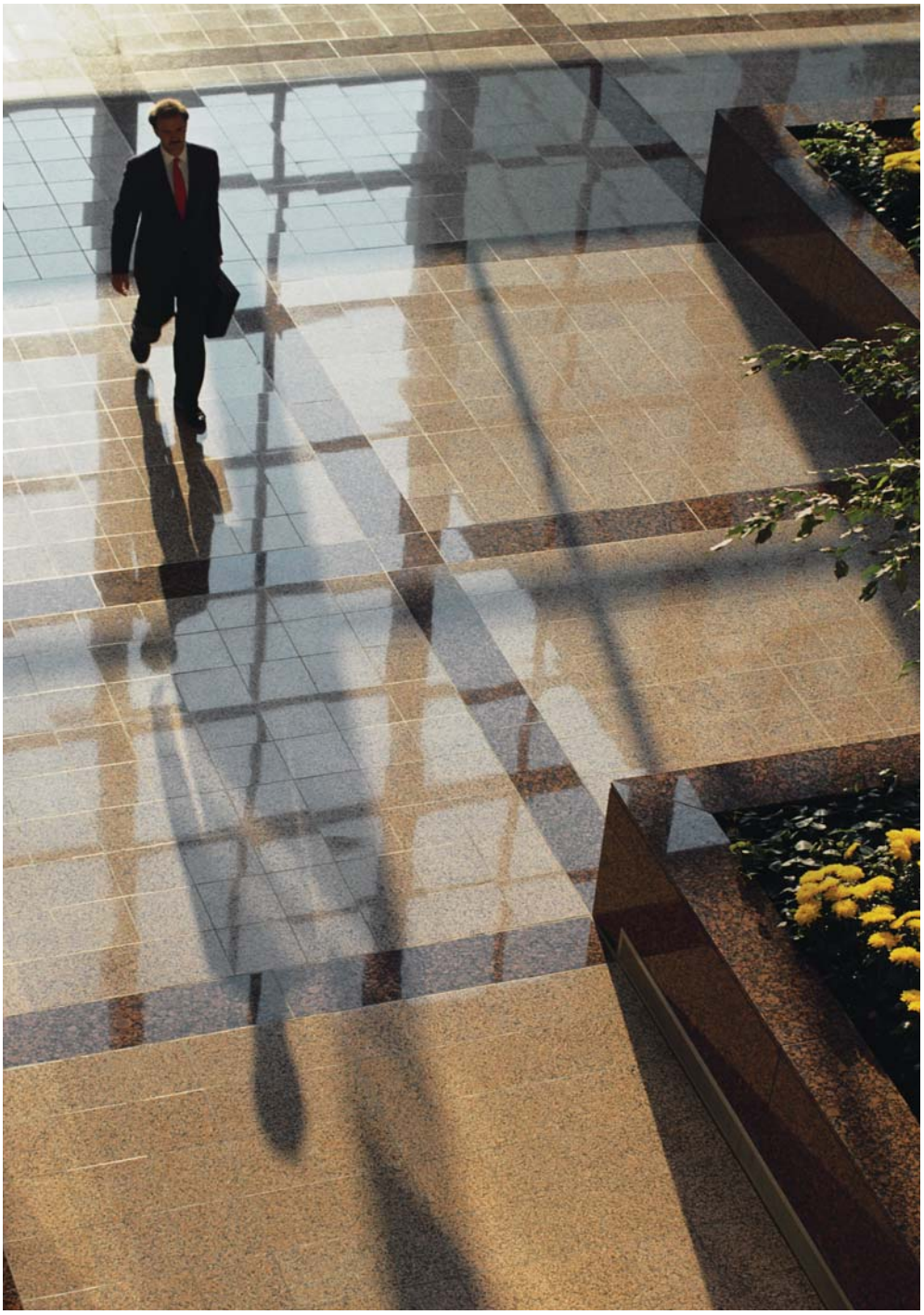
Pitney Bowes

Maintaining mail safety and security on a budget



WHITE PAPER

Introduction

"Never waste a good crisis." This phrase is being heard everywhere these days. Faced with tight or even "crisis" budget levels, many organizations may be tempted to scrimp on spending for their mail security activities. They should however be using this unique opportunity to implement preventative actions to both save money on their mail operations and reduce the likelihood of potentially catastrophic security events down the road.

