WHAT THE MOST PREPARED ORGANIZATIONS KNOW

A MAIL SECURITY BRIEF

Compare Mail Security In Your Organization To Industry Benchmarks

Most companies hold their security operations close to the vest, which can make it difficult to know how your own organization stacks up.

This Brief shares the results of a survey conducted by the SafeMail® team at SoBran that uncovers how organizations view the potential for mail terrorism and how they structure their mail security operations to minimize risk. Organizations are now able to see how their own security concerns and operations compare to industry averages and best practices.

By learning how other security teams combat the threat of mail terrorism, you'll be better equipped to implement effective strategies in your own organization.

What Makes This Survey So Important?

Mail terror is real

The FBI and US Postal Service receive thousands of dangerous mail reports every year, with no sign of a decline.

Forty percent of respondents to SafeMail's survey confirmed they had received at least one harmful or threatening piece of mail at their business within the last year. Twenty-five percent of those had received six or more threats.

Terrorism activity fuels concerns about mail safety

The SafeMail survey reveals that 56% of organizations are as worried about mail terrorism as they were in the previous year, and 43% are more concerned.

Seventy-six percent of respondents say they are aware that terrorists groups like ISIS are working on chemical and biological weapons, with 75% saying they are only somewhat confident or not at all confident that chemical and biological threats would be detected successfully at their own organizations.

All businesses, regardless of their previous experience, face an uncertain future.

Factions in the Middle East have publicly stated their intention to attack American interests at home and ISIS-related cases have been opened in all 50 U.S. states, At least one ISIS publication has referred to mail terrorism as a potential method to cause harm.

Law enforcement has 900 active cases involving homegrown extremists. These types of extremists, from the Unabomber to the Anthrax attacker, have used the mail as a vehicle for terror for decades.

40%

of respondents to SafeMail's survey received at least one harmful or threatening piece of mail at their business within the last year.

Most organizations are underprepared

Despite the evidence of mail terrorism and rising concerns over the past year, only 22% of organizations surveyed have improved their mail screening procedures in that time, and only 15% have chemical or biological screening capabilities.

There is a great deal of room for improvement.

Like an insurance policy, mail screening protects against potentially very high costs. Even a hoax attack disrupts business continuity. Shutting down a business for hours or days limits productivity, reduces customer satisfaction and impacts employee morale.

Estimate that a 1,000 person facility is evacuated for four hours while a hazmat crew investigate a mail threat. That can result in:

- Loss of $100,000 or more in productive time
- Disruption to customers
- Negative publicity
- Increased employee stress and absenteeism

The SafeMail team's goal is to help organizations prepare for the worst. We hope that sharing the results of this study will start a conversation within organizations about risk management and mail screening best practices.

32%

of respondents have their mail screened in a separate building from where most general employees work.

How Do Organizations Conduct Mail Screening?

Onsite versus offsite screening

Thirty-two percent of respondents have their mail screened in a separate building from where most general employees work. Thirty-eight percent screen their mail in the same building as most employees.

Most alarming, about 20% say that their mail is not screened at all.

What the most prepared organizations know

" Offsite screening," in which mail is screened in a separate location from where most employees work, is the most effective way to minimize potential harm.

- 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.

Should you consider offsite screening?

Ask yourself the following:

1. Does the mailroom share a ventilation system with other departments, such as accounting, support or sales?
2. Is your mail screening area shared with another organization? Is it in a building with multiple tenants?
3. Does your organization lack the specialty equipment needed to detect chemical, biological and radiological threats?
4. If you purchase specialty equipment, will space for the additional staff and equipment be a challenge?
5. Does your staff have limited time to keep up on the latest threats, training and cutting-edge equipment?

If you answered "yes" to two or more of these questions, offsite mail screening is likely the best option to keep your facilities operating and your employees safe.

If offsite screening is not an option, consider consulting an expert on the proper design and equipment needed to maximize detection while minimizing impact outside your mailroom.

What type of screening procedures do organizations use?

