

# Pivotal THOUGHTS

*Ideas for customer-focused  
senior executives*



## ENTERPRISE-WIDE

## MAIL

## AND

## DOCUMENT

## SECURITY

### In this issue

The New Meaning of Corporate Security

The Vulnerable Portal: Securing Your Company's Mail Operations

Safeguarding Your Mail and Document Flow

Turning to the Experts

Leading in Times of Crisis

Building a Crisis Team

Recognizing the Paper/Digital Partnership

And more

## LETTER FROM THE EDITOR

*Dear Colleague,*

*Business has always been concerned about keeping its employees safe and its enterprise running without disruption. But in today's world, the threats are so severe and omnipresent that executives must now seek solutions before problems emerge.*

*That is why the theme of this Pivotal Thoughts issue, "Enterprise-wide mail and document security," is such a critical one. On the following pages, you'll read about a recent survey among senior executives regarding their attitudes toward corporate security. And you'll find recommendations on how to help secure your company and employees against external threats. Finally, be sure to see page 29 for two free offers from Pitney Bowes.*

*I hope you find Pivotal Thoughts to be worthwhile reading, and I would like to hear your feedback. Please feel free to e-mail me at [pivotalthoughts@pb.com](mailto:pivotalthoughts@pb.com) with your comments and suggestions.*

*Sincerely,*



*Matthew L. Sawyer  
Editor-in-Chief*

## CONTENTS

- 1.** The New Meaning of Corporate Security
- 4.** The Vulnerable Portal: Securing Your Company's Mail Operations
- 7.** Safeguarding Your Mail and Document Flow
- 11.** Turning to the Experts
- 13.** Leading in Times of Crisis
- 15.** Building a Crisis Team
- 18.** Recognizing the Paper/Digital Partnership
- 20.** Turning to Pitney Bowes for Mail Security
- 25.** Beyond the Envelope
- 27.** Engineering the Flow of Communication
- 28.** About Dr. Robert F. Hahn II
- 29.** Two Valuable Offers from Pitney Bowes



**THE  
NEW  
MEANING  
OF  
CORPORATE  
SECURITY**



## **THE NEW MEANING OF CORPORATE SECURITY**

Not long ago, “corporate security” meant preventing company assets from being stolen and stopping Internet viruses. Three autumns ago, that all changed.

With the anthrax scare of 2001 and a war on global terrorism, security has become no longer just about protecting assets; it has become about protecting the business. Senior executives are thinking about security in a whole new light. And over the past three years, corporate security has increasingly focused on such topics as business continuity, disaster recovery and the flow of mail and packages — preparing for and dealing with threats that can shut down a business, damage or destroy facilities, and harm employees and customers. And of course, a security discussion is never complete these days without mention of privacy and data security issues.

“Corporate executives now must deal with a wide range of security threats through an integrated approach,” says Dr. Robert F. Hahn II, VP of Strategy & Secure Mail Solutions for Pitney Bowes Management Services. (Dr. Hahn’s professional biography appears on page 28).

“At one time, if you had an off-site data backup location, you were covered. But now executives have realized how vulnerable their facilities and their people really are, and how easily their businesses can be shut down.”

In 2001, cleanup of two anthrax-infected U.S. Post Offices required some \$150 million and 30 months — during which facilities were off-limits to all but biohazard-suited cleanup crews. Since then, an estimated 20,000 incidents involving suspect mail have occurred in the United States, prompting not just fear and concern, but serious financial consequences.

“Many companies struggle to deal with the disruption

of their operation when an office building is unexpectedly shut down for two or three days,” said Hahn. “The loss of access to facilities for an extended period of time due to a bioterrorism incident could be potentially devastating.”

A quick look at recent headlines shows that scenario is not just idle conjecture. Witness worldwide threats like the SARS outbreak of late 2002...regional system failures like the Northeast blackout of 2003...natural disasters like the Florida hurricanes of 2004. All resulted in major disruptions to business, and it has executives justifiably wary about 2005 and beyond.

