipment	40%
Trained employees	28%
Lack of management support	24%
Organizational awareness/apathy	21%
Space	17%
Time	13%

If your organization is handling mail screening internally, particularly on premises, it is critical to increase the knowledge of mailroom staff as well as anyone who handles incoming mail. While general employees can be trained to visually screen the mail, a smaller group of employees should receive specialized training on equipment for advanced screening so they can prevent the most dangerous threats from entering your organization. Keep in mind, training is not a 'once and done' activity as new employees enter the organization and risk factors change. It is essential to continually train staff on the latest threats and screening techniques.

Moving screening offsite is the most effective way to keep employees safe

In the coming year, seven percent (7%) of respondents are planning to move mail screening offsite, either by working with a third-party mail screening service provider or by separating screening activities from general employees.

Offsite screening is the most effective way to mitigate risk.

- It reduces exposure to employees, decreasing health concerns as well as psychological issues from real or hoax threats.

- Operations are not disrupted by a hoax or real threat, so organizations can maintain operations and customer expectations.

- Cleanup of any hazardous materials is contained in a purpose-built environment.

- Any detected threats are not closely associated with the organization, reducing negative publicity.

⅓

are more concerned than they were this time last year.

Conclusion

Every day, threatening letters and parcels land at corporate and government offices. Most are inconvenient. Some cause damage. A few change everything. As long as terrorists have low cost and easy access to mail, all organizations must consider comprehensive mail screening an essential part of a security program.

SoBran SafeMail keeps your team safe and your operations running.

SoBran sets the standard for the design and operation of mail screening programs. We've been keeping clients safe from mail borne attacks since 2001, when we worked with the U.S. Army to develop and operate a facility to protect against Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) mail threats.

Our expert team provides you with:

Onsite Screening Services

The SoBran team provides technical and operational support for mail screening facilities. We work from your location to perform visual screens, operate all screening equipment, and keep your mail operations running smoothly.

Offsite Screening Services

You don't have to allocate space or expose your team to potential threats. We pick up your mail, screen it at one of our offsite facilities, and deliver it promptly to your door. You'll receive your mail fully screened – on your timeline, regardless of your location.

Additional Services

- On-site risk analysis, system design, integration and implementation for mail screening programs
- Design of site-specific protocols for crisis communications, evacuation, and emergency action plans
- Compliance with 41 CFR, Department of Defense and OSHA safety programs

SafeMail®