Although organizations are concerned about the potential for an attack, most organizations are not implementing comprehensive screening strategies.

Over 80% of respondents include visual inspection in their mail screening process. Just over 50% use X-ray. While these methods can help detect wires and metal weapons, visual screening and X-ray detection do not detect chemical, biological, radiological, nuclear or environmental (CBRNE) threats.

Less than 16% of respondents use dog sniffing or other techniques for biological, chemical, radiological or nuclear detection screening.

There are misconceptions that keep organizations from implementing advanced screening:

- They are not aware that the mail can be used to deliver these threats
- They believe their organization will not be a target for terrorism.
- They assume that the Post Office or other delivery service screens for CBRNE threats
- They believe they do not have budget for more comprehensive screening

These misconceptions may be putting employees and operations in harm's way.

What the most prepared organizations know

As discussed, thousands of mail threats are reported every year and 40% of organizations surveyed by SafeMail have received threats or hoaxes themselves. Organizations that receive mail threats range from government organizations to associations, and across all types of industries. Organizations can be targeted randomly, by a customer with a service complaint, a disgruntled employee or a member of the public opposing their values.

In addition, the anthrax incidents showed that certain chemicals or biologicals can contaminate other mail during the delivery process. That means that even if a different organization is targeted, any organization that shares a Post Office or mailroom can also suffer.

Unfortunately, while U.S. Post Offices provide X-ray screening, they do not screen every item, and do not offer comprehensive mail screening for CBRNE threats.

almost

60%

of respondents to SafeMail's survey believe training to be the most important way to help mailroom staff respond to a terrorist threat.

CBRNE screening does require specialized equipment and personnel training. However, if budget or personnel are limited, offsite screening is an affordable option for most organizations. Most importantly, it is much less expensive than the cost of remediating damage caused by a mail threat.

How do organizations stay prepared?

Almost 60% of respondents in the SafeMail survey said they believe "Training" to be the most important way an organization could help its mailroom staff respond to a terrorist threat.

What the most prepared organizations know

Organizations can increase the knowledge of mailroom staff as well as anyone who handles incoming mail with a variety of training strategies.

1. Research indicates "learning by doing" achieves a 75% retention rate. Threat simulations, in which staff practice screening as well as response activities, can help organizations prepare for the real thing.
2. Ensuring a documented plan is in place to detect and respond to a threat will help employees know the process. The documents can be required reading for new hires awaiting hand-on training.
3. Distributing posters or fliers that describe how to identify suspicious packages increases awareness for all employees.
4. Posting emergency numbers such as the fire department, the Center for Disease Control and the building manager near phones throughout the mailroom ensures the numbers are on hand when there is an emergency. Also, they serve as a daily reminder that a threat could occur and that the team needs to be vigilant.

Conclusion

As concerns of terrorism are on the rise, mail security strategies should rise accordingly.

Yet, as this survey reveals, while many organizations are taking appropriate steps to lower their risk, the number of organizations that have inadequate protection against mail threats is disturbing.

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.