### **Corporate executives speak out**

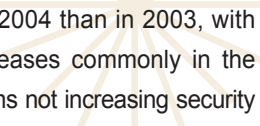
It comes as no surprise, then, that security threats are rated as highly important concerns by nearly 75% of respondents in a recent Pitney Bowes/BusinessWeek Research Services Survey of 10,000 senior corporate executives. The “Security in the Workforce” study, conducted in August 2004, sought to clarify the very real security challenges that today’s corporate executives face. And it was enlightening indeed. In brief, the survey points to these 11 key conclusions:

#### **1. Security concerns remain high**

Executives continue to view security as a top concern for their organizations. But despite the terrorist attacks of three years ago, their main concerns appear to revolve not around physical security, but around the security of their technology infrastructure. Physical threats to employees, for instance, were viewed as a primary concern by less than one-third of responding executives.

#### **2. Concern begets (some) action**

80% reported that their companies were spending as



much or more on security in 2004 than in 2003, with year-over-year spending increases commonly in the 10% to 20% range. Among firms not increasing security spending, four out of ten respondents said that their firms were “concentrating instead on traditional business and cyber crime” and not on security related to terrorism or facilities.

### 3. Security responses are mostly incremental

More than 80% of respondents said their companies’ higher security expenditures were focused mainly on upgrades of existing equipment and systems — twice the proportion who said that their companies were investing in new systems.

### 4. Formal security audits increase

Heightened concerns over corporate security have done more than boost security expenditures. They also appear to have prompted firms to conduct formal security audits. Nearly 7 in 10 respondents said their firms have undertaken a formal security audit during the past year.

### 5. A new title, “CSO,” emerges

“Chief Security Officer.” A few years ago, the position barely existed. And even today, only a quarter of respondents’ companies have appointed a CSO. But the trend is upward.

### 6. Chief Security Officers prompt action

Companies with a CSO are much more likely to have increased security spending, to have conducted a formal security audit, and to have undertaken other steps to improve security and risk assessment.

### 7. Important barriers to action remain

A significant plurality of respondents indicated that the presence of “ideal solutions” versus “real or practical solutions,” along with a lack of clear guidelines and standards, impeded their efforts to enhance corporate security.

### 8. Some security technologies are more familiar than others

A large majority of respondents are familiar with common security technologies such as remote video monitoring and smart cards, and about half now

employ these devices. By contrast, fewer than half were familiar with more recent technological innovations like biometrics and sophisticated mail screening systems, and only a few companies had actually put these technologies into operation.

### 9. Contingency plans take hold

In addition to taking steps to prevent the occurrence of damaging events, respondents also said their companies had undertaken activities intended to ameliorate the effects of such as event. 72% have instituted evacuation or other safety plans. 63% have established specific guidelines for employees to follow in an emergency. 56% have developed contingency plans or guidelines to service customers in a crisis. And 52% had put business continuity plans in place.

### 10. Mail screening technologies are deployed

Companies with CSOs were more than twice as likely to have put mail screening technologies into place, and those that had carried out a security audit were about six times more likely to have implemented such technologies. The implication is that mail systems may be a key area of undiscovered vulnerability in companies that have not conducted a security audit.

### 11. Mail processing is off-sited

Large firms were about three times more likely than smaller firms to outsource mail inspection and sorting operations. They were also more likely to conduct these operations in an off-site location. Moreover, firms that had conducted a security audit were nearly four times as apt to be outsourcing their mail processing operations.

For a copy of the full Pitney Bowes/BusinessWeek Research Services Survey “Security in the Workforce”, please call 1-866-DOC-FLOW or log on to [www.pb.com/security](http://www.pb.com/security).

*What does the term*  
**“security”**  
*mean when applied to*  
*your company today?*



**THE  
VULNERABLE  
PORTAL:  
SECURING  
YOUR  
COMPANY'S  
MAIL  
OPERATIONS**

# THE VULNERABLE PORTAL:

## SECURING YOUR COMPANY'S MAIL OPERATIONS



Since the fall of 2001, which lent top-of-agenda status to business continuity and disaster recovery, organizations have questioned the security of every aspect of their operations. Among the first areas to be reassessed was one of the most valuable, yet also most vulnerable, “portals” in an organization: mail and document operations.

And for good reason. Following the anthrax scare, a steady onslaught of hoaxes began appearing, and continue to appear, in the mail stream. These usually consist of some form of powder and an accompanying letter warning the recipient that they’ve just been exposed to anthrax or some similarly dangerous substance.