Economic downturns and the resulting budget cuts they produce, cause people and organizations to do many things differently. While some changes, such as reducing unnecessary expenses can be beneficial, others may actually increase the risk of negative outcomes. One area where this is particularly true is activities related to mail safety and security. At a time when we have seen rapid growth in the threat from suspicious mail, many organizations are cutting back on their commitment to mail screening or abandoning the process all together. This both increases the direct risk to their people and facilities and sets their business up for a potentially catastrophic disruption. Increased threat levels and a decrease in vigilance are a deadly duo. Individuals who are responsible for the administrative and security functions in organizations should take this opportunity to conduct a complete review of their mail security processes. They will find that with some help from outside experts, they should be able to both reduce the cost of their current operations and decrease the risk that suspicious mail poses to their organization.

Current state of the threat

According to the United States Postal Service, the overall volume of First Class mail has been decreasing steadily over the past four years and the volume of stamped mail is now down to 1964 levels. Despite this decrease, an analysis of incident reports by Mailroom Safety News suggests that the number of mail-related threats has continued to rise at an annual rate of over 10 percent since 2005. In fact 2008 was a particularly challenging year for the mail and security professionals who had to deal with an extraordinary number of white powder related incidents targeted at major financial institutions such as JP Morgan Chase, U.S. federal government agencies, state governor's offices and international media outlets.

While the total number of suspicious mail incidents is difficult to document, the Mailroom Safety News analysis of publicly available incident reports suggests that the number of white powder incidents involving mail is up 40% from 2005 levels. The number of threatening letters, or as it is more popularly known, "hate mail", has also increased more than 37% over the past three years. Only the number of mail letter bomb-related threats seems to have decreased, with the total number of threats, hoaxes and actual explosive devices down almost 43% from the 2005 level. According to the U.S. Postal Inspection Service website, "Postal Inspectors have investigated an average of 16 mail bombs over the last few years."

In addition to an increase in the number of suspicious mail incidents that are taking place, there has been a change in the type of individuals who are sending suspicious letters and the purposes for which they are doing it. Actual terrorists seeking to injure or kill people are relatively few in number. More likely, mail threats will originate from someone who is merely upset about a public policy decision by the government or a company's involvement in controversial practices such as animal testing. The economic environment is also creating new security risks. In late-2008, a man who lost $63,000 in investments sent threatening white powder letters to 52 Chase Banks because he felt JPMorgan Chase was responsible for his losses. Currently, the large number of company layoffs is producing an increase in "hate mail" from employees who believe they were treated poorly by their company. While much of this has been in the form of threatening e-mails, security and risk experts are now cautioning senior managers to be on the lookout for white powder and bomb threats in their physical mail. According to the 2009 ASIS International survey of chief security officers entitled "Impacts of Current Economic Environment on Security," employees lay-offs and furloughs ranks second on a list of items creating an increased need for security.

Whether designed to actually kill, or merely to disrupt, suspicious mail has largely the same impact. Any white powder that spills from a letter onto the desk of an employee will temporarily shut down the functioning of an organization and likely disrupt operations for several days. According to the FBI press release issued after the conviction of the individual who sent the Chase Bank letters in late 2008, "a total of 65 threat letters were received in 11 different states and the District of Columbia. Sixty-four of the 65 contained an unidentified white powder, along with a threat that the person breathing the powder in would die within 10 days." Not only did these letters impact the specific office that received them, they psychologically impacted all Chase employees handling mail anywhere. They also adversely affected the morale of employees in other banks as some began asking themselves the question, "will we be next?".

Letter bombs and "hate mail" have become relatively familiar terms to most people during the past few decades. Anthrax and "suspicious white powder" were added to the list in late 2001 and Ricin in early 2004. There are also a number of new threats that corporate security managers should expect to encounter during the current decade. In late 2008, then Homeland Security Secretary Michael Chertoff predicted that more terrorists will soon learn how to make biological weapons and dirty bombs. We should expect to see additional types of biological threats enter the mailstream in the near future. While dirty bombs will probably not be shipped by FedEx or UPS, even a small amount of improperly marked radioactive medical waste material in a small package may prompt a significant and highly disruptive response on the part of local first responders. Therefore, any mail screening system must be both responsive to the current threats and sufficiently adaptable to deal with a wide range of future ones.