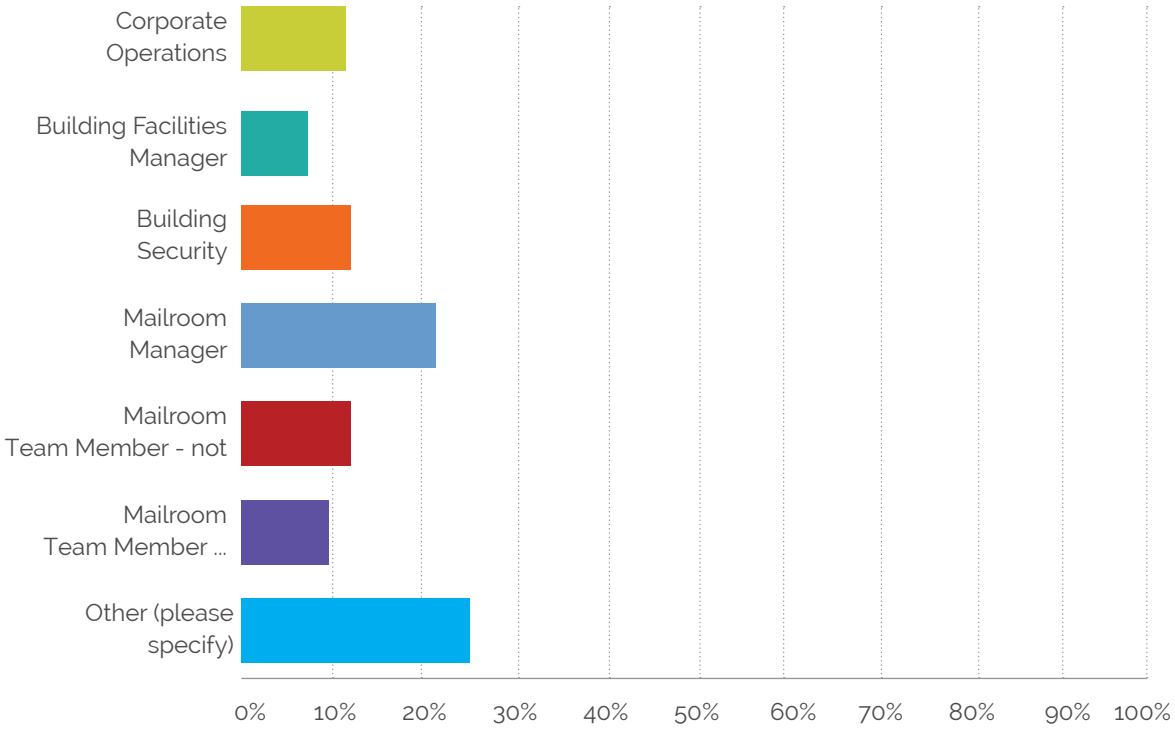
About the SafeMail Survey

The survey was conducted online between December 14, 2015 and February 8, 2016.