Because of the impact of the original anthrax letters, these hoaxes must be treated as potentially dangerous substances until proven otherwise. While less deadly to the recipient than anthrax itself, hoaxes can be just as damaging to business operations, disrupting activities for hours or even days.

A related concern is hate mail — threatening letters to senior management or the company as a whole — which can create a similarly disruptive effect on business operations. When this mail is identified early, the impact can be contained, frequently requiring nothing more than a call to the corporate security office. But if hate mail finds its way downstream to unsuspecting recipients, the impact can be much greater, causing emotional damage and engendering concerns among large groups of employees.

Certainly, then, package and mail tracking has become of paramount concern. How to handle package and mail security from the curb to the mailroom?

What measures to take to secure points of entry and egress? How can packages and documents be tracked from the corporate mailroom to their final recipients? Did the right person receive the package? Who touched it en route? And how reasonable is it to screen every mail piece and package for hazardous materials?

Clearly, quality in mail and package processing is no longer a choice; it’s an imperative for organizations seeking to enhance the safety of their employees and maintain the confidence of their customers.

“The safety of those who handle the mail and its contents depends upon the quality of the people you employ and the processes and technologies you deploy,” says Dr. Robert F. Hahn II, VP of Strategy & Secure Mail Solutions for Pitney Bowes Management Services.

### Enhancing mail center security

In most corporate mail centers, a copy of the U.S. Postal Service’s “Suspicious Mail” poster is hanging on a wall. Individuals sorting the mail are encouraged to look for mail bearing any number of tell-tale signs that would suggest a potentially dangerous letter or package. If they find anything, they are told to contact the corporate security officer or the local fire department or HAZMAT unit.

While this level of mail screening provides a basic level of protection, organizations seeking to bolster mail center security can add a variety of measures to enhance their operations based on perceived level of risk, tolerance for mail delivery delays, and availability of funding.

## **Enhancing the Basic Receipt and Delivery Process**

Just as an unauthorized person wouldn't be allowed to enter a facility without oversight, no longer can organizations allow unrestricted entry to unknown pieces of mail, overnight couriers or even bicycle messengers.

All mail and package deliveries can be channeled into a single secure area and undergo a centralized and comprehensive screening process. A manual screening and sorting process can separate suspicious pieces. A central point of control will also eliminate any unauthorized persons from entering the facility to make deliveries in work areas.

All packages can be reviewed and approved upon receipt, then released for internal delivery — by internal personnel — only after receiving a special “accepted” stamp. The progress of all internal packages and courier deliveries can be monitored via software that digitally captures signatures and provides a precise and verifiable record of internal delivery.

## **Adding Technology to the Screening Process**

As the need for additional mail center security increases, procedures for handling mail intensify and the technologies utilized become more sophisticated. X-ray technology might be deployed to scan all or a portion of all carrier, courier, U.S. Postal Service mail and parcels upon receipt and prior to eventual internal delivery.

New imaging technologies can be utilized to capture images of suspicious packages, to notify the intended recipients via e-mail — with an attached image of the package — and to receive authorization to permit delivery of the package.

New imaging technologies can be utilized to capture images of suspicious packages, to notify the intended recipients via e-mail — with an attached image of the package — and to receive authorization to permit delivery of the package.

## **Providing Premium Level Security**

Security provisions can be further tightened for offices of elected officials, government agencies or high-profile individuals in television and print media, defense, banking, financial services and other sensitive industries.

All mail and packages can be opened and inspected prior to delivery at a secure on-site or off-site location. Mail can then be delivered physically, or a digital image of it can be captured and sent to the recipient via e-mail.

If a security audit suggests a biohazard risk, special mail processing procedures can be implemented in the mail center and additional types of protective and screening equipment can be added to the facility. These can include:

- Protective clothing and equipment for mail handling personnel
- Secure, self-contained work stations or glove boxes for opening mail
- High-efficiency vacuums and air filtration systems.

Also, a number of advanced mail screening systems can be used to detect biohazards and other substances that would not be identifiable through normal routine mail processing. Screening technology has improved greatly since the original anthrax incidents, and today's systems are much faster, more affordable and more reliable than was the case three years ago. Still, they are most effective when they can be integrated into a secure off-site mail processing center.

