



DualDraw LLC White Paper Series:

The Mail Center – A Forgotten Vulnerability in the Post 9/11 World

INTRODUCTION

It's been close to six years since terrorists used Anthrax laced letters as weapons of mass destruction. The impact of those attacks has diminished. Mail Center Security has been forgotten as a top priority for security professionals and facility managers – many times it doesn't even make today's list of security concerns. This is a costly mistake. To ignore this vulnerable area exposes the soft underbelly of an organization and widens the possibility of suffering human and financial consequences from an attack. More likely, an organization will need to react to one of the many chemical / biological / explosive hoaxes sent through the mail system on a regular basis. Do you receive mail at work? Then this article is for you – it is also for any professional responsible for the protection of employees in the workplace.

COSTS OF COMPLACENCY

White powder hoaxes happen on such a frequent basis they are difficult to track as many are not reported. One estimate from an industry expert puts the figure at approximately 40,000 since 2004. Below is a snapshot of a few of the reported incidents taken over a two week period:

- Maryland Courthouse Evacuated After Receiving Bomb Threat Letter and Powder (Washington Post, 4/10/2007)
- BioWeapon, Bomb Threat Scare at Maryland Courthouse (News Service, 4/9/2007)
- Mystery Powder In Mail Triggers Scare At Gerber (Grand Rapids Press, 4/13/2007)
- Anthrax Scare Shuts Down the Boise School District Building (Fox 12 News, 4/17/2007)
- Leaky FedEx Package Creates Hazmat Scare (San Antonio News Express 4/17/2007)
- Illinois Tax Office Closed For Suspicious Powder Scare (CFN News, 4/19/2007)
- Probe Follows Anthrax Scare in Canadian Lab (Edmonton Sun, 4/21/2007)

What these headlines do not include are the costs associated with a hoax. How prepared were any of these organizations for a threat of this nature? Do you think they had protocols in place to handle a mail threat? Were first responder resources diverted from other real emergencies in the community to respond to these hoaxes? How many people were evacuated as a result of these seven incidents? What about the opportunity costs and productivity loss? Do you think employees feel safe returning to work? The scope of this article does not include all of the answers to the above but most organizations are critically under prepared in this area of workplace security.

THE POST OFFICE – PROVIDING PROTECTION, BUT LIMITED

You may be asking "doesn't the post office protect us from these kind of threats?" The answer is "well, sort of". In September of 2005, the United States Postal Service unveiled a \$971 million dollar biological detection system (BDS) to help reduce the risk of Anthrax being delivered through the mail. Approximately 218 large distribution centers across the country now have this technology. This is encouraging although there are gaps in the current system that leave organizations vulnerable and has in some cases created a false sense of security among security professionals. The system currently checks standard envelope size mail. Flats, boxes and non-standard envelopes are not checked although there has been discussion about adding other sized envelopes and packages to the system. Also, it only analyzes for the biological agent Anthrax. According to Postal Inspectors, the system can be upgraded to check for other harmful pathogens however no such upgrades have taken place as of the writing of this article. Ricin, an easy to make, deadly pathogen sent through the mail to Senator Bill Frist's office in February of 2004, is currently not detected by the system. Thankfully, no injuries or fatalities occurred as a result of this incident although a lethal dose of Ricin only takes 0.2 milligrams can be lethal in less than 6 hours.



The capitol police hazmat team scrubs up outside a Senate office building after testing for Ricin. Mark Wilson/AP

MAIL CENTER SECURITY STARTS WITH YOU

The intent of the information above is not to frighten your organization into spending lots of money and resources on Mail Center Security. Instead, the objective is to refresh our collective memory of a vulnerable area of operational infrastructure that is often overlooked. Ultimately, the resources spent on the security of the mail center are an outcome of voluntary and discretionary decisions made by the owners and operators of a facility. To effectively provide decision makers with the information needed to prioritize Mail Center Security resources, the second half of this article provides summary information on how to develop a Mail Center Security Plan.

PART OF A LARGER PLAN

A Mail Center Security Plan needs to integrate into an organization's overall security architecture. Ideally, the development of this plan should be accomplished using some of the same planning tools, techniques, and resources used to develop an organization's master security plan. Importantly, the effort to develop a Mail Center Security Plan needs to have leadership buy-in but also the endorsement of the mail center personnel – those most directly affected by its implementation. For large organizations with multiple offices, it should be developed at a headquarters level and tailored specifically for the smaller mail centers throughout an operation. Single facility organizations should develop a plan according to the specific physical layout of the mail center.