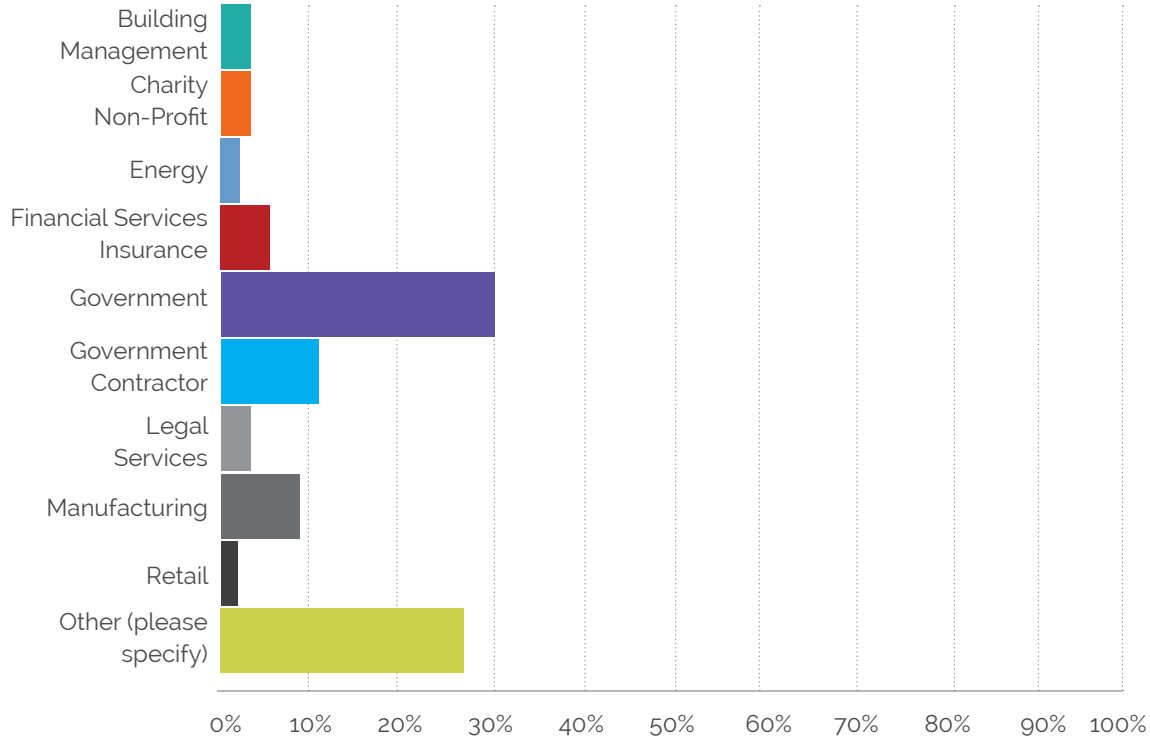
Broad Range of Respondents

Respondents to the survey included 92 members of the mail community. Mailroom managers and non-managers, transportation supervisors and building managers completed the survey. Government organizations were well represented, along with manufacturing, financial services, IT, legal and law enforcement.

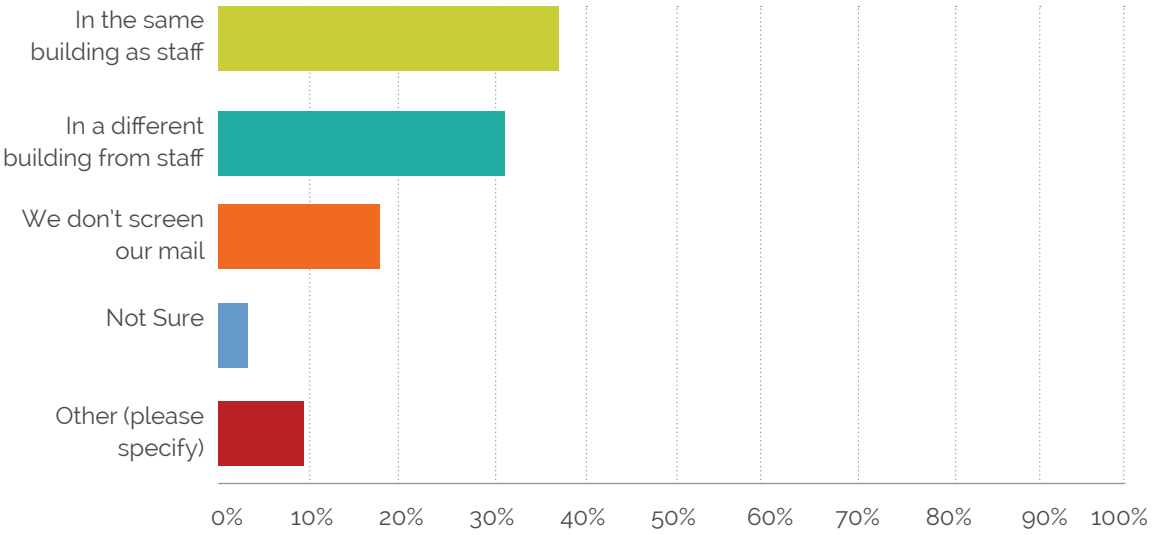
Which best describes your primary role in your organization?