*How vulnerable is your company to physical, electronic and biological threats*





## **SAFEGUARDING**

**YOUR**

**MAIL**

**AND**

**DOCUMENT**

**FLOW**



## **SAFEGUARDING**

---

### **YOUR MAIL AND DOCUMENT FLOW**

There are definitive ways to enhance the security of mail throughout your operation.

#### [Look for metered mail](#)

Does the mail piece have a stamp or a meter imprint? It matters. Metered mail is more secure than stamped mail or permit mail, because the identification number on each piece of metered mail is traceable back to the location (and sometimes even to a specific floor of a building) from where it was mailed. Senders of hazardous mail content have used stamps, the postal equivalent of cash. Stamp users and their points of origin are untraceable if the senders don't identify themselves.

Anyone intending to cause harm through a piece of mail would leave themselves vulnerable to identification by using a meter traceable to them — so they don't do it. As issues with mail security continue, both consumers and companies have recognized that metered mail is more trustworthy than stamped mail.

It stands to reason, then: Metered incoming mail is more secure than stamped incoming mail. And for outgoing mail, using your company postage meters helps recipients (including your customers) feel safer.

#### [Consider address management software](#)

For receiving mail from an unknown person or location, address management software is available to help validate return addresses on incoming mail. This software can enhance your ability to detect suspicious incoming mail if a sender uses a non-existent return address.

#### [Investigate tamper-revealing products](#)

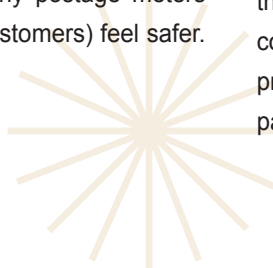
Products such as seals, marks, tapes and encryption technologies can help assure the authenticity of the mail piece and reveal attempts at tampering. Look for them on items you receive, use them on items you send.

#### [Track all mail](#)

The U.S. Postal Service has various systems for securely tracking mail-handling at every step along its route. Companies like Pitney Bowes offer products and technologies that enable recipients to track and trace the mail along its journey.

#### [Identify and remove hazards](#)

New technologies can identify specific hazards such as explosives in unopened letters or packages. And there are processes to validate the security of mail contents from other organizations. Trained mail center professionals can screen out individual letters or packages more likely to contain hazardous content.



There are a variety of ways to remove hazards from mail recipients. One is to have the mail opened and scanned at a secure facility and delivered electronically to the recipient. Another is to remove the hazard from the mail piece, but preserve it for future analysis. A third is simply to destroy the hazard. The choices of which approach to take and which technology to deploy are decisions that require expert advice.

### Filter selectively

Your organization may want to require that incoming mail, documents and packages fit a profile created by the recipient. Systems and processes can be deployed to create that profile and manage according to it.

### Instilling confidence in your customers

There's a solid reason to secure your outgoing mail: It instills confidence in your customers that the mail they receive from you is safe. Nearly every business communicates with its customers via the mail, whether for direct marketing, issuing statements and invoices, or simply maintaining business correspondence. Since a disruption in that process can be damaging to your company's profitability, it makes sense to have the right pieces in place to maintain your customers' confidence in your mail.



To help protect your employees, your business and your customers, you can perform a comprehensive audit of mail center security, followed by action to secure this critical area.

Here are suggested protocols that can help you keep your mail safe:

### Secure your mail center

Mail and document security begins with securing your mail center. The actions you take will depend on many factors: where your mail center is located in the building, how many people work there, how many employees it serves, and the volume and type of mail it processes, among others.

Securing your mail center is not only critical to the security of your employees, but it's also the first and most effective step you can take to instill confidence with your customers. Be mindful of the “three P's” of mail center security:

- **Personnel.** Your mail center is only as secure and dependable as the people who work in it.
- **Place.** A mail center that's accessible to everyone makes it easy for an incident to take place.
- **Procedure.** Procedural checks and balances ensure that mail is handled only by those with the authority to do so.

### Know your employees

A stable, well-trained work force is the foundation of effective and secure mail, parcel and document operations. To help ensure a safe mail center environment, it is essential to have mail center employees who can handle all aspects of mail security. In addition to being gatekeepers of incoming mail, these personnel are privy to confidential information about the company, as well as the private information of employees and customers, including credit card numbers and other financial and personal details.