A key measure of a successful Mail Center Security Plan is the balance it strikes between effective security and being able to conduct business as usual, without major disruption to standard practices and procedures. This balance can be deliberately tilted one way or another based on the particular risk profile of an organization. To obtain a risk profile, a risk assessment is needed.

A risk assessment is the fundamental tool that helps organizations effectively prioritize their security needs

Sample Questions to Ask as Part of Your Risk Assessment

1. What is my organization protecting?
2. How much would this loss cost your organization in time, lost productivity or business? What is the key function your mail center plays in this role – this is the one that you need to restore/preserve under a disaster recover scenario.
3. Does your organization deal internationally, have foreign affairs officers, suppliers or been the primary focus of a recent crisis or other public interest?
4. Who are your adversaries?
5. Is your organization doing business where there is political/religious unrest?
6. Has your organization undergone recent downsizing, reduction in force or hiring freezes?
7. Has anyone in your organization received an employee threat recently?
8. Is your organization involved in research, products or services of public controversy?
9. What can you do to ensure that your vulnerabilities are limited and countermeasures are applied?

Adopted from the GSA Mail Communications Office, Mail Center Security Guide, Third Edition

and thus allocate resources accordingly. This assessment can come be performed with the help of security consultants with assessment expertise or it can be a simple checklist developed by a mail center employee or facility manager. Some of the critical elements of a Mail Center Security Plan are highlighted below:

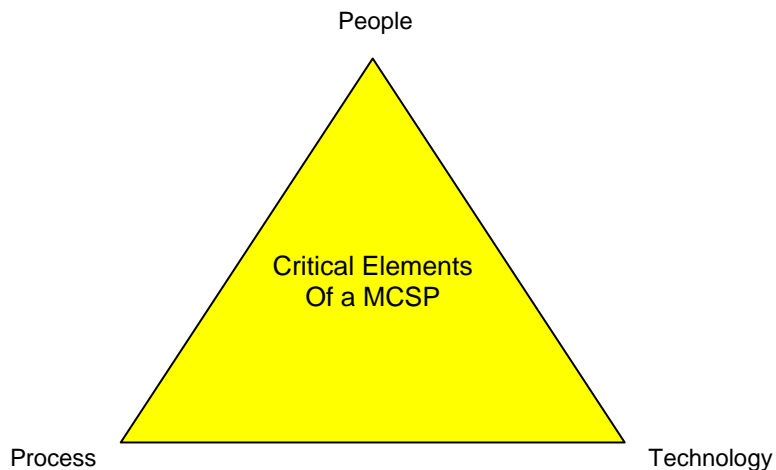
Critical Elements of a Mail Center Security Plan

1. Risk Assessment
2. Operating Procedures
3. Training, Testing, and Rehearsal Plan
4. Managing Threats
5. Communications Plan
6. Occupant Emergency Plan (OEP)
7. Continuity of Operations Plan (COOP)
8. Annual Reviews

Adopted from the GSA Mail Communications Office, Mail Center Security Guide, Third Edition

There are many free resources available to help organizations develop each of the critical elements of a Mail Center Security Plan as cited above. These steps are taken from the GSA Mail Communications Office, Mail Center Security Guide, Third Edition and is located at http://www.gsa.gov/Portal/gsa/ep/contentView.do?P=MTM&contentId=15082&contentType=GSA_DOCUMENT. Another important resource is the USPS list of best practices for mail center security, located at: <http://www.usps.com/communications/news/security/bestpractices.htm>

An important approach to consider when developing a Mail Center Security Plan is the affect of the critical elements of the plan on People, Process, and Technology.



The impact of each critical element of a plan should be assessed based on how it affects each of the above three components. How will the people of your organization be affected? Will the plan affect their job responsibilities? Is mail security a concern of your employees and will a plan that is executed properly help reduce anxiety? Will the processing mail take longer? Is the organization prepared to potentially delay mail delivery for the sake of safety? Is there new technology that will be introduced? Equipment investment such as negative air workstations and detection may require training and maintenance to be used effectively to combat the threats.

CONCLUSION

In a post 9/11 world, organizations cannot afford to be complacent in the vulnerable area of mail operations. While there may appear to be many things to consider when developing a Mail Center Security Plan, the reality is that with some thought, basic preparation and tools organizations can increase safety and decrease employee anxiety in the workplace. It all starts with a plan.

*Written by Dan Prather, Senior Vice President of DualDraw, LLC, a manufacturer of mail center security equipment. www.dualdraw.com
Dan is also Sector Chief of the Postal and Shipping Critical Infrastructure Area for Infragard, a public/private information sharing organization between the FBI and private sector.*