ARMADA

Providing Comprehensive Risk Mitigation and Security Solutions

Strafford

Strengthening Security in Company Mail Operations Teleconference

Nov. 28, 2007

Tom Foos, Armada USA

tfoos@armadausa.com

Mail Security In A Small To Mid-Sized Corporate Environment

Presentation Agenda

- Assessment process
- Applications of mailroom security in small to mid-sized corporate environments
- Examples of applied solutions
- General findings/current awareness levels
-
- Policies/procedures and technologies used

ARMADA

Assessment Process

- Mailroom security should be evaluated as a part of an overall organizational “security review”
  - Don’t just think of it as a “mailroom”; rather, a mail *service* (receiving, screening, sorting, delivery, etc.)
  - Review the process and implement mitigation steps for the process, not just the “room”
- Outline findings and mitigation steps (suggest observations and recommendations format)

ARMADA

Application Of Mailroom Security

- Like many other areas within small and mid-sized business, “mailroom” security is often ignored
- “Mail” security programs should be included in an organization’s overall security plan
- “ Top-down” buy-in is critical regarding mail security
- Review the facility make-up, technologies, policies and procedures, training, sourcing (in-house vs. outsourced), etc.

ARMADA

Practical Application: Small Business

- Most small businesses will not rely on technology to enhance security
  - Typical methods
    - No policies and procedures
      - “Receive it and deliver it”
    - Minimal training – Typically system-related, not security related
    - “Emergency” notifications only – Not suspicious packages
  - Recommended methods
    - Usable polices and procedures
    - Regular training on systems and security
    - Flow chart/call tree
    - Test/evaluation mitigation steps
    - Augment with basic technologies
      - Add a CCTV camera to the area, access control, etc.

ARMADA

Practical Application: Small Business

- Identify those who may have mail duties
- Establish practical policies and procedures for the specific business
  - Deliveries through front entry or “delivery entrance”
  - Time of day to accept deliveries/mail
  - List of known delivery personnel (pictures if applicable)
  - Process to verify “temporary” delivery personnel
    - Phone numbers to call: USPO, DHL, UPS, FedEx
  - General inspection standards
    - FBI suspicious package posters
    - Isolation area for suspicious packages
    - Acceptable response procedures (don’t handle it)
  - Notification call tree/flow chart
    - Internal vs. external

ARMADA

Practical Application: Small Business

- Outline mail delivery protocols
- Place in “community area” individual mailboxes
  - Deliver directly to offices (securable)
  - Request direct pick-up by employees (sign for it)
- Train personnel (and their alternates) on the process
- Test the process
- Make adjustments as needed

ARMADA

Practical Application: Mid-Sized (Or Larger) Business

- Appoint a mail security coordinator (MSC)
  - MSC needs to be a responsible & trustworthy person
    - A long-term and respected employee
  - Alternate designated who meets the same criteria
- MSC and alternate are “internal experts”
  - Should receive postal training and training on handling suspicious packages
  - Develop and deploy appropriate procedures/postings
  - Train management/other personnel on internal company policies regarding how to handle mail

ARMADA

Practical Application: Mid-Sized (Or Larger) Business

- Policy and procedure development
  - Mail delivered directly to the mailroom – Only MSC or alternate should receive it
  - Mail delivered to personnel's office or work area
  - Only authorized personnel allowed in mailroom
  - Designated area (remote if possible) in which to put suspicious packages pending investigation
  - Conduct emergency preparedness drills simulating, among other events, potential mail bomb or suspicious substance in the mail
  - Open mail with rubber gloves
  - Personnel encouraged to practice good hygiene, i.e. washing their hands after processing the mail

ARMADA

Practical Application: Mid-Sized (Or Larger) Business

- Technology upgrades
  - Access control system
    - Only authorized personnel are provided the appropriate access control level to enter mail room
  - CCTV
    - Cameras added to mailroom and surrounding areas
  - X-Ray/screening machines

ARMADA

Applied Solution: Courthouse

- Contracted to complete the initial assessment and provide general mitigation steps
- The client developed and implemented the final mitigation steps
- Appointed a mail security coordinator – Mail clerk
  - Background check conducted during employment-screening process
  - Alternate designated, background checked
  - Recommended training sessions for mail center, security and management personnel to validate the practicality of all phases of the mailroom security and screening program

ARMADA

Applied Solution: Courthouse

- Policies and procedures - Highlights
  - Developed general screening and inspection procedures for all incoming mail or package deliveries and outlined training requirements for employees regarding those procedures
  - Developed specific mail center handling protocols for items identified through screening as suspicious and dangerous
  - Designated an isolation area for suspicious packages encountered through the screening process
  - Establish a safety zone around the isolation area
  - Completed training sessions for mail center, security, management personnel and administrators to validate the practicality of the mailroom, screening and delivery program

ARMADA

Practical Applications Of Mailroom Security: Courthouse

- Technology
  - X-ray machines for all mail, FedEx and other packages
  - Mailroom added to access control system
  - CCTV system augmented to include coverage of inside the mailroom and area outside
  - Biological screening machines

ARMADA

General Findings/Current Awareness Levels

- Mailroom security is typically overlooked
- Businesses may not even consider the basics
  - General policies and procedures
  - Regular, consistent and site-specific training
  - Include the mailroom when developing security technology systems
    - Access control, CCTV, screening, etc.
- Outsource vs. keep duties in-house
  - In-house: Vested interest, better control over duties/processes, known employee, discipline if needed

ARMADA

General Findings/Current Awareness Levels

- Even if mail policies exist, “mail clerks” typically have little or no training regarding security related topics
- Top-level management buy-in may not exist
  - Management typically doesn’t feel that the potential threat/vulnerabilities warrant the investment or deployment of training/technologies other than what already exist

ARMADA

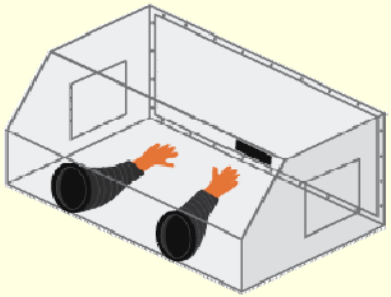
Policies/Procedures

- Policies and procedures
  - Appoint a mail security coordinator
    - Becomes a subject matter expert - Trained
  - Establish a strict employee identification/personnel security program
  - Establish health safety procedures
  - Conduct training, emergency preparedness drills and information update meetings, as necessary
  - Shut-off points of processing area's ventilation system should be mapped and should be part of an emergency procedures handout

ARMADA

Technologies Used

- Technology used
  - Mail batch processor



  - X-Ray

ARMADA

Takeaways/Lessons Learned

- Once management has been educated on the potential risks, there is a greater willingness to deploy recommendations, particularly in regard to:
  - In-house vs. outsource
  - Appointment of a “mail security coordinator”
    - Ensure they have appropriate and thorough training
  - Development of necessary security policies and procedures
  - Deployment of “appropriate” technology upgrades in areas such as access control, CCTV, screening, etc.

ARMADA

Takeaways/Lessons Learned

- Continuous actions
  - Like the general security of your organization, “mailroom security (better referred as “mail service security program”) needs to be part of a continuous improvement process
  - Test and evaluate your protocols

ARMADA