To ensure the veracity of your mail center employees, you may want to conduct legally compliant background checks of prospective and current employees. That can include criminal background checks, drug screens and previous employment history and reference checks. Authorization in writing from and advance notifications to the employee are legally required for certain reports, screenings and employment actions. Be sure to consult with your legal advisors before proceeding in this area.

### Establish mail center protocol

Appoint a sole individual to oversee the mail and mail center operations, and limit and monitor access by all others. Be alert to and report attempts at unauthorized access. Your mail center protocol can include the following elements:

- **Track and audit mail pieces.** Accept packages only for listed employees, and only from authorized mail delivery personnel with identification. For each piece of mail, create a detailed audit trail that captures each point of transfer. Make special provisions for the safekeeping of valuable incoming items, especially temporarily undeliverable packages. Keep outgoing mail in a separate, secure area until pickup.
- **Secure the postage meter.** Limit usage of the postage meter to authorized users who are accountable for its proper use.

- **Train and re-train.** To maintain a constant state of alertness, all employees should undergo refresher training at least once a year. (As an example, Pitney Bowes provides its employees with initial workforce training and periodic updates on procedures, including a refresher on suspicious letter/parcel identification and security video training.)

### Consider additional security precautions

Certain businesses may require special precautions such as using access control systems with card readers, intrusion alarm systems, surveillance cameras or X-ray screening.

Also be sure your meter is secure. Ensure that only a limited number of screened and trusted employees have access to your meter by locking it in a secure room and giving only those authorized the key. Your meter now becomes the location of final checking of outgoing mail and a final “seal of security”.

### Tell your customers

In the event of a crisis, immediately use both postcards and e-mails to inform your customers and prospective customers about the steps you’ve taken to secure your mail center and the mail they receive from you. If possible, also inform them of any imminent mailings coming from you, such as promotions or offers.



*Is security more or less  
important an issue in  
your company  
today  
than it was 12 months ago?*



**TURNING**  
**TO**  
**THE**  
**EXPERTS**

## TURNING TO THE EXPERTS



With corporate operations fielding concerns that didn't exist just a few years ago, today's executives are grappling with how best to re-address mail center security.

One of the first priorities for an organization seeking to improve mail center security is to have a well-trained, qualified mail center staff. Employees handling incoming mail are an organization's first line of defense, and they can be trained to protect themselves, the facility and the business.

Whether you decide to continue to manage the mail center internally or use an outsourcer for its expertise, safety training programs can be comprehensive and proven effective. They can be based on or similar to those offered to government agencies or other organizations that are considered most "at risk." In addition, mail center employees can undergo rigorous screening, such as background checks and drug testing.

At the very least, organizations are recognizing that a comprehensive audit of their mail stream is in order. After all, parcels and documents enter facilities from myriad sources — U.S. Postal Service, couriers, vendors, etc. — and the typical organization does not have a sole individual who is responsible for overseeing all of it.

To that end, then, they're bringing in mail operations experts, who conduct a company-wide audit of the mail stream and recommend and develop a consistent process to secure the facility against suspicious mail and packages. A secure mail consultant can also provide mail room personnel with training on mail center management.

### **Outsourcing the operation**

Some security-conscious organizations are going one step further. Citing the rising time and capital investments to hire and train employees and run a secure mailroom, they're turning over the operation to outside professionals.

The reasons go beyond the obvious priority of employee safety. The fact is, unless the latest, high-speed screening technologies are employed, a secure mail facility that screens all incoming mail pieces can slow business to a crawl. And for many companies, the costs of that delay can add up quickly.

Take the example of a financial services company with a daily inflow of 100,000 mail pieces, many of which contain payment checks. A tedious screening process could delay payment processing for two to three days or more — with significant float consequences.

"A hundred thousand envelopes with checks in them is real money for any size company," says Dr. Robert F. Hahn II, VP of Strategy & Secure Mail Solutions for Pitney Bowes Management Services. "A high-quality outsourced mail screening solution can accelerate the screening and clearing process, and save considerable costs."

An outsourced mail operation assures companies of experienced and well-trained employees, rigorously designed processes, and specialized technologies, such as dMail imaging of incoming mail. And an outsourcer's cost of screening incoming mail for a year is typically less than the cost of shutting down a facility for given periods of time.