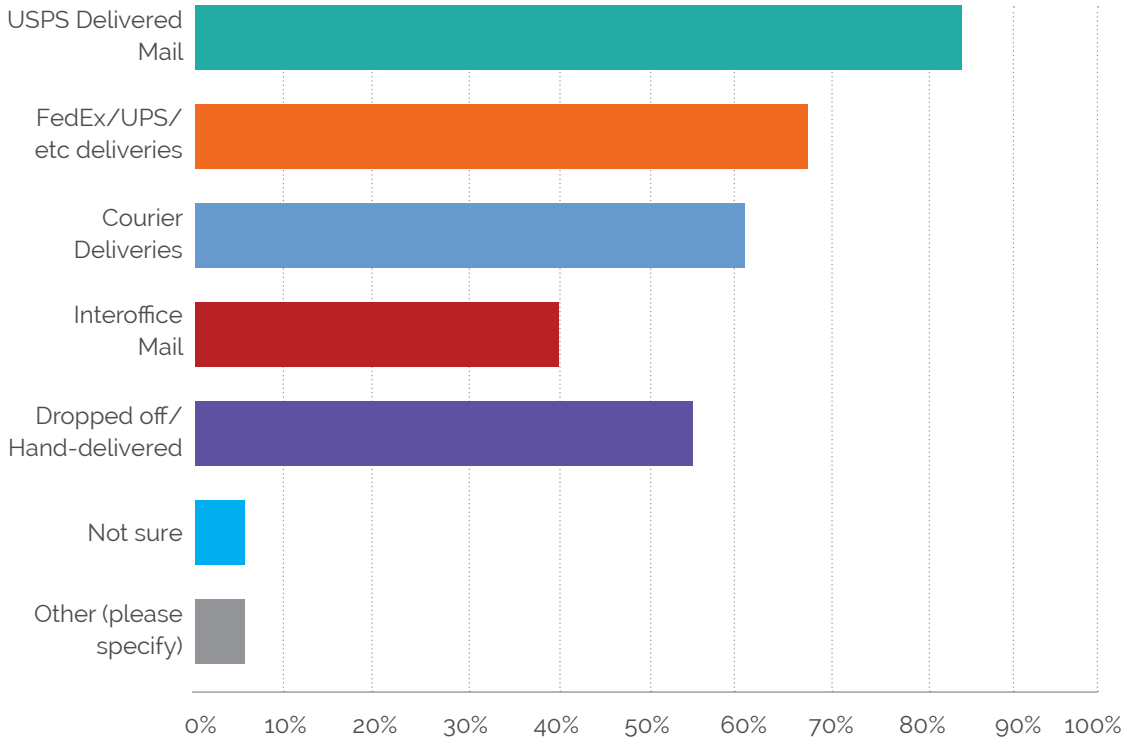
What is the primary industry for your company/organization?



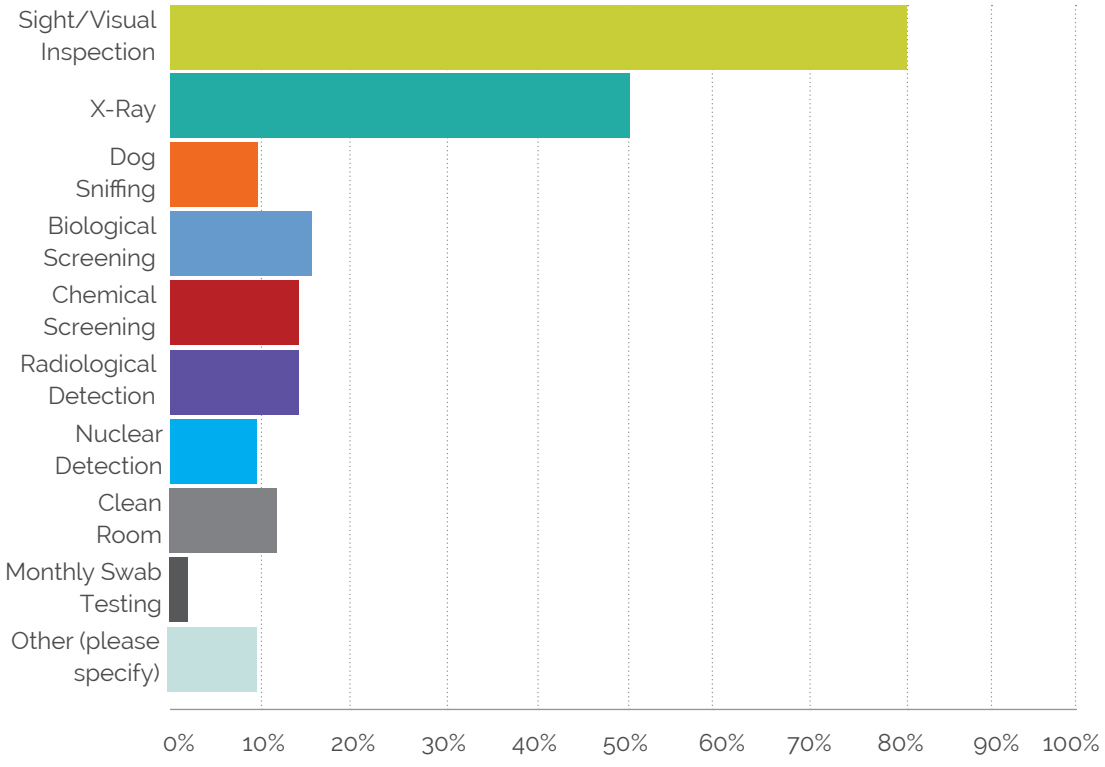
Where is your mail screened?



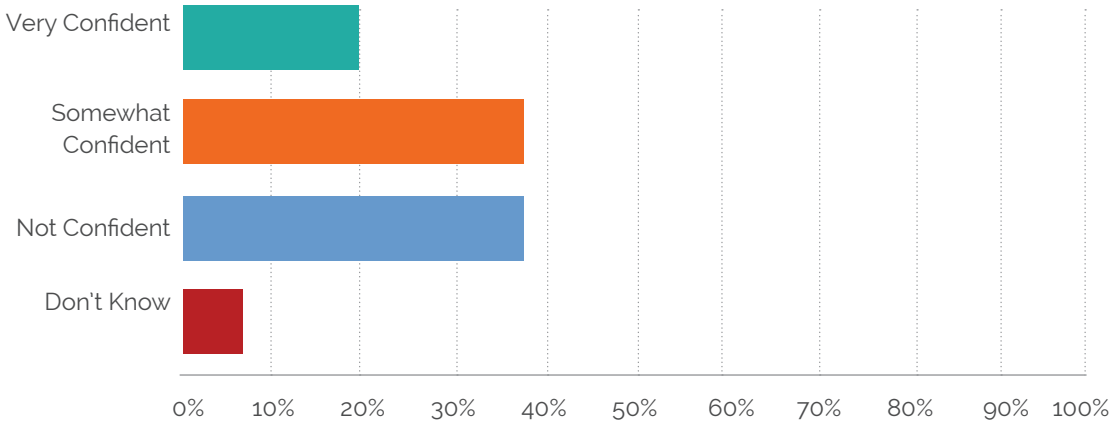
What types of mail are screened? (check all that apply)



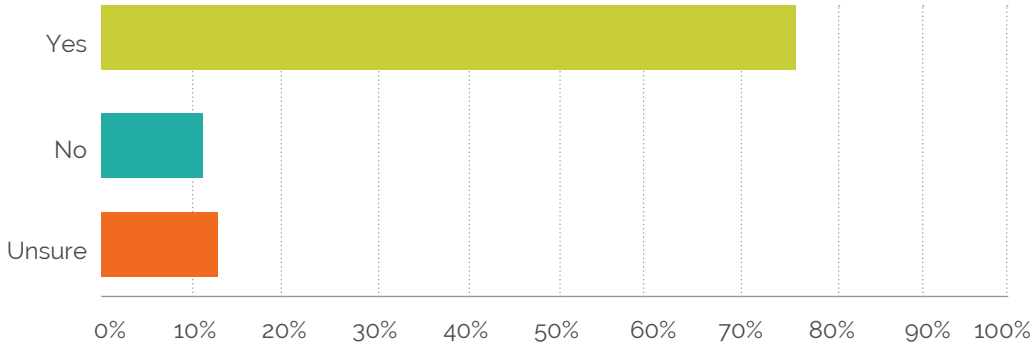
What procedures does your organization use to screen the mail? (check all that apply)