Current state of technology

There are a full range of technologies now available to help a mail center manager or security chief defeat the mail security threat in their facility. These technologies range from those designed to help detect explosives to those that actually destroy biohazards in mail. The combination of screening technologies employed will vary based on the overall state of the mail security threat and the particular requirements identified as the result of a local risk assessment by an individual company or organization.

The most common mail screening system in place right now is limited to having individual mail center personnel visually "screen" for suspicious mail based on the traits outlined in a poster produced jointly by the U.S. Postal Inspection Service, the FBI and the Department of Homeland Security. These posters should appear in almost every mail center and list common things like a missing return address and excessive postage as key identifiers. The USPS also cautions mail handlers that "mail bombs may have protruding wires,

aluminum foil, or oil stains, and may emit a peculiar odor."

Unfortunately, while having attentive mail handlers does serve as the first line of defense, it is rarely enough to deal with today's more sophisticated explosive devices and biohazards. To help deal with some of these more challenging security requirements, many mail centers have added explosive detection canine teams, X-ray scanners, biohazard detection systems, radiation pagers, and similar technology to supplement the visual screening ability of their mail handlers. More and more frequently, inbound mail centers are being enclosed within a negative pressure air room that helps contain and reduce the impact of any potential biohazards, such as anthrax, that may be in the mail. A few high risk mail centers have added a decontamination system that uses a combination of technologies including electromagnetic irradiation, ultraviolet, microwave, high-intensity broad beam, infrared, and other light sources to kill biological hazards that may be present in the mail. Some organizations have placed limitations on physical mail altogether and transform hard copy mail into digital mail using desktop scanners and the appropriate mail imaging software. In addition to providing enhanced security, this process often speeds up the core functions of the organization, so customer service and records management tasks are easier to accomplish.

One development that has significantly increased the security of organizations against mail related threats and enabled businesses to reduce their administrative services and real estate budgets is the shift to offsite, multi-client facilities. These facilities integrate the best available mail screening and processing technology and highly trained personnel in a manner that provides the best of both worlds, superior security and lower capital and operating costs. They also frequently provide organizations the ability to increase or reduce the range of mail screening procedures as threat levels change. Even the largest firms that could technically afford to build and maintain their own in-house facilities have found that the combination of savings and security provided by vendor operated offsite facilities more than offsets any perceived "loss of control" that may have limited the ability to use this model during the good budget years. And once the move to an offsite facility is made, real estate can be reduced or repurposed as necessary.

Integrated approaches to enhance safety and security

As is immediately evident in the above discussion, there are a wide variety of tools available to help deal with the task of identifying and protecting against threats in the mail. Today's best practices in mail security focus on the creation of an integrated approach to the problem. This also requires an integrated approach to understanding the challenges and risks associated with an organization's particular mail operation and business functions. Organizations that receive a high volume of common mail such as credit card payments will have much different screening and processing needs than those that receive handwritten personal mail from individual grant seekers or a global fan base. The first type of business will emphasize the need for speedy processing, while the second organization will tend to view their mailstream as potentially more risky and require more deliberate mail screening processes.

Sorting out the local risk factors, mail processing requirements, and screening procedures requires the focused interaction of the security, administrative services, and operational components of each organization. Only when these three groups work together can an organization develop a response to the mail security threat that both protects the organization and helps it continue to grow and profit. The next section provides an outline of introductory questions developed to help the various stakeholders begin the process of analyzing their needs and developing an effective and affordable response.

Five questions to ask your mail center manager and/or your mail vendor

Whether an organization has an internal mail center operation, or you have already outsourced one or more components of your mail operation to an external mail services vendor, there are a number of questions that you should ask.

1. **Who in the company will be most impacted if we lose our mail operations?** The primary purpose of mail security and mail screening operations is to protect employees, facilities and customers. An equally important purpose, however, is to protect and maintain the business functions that require the free flow of mail to operate successfully. It is very important to document the flow of mail into and out of the organization and then analyze the risk factors throughout the flow and the impact any disruption may have on the customer facing and back-office functions of the organization.

2. **When was the last time we did a mail center security audit and what did we learn?** The bad news is that the managers of administrative services functions rarely ask themselves this question until after a security "event" happens. The good news is that most organizations perform annual security audits. Unfortunately, this process frequently stops at the loading dock door. Often the management of administrative services functions are not asked to contribute to the process and don't receive the results. Security managers must require the participation of administrative services and operational management in the conduct of their security audits and must share the results. If this doesn't happen, administrative services managers must ask for them.