*Is your company's incoming mail  
sorted and/or inspected at an*

*offsite*

*location other than the main  
facility where the majority of your  
employees work?*



**LEADING  
IN  
TIMES  
OF  
CRISIS**



## LEADING IN TIMES OF CRISIS

It's human nature: In a crisis, people are desperate for facts. If those facts don't come from an authoritative source, history has repeatedly shown that the information vacuum will be filled by fact's evil twin: rumor.

Today, with traditional rumor-mongering accelerated by the Internet, business-disrupting events, natural or otherwise, can quickly become a situation that is unproductive, or even out of control. To protect both the physical and mental welfare of your employees and the integrity of the business, company leaders must communicate accurate information to the workforce.

With leadership and communication, even a crisis can become a manageable situation. Here are musts for an effective communications strategy:

### Never delay

If there is one key to successful crisis communications, it's speed. Communicate what you know, even if you don't have all the information for a full briefing; in a crisis situation, responsive leadership can be reassuring.

### Get the word out — way out

Use every form of communication — memos, e-mails, company-wide e-broadcasts — and best of all, if possible, personal contact. During a crisis, **now** is the time for management leaders to be seen and heard.

### Project calm

Your employees will be watching you for any sign of fear or confusion. Communicate confidence and assurance.

### Be forthright

The more information people have, the more limited the opportunity for rumors and fear. Divulge everything you know, and admit what you don't. During crises, there's no time for parsing or playing corporate politics.

### Say what you've done

Inform employees of actions underway to address their safety. This will help them re-focus on their work.

### Allow time for questions and suggestions

People feel better when they have an opportunity to express themselves. Acknowledge the crisis and create a climate of acceptance for the range of reactions to it.

### Offer assistance

Ask management and supervisors to be alert for signs of emotional impact. If counseling is called for, make it available to those who need it. Help employees with transportation or other emergency arrangements.

### Be understanding

Make allowances for less than peak performance, to allow employees to cope and to avoid accusations of managerial insensitivity.

*Does your company have a  
Chief Security Officer  
(CSO)?*



**BUILDING**

**A**

**CRISIS**

**TEAM**



## BUILDING A CRISIS TEAM

When business disruptions occur, it's often too late to begin constructing a crisis management team. That can take place now. With a top-notch crisis team assembled in advance, a crisis can be quickly and effectively managed — or even averted. The existence of a trained, prepared crisis team following established crisis-management procedures can significantly limit the risk to your employees and business.

### What does a crisis team look like?

Experts agree that the most effective crisis teams are trained in advance, and able to act quickly, and as small as possible.

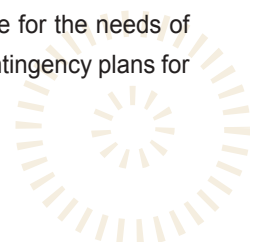
### What is the personality profile of a highly effective crisis team member?

Experienced. Ability to remain calm under pressure. And a personality that breeds respect, authority and compliance.

### Who comprises a crisis team?

Certainly, the nature of your business will determine the composition of your team. (If your business involves chemicals, for example, an environmental specialist would be critical to the team.) But here are the most common participants:

- **Chief Executive Officer and/or Chief Operating Officer.** An ultimate decision-maker who can determine and prioritize appropriate actions.
- **Chief Information Officer.** A technology person familiar with company systems and processes.
- **Chief Financial Officer.** An advisor who can judge the costs and risks of any potential action.
- **Chief Security Officer.** A professional with experience in investigation, reporting and enforcement.
- **Human Resources.** A person who can advise on all matters pertaining to your employees.
- **Medical.** A doctor or other health professional to advise on medical matters impacting employees or the public.
- **Legal.** A counselor who can offer a legal perspective on the ramifications of various courses of action and advise on liability.
- **Public Relations.** Someone experienced with external communications who can maintain the integrity of corporate statements.
- **Investor Relations.** A professional who understands how the market might react to a crisis in your company and who can communicate with security analysts and other stakeholders.
- **Internal Communications.** A person who can create and craft messages quickly to communicate to employees, as needed.
- **Sales and Marketing.** An advocate for the needs of the customer who can formulate contingency plans for maintaining revenue.



## Integrating corporate functions

The new security environment has created a convergence of the responsibilities of a wide range of corporate functional groups. IT, Security, Environmental Health & Safety, Facilities Management, Administrative Services, and multiple other organizations and operating units are collaborating to analyze potential threats to business operations.