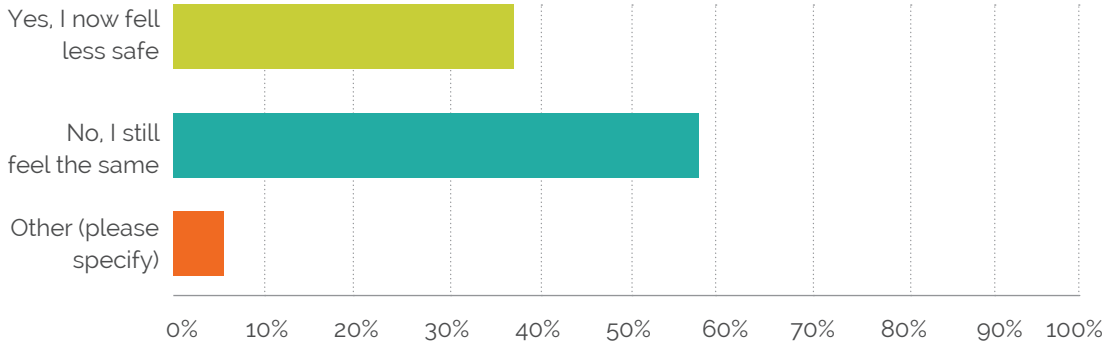
How confident are you that biological and chemical threats will be detected by these procedures?



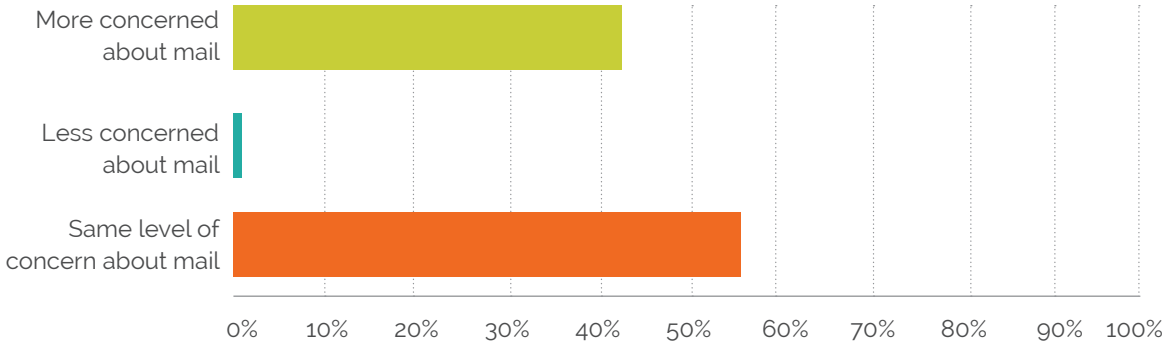
Are you aware that ISIS is working on Chemical and Biological weapons?



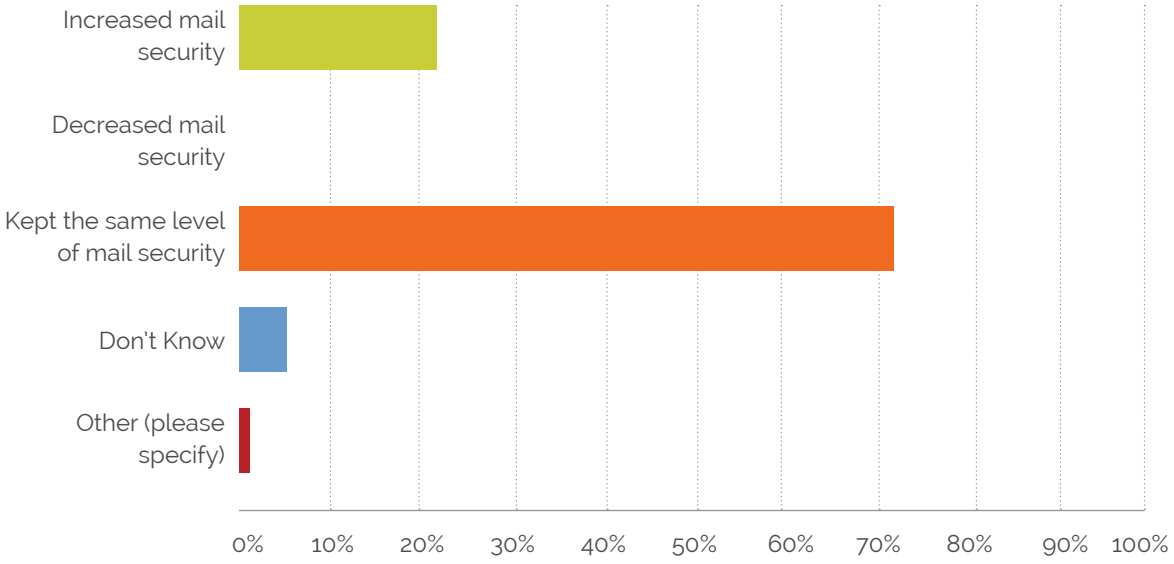
If yes, does this change how safe you feel?



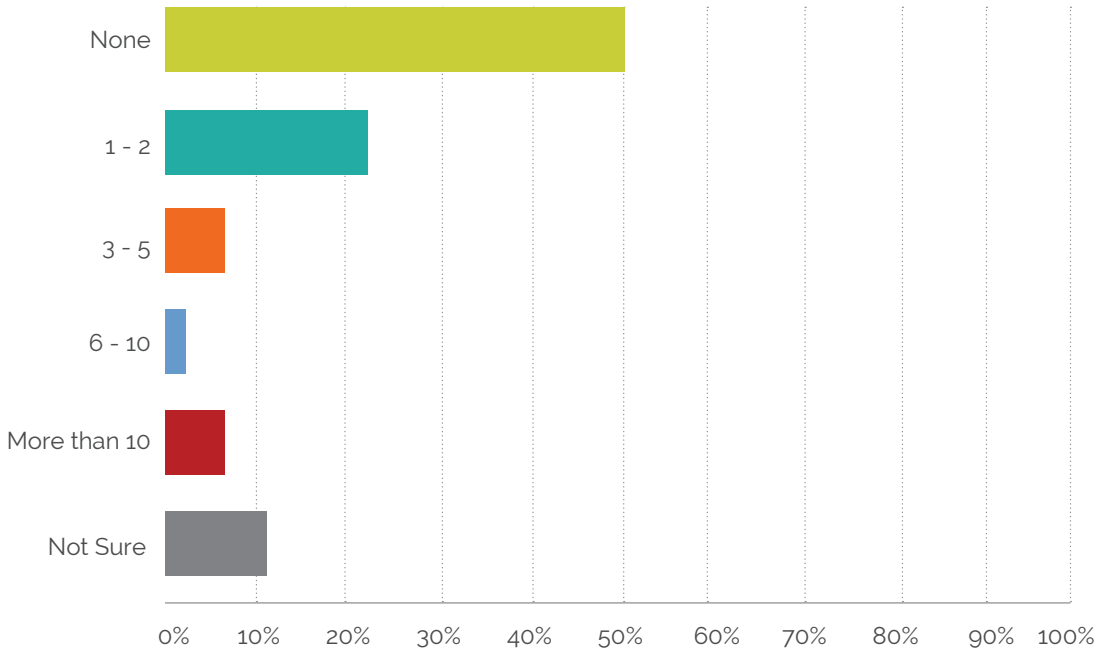
Compared to a year ago, are you:



Compared to one year ago, has your organization:



Over the last year, about how many threats (hoax or real) have been detected at your organization?



Proper mail screening keeps your business running and your team safe.

Every day, threatening letters and parcels land at corporate and government offices. Most are inconvenient. Some cause damage. A few change everything.

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
- Training to make sure your entire team – both inside and outside the mailroom – can identify and respond to mail borne threats.

SoBran SafeMail keeps your team safe and your operations running.

SoBran INC.

SafeMail

SoBran, Inc.
2677 Prosperity Avenue, Suite 200 Fairfax, VA 22031 • 703.352.9511
SafeMail@SoBran-Inc.com • www.sobran-inc.com