3. **When was the last time we trained our people on suspicious mail and emergency response procedures?** Suspicious mail training in far too many organizations

consists of hanging a USPS poster in a mail center and telling employees to look for suspicious mail when they are sorting it. Security managers must ensure that administrative services personnel are trained upon hiring and receive refresher training at least annually. The organization's internal security manager can provide this training or hire one of the many highly qualified security consultants specializing in mail and package screening operations. The training must also include emergency response procedures for a wide variety of potential incidents and should involve the local first responders (fire department, police department, emergency medical teams, etc) whenever possible.

4. **To what extent does our corporate business continuity plan cover our mail operation?** Mail is critical to most successful operations. It is highly likely that an organization will lose access to the facility that provides its mail processing if a suspicious mail incident occurs. At a minimum, it will take several hours, and in many cases days, to reopen a mail center that has experienced a white powder incident. It actually requires months and in some cases, years, to reopen the facilities, as was the case with buildings that were determined to have been exposed to anthrax in October 2001. Events such as storms and power failure may also close a mail center. It is important to ensure that the organization's overall business continuity plan address the mail center and mail operation. Even if a company does not send its mail to an offsite multi-client facility for processing, it may find value in contracting with such a facility for business continuity purposes.

5. **What is the one thing you think we should do now to improve the safety, security, and continuity of our mail operation?** Most managers now realize that they can learn a lot about their operations by asking their employees what is going right and equally importantly, what is not quite right in their organizations. Administrative services and security managers should regularly ask these questions of their employees and themselves when considering the safety and security of their mail center operations. Frequently, major improvements in employee morale can be achieved by making small changes in processes or investing in things like gloves and facemasks for wear by their mail center personnel. In other cases, outsourcing mail screening operations may enable an organization to continue to function safely and effectively despite hiring freezes or significant budget cuts.

Conclusion

Successfully dealing with threats in the mailstream requires a strongly proactive approach. Perhaps nowhere is the old adage "an ounce of prevention is worth a pound of cure" more appropriate than in the area of mail security. Facility managers must understand the risks that suspicious mail can pose to their people, their facility, and the business processes they support. They must implement an integrated screening process that leverages the currently available technology and highly trained personnel who can detect and properly respond to threats in the mail. For some organizations, the screening process may be as simple as just spending a few extra seconds looking at each letter as it is being sorted. For others, the process will involve a specially designed offsite facility, complete with x-ray equipment, biohazard detection systems, chemical sensors, and decontamination equipment. In all cases, the process must be capable of dealing with the current level of risk to the organization and be capable of rapid upgrade in the event that the threat posed by suspicious mail changes quickly.

Few organizations have the experience, resources and time to design and manage an appropriate response to the threat of suspicious mail. Most would be well served by seeking help from an external security consultant or one of the larger mail services outsourcing companies. These organizations focus on the suspicious mail threat on a daily basis and understand the risks and rewards associated with the alternative screening approaches that can be implemented. Mail security consultants can work directly with mail center managers and security teams to complete a proper risk assessment and design a mail screening system that is appropriate, effective and affordable. Similarly, high quality mail services companies can help with these tasks as well as take on the daily task of providing onsite mail screening and processing. Additionally, they will be able to provide access to a single or multi-client offsite mail facility that incorporates not only the best screening technology, but highly trained screeners and consistent processes. Finally, the use of full service offsite mail facilities will help reduce real estate expenses, lower outbound postage costs, and in some cases, provide access to services such as digital printing and document imaging.

While the threat of suspicious mail can never be totally eliminated, it can be properly managed and mitigated to ensure the safe and continuous operation of any organization's mail processing system. While the adage "never waste a crisis" may make good sense in the political arena, and may enable more rapid internal changes than would be possible in "normal" times, it still makes good business sense to try to prevent a crisis from occurring in the first place. With a little bit of focus and a little bit of help, managers can prevent mail security risks from becoming a mail incident-related crisis in their organizations.

For more information on Pitney Bowes Management Services, please call 888-245-PBMS.

Pitney Bowes Inc.
1 Elmcroft Road
Stamford, CT 06926-0700
Telephone: (888) 245-PBMS

For more information about our products and services, please logo onto our web site: www.pb.com/pbms