Then, based on that analysis, they're developing integrated disaster recovery and business continuity plans to protect employees and enable the business to serve its customers during emergency situations resulting from terrorist attacks or other disruptions.

## Extending the team outward: public/private cooperation

Once an internal crisis management team has been assembled, a wise move is to extend your efforts beyond the four walls of your facility — that is, to the community. Since the formation of the U.S. Department of Homeland Security (DHS), significant emphasis has been placed on expanding communication and planning between corporations and the communities in which they do business.

Local community “first responders” are visiting corporate facilities, reviewing security and emergency preparedness plans in place there. They're working closely with company security, facility management

and environmental health and safety representatives to outline specific requirements in response to a variety of possible terrorist scenarios.

On a broader scale, DHS has also been establishing organizations and activities to encourage closer public-private interaction at the national level. The Protected Critical Infrastructure Information (PCII) program enables the private sector to voluntarily submit infrastructure information to the federal government to assist the nation in reducing its vulnerability to terrorist attacks. DHS has also created Information Sharing and Analysis Centers for a wide range of industries, including agriculture, food, water, public health, emergency services, government, information and telecommunications, energy, transportation, banking and finance, real estate and the chemical industry.

And DHS launched a Ready Business website [<http://www.ready.gov/>] to help owners and managers of small to medium-sized businesses prepare their employees, operations and assets in the event of an emergency.



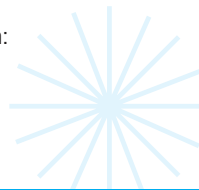
For more information on mail security from some of the foremost authorities on the topic, refer to the links below.

FBI Advisory Handling Suspicious Mail  
Illustrated guideline for suspicious mail  
<http://www.fbi.gov/pressrel/pressrel01/mail3.pdf>

U.S. Department of Health and Human Services:  
Biological Incidents: Preparedness and Response  
<http://www.bt.cdc.gov/agent/ricin/index.asp>

Health Information Center for Disease Control (CDC):  
Health Alerts, Advisories, and Updates;  
Information on Anthrax  
<http://www.bt.cdc.gov/>

American Psychiatric Association:  
Coping With a National Tragedy  
[http://www.psych.org/public\\_info/](http://www.psych.org/public_info/)



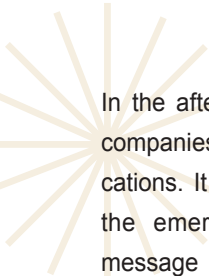


**RECOGNIZING  
THE  
PAPER/DIGITAL  
PARTNERSHIP**

## RECOGNIZING THE

# PAPER/DIGITAL

## PARTNERSHIP



In the aftermath of the 2001 anthrax attacks, some companies considered moving to all-digital communications. It was tempting to assume that, because of the emergence of digital electronic messaging, message security issues could be addressed by a complete and immediate move from physical mail to pure digital, electronic communication.

That strategy quickly proved to be misguided. Individuals, organizations and societies overly dependent on electronic communications have quickly discovered that they haven't reduced security risks, but have simply traded one set of risks (biohazards and other dangerous substances) for another (viruses, worms, hackers, spyware, etc.).

The reality is that physical and digital mail share a co-dependent business relationship. Some physical mail volume is stimulated by e-mail, and vice versa. According to findings in a recent study conducted by Vishal Chopra of Pitney Bowes Corporate Strategy Group, "It is commonly understood that Internet adoption has substantially changed media usage by displacing other media, yet several studies point to the Internet as improving the efficiency of users to consume more media, and note that the Internet is utilized in addition to other media. The latest studies show that the 'most wired' people are actually receiving more mail. Historically, mail volumes have continued to grow slowly over time in spite of the introduction of competitive media."

For example, the Internet has increased the need for package deliveries. It has also increased the need for direct mail to help drive customer traffic to a specific Web site. E-mail notification of direct mail campaigns can increase the likelihood that direct mail will be opened when it arrives. Synergies are gained by using the inherent properties of paper and digital communication to their best advantage.

Also, as high-quality customer service becomes a greater determinant of business success, executives are asking customers how they wish to receive their bills, statements and other messages — via mail or e-mail. Digital document delivery systems give mailers the flexibility to deliver messages in paper or electronic form, based upon the recipient's needs and preferences.

Corporate America is comfortable with a balance of physical/digital mail for another reason: paper-based mail has certain advantages for large segments of our population — universality, ease of access and use, portability, tangibility, privacy and ease of crediting the source of the message.

Lately, physical mail has been adapted to take advantage of the capabilities of electronic communications. One compelling example: employing hybrid mail/e-mail communications, in which a single message is delivered electronically to eliminate geographic and time barriers, followed by a paper-based rendering of the message at the point of receipt. Another example is the ability of the Internet to track the movement of specially tagged letters and packages.

Harnessing and balancing the unique advantages of physical and electronic mail can unlock new ways of building relationships with customers.

*What steps has your  
company taken to improve*

*security*

*over the past two years?*



**TURNING  
TO  
PITNEY BOWES  
FOR  
MAIL SECURITY**



## TURNING TO PITNEY BOWES FOR MAIL SECURITY

We live in challenging times. To help protect against the possibility of a business-disrupting event, Pitney Bowes has developed a full array of mail and related security products and services, ranging from simple security solutions for small and mid-size companies to custom solutions for large enterprises and high-risk organizations and situations.

As the global leader in mail and document management, Pitney Bowes has developed a set of best practice guidelines for mail center security. We have the expertise to provide the levels of security appropriate for various mail, document and/or package streams in your organization. We are also uniquely qualified to analyze your mail and document management processes, and then develop a business plan to help your organization gain optimal security, quality and cost-effectiveness.

### **Of security and snake oil**

Amid the anthrax paranoia of 2001, upstart mail security companies and solutions sprang up like so many mushrooms. Some solutions worked; many were the postal equivalent of snake oil.

Even some legitimate solutions of three years ago are no longer sufficient to detect today's biohazards and chemical threats. As a result, the U.S. Department of Homeland Security has funded research on new and enhanced document screening techniques and products.

"These new solutions can help detect anthrax, ricin and explosives in mail processing centers that process a million pieces per day," says Dr. Robert F. Hahn II, VP of Strategy & Secure Mail Solutions for Pitney Bowes Management Services. "That's a capability that clearly didn't exist just a couple years ago."

Pitney Bowes has leveraged its unparalleled experience and patented technologies to organize, streamline and greatly increase the security of corporate mail and document operations. During the anthrax scare, we developed a response and solution that was rapidly implemented by government agencies and many enterprises that is still in use today.

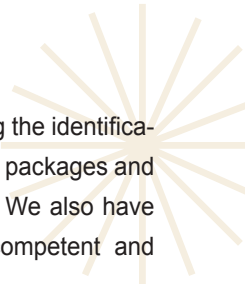
Secure, cost-efficient mail handling and document management have long been a core competency of Pitney Bowes, a company with over 80 years of expertise dealing with all aspects of the mail industry, from mail center management to secure electronic funds management.

Our services are an integral part of our customer mail centers throughout the world. From small businesses to some of the largest corporations and governmental organizations, we have built a base of intelligence and knowledge that is proving invaluable in developing best practices for today's security needs.



### **Research and development**

Pitney Bowes invests more in mail security research and development than any other company in the



industry. With more than 3,500 patents in our portfolio, we are one of the top 200 corporations receiving U.S. patents each year.

Pitney Bowes Advanced Concepts and Technologies (AC&T) labs in Shelton, Connecticut create concepts and develop prototypes of new products and services for Pitney Bowes and our clients. The Secure Systems group provides expertise in all aspects of secure systems, developing technology-based product concepts that include encryption, authentication, digital signatures, key management, fraud analysis, secure protocols, access control, tamper protection and trusted systems.

Among Pitney Bowes solutions for enhanced mail and document security are:

## **Mail Center Management Services**

### **Audits of mail and document management systems**

Pitney Bowes can provide a comprehensive audit of your entire enterprise or a specific mail center, mailing hub, division or department. An audit is usually an excellent first step to help you understand where you are and outline what is needed to achieve your security objectives.

### **Outsourced secure mail centers**

Many companies prefer to outsource their mail centers for operational efficiency and cost savings. Pitney Bowes is a leading choice, managing hundreds of mail centers worldwide. Our outsourcing may be done on- or off-site, depending upon the sensitivity of your incoming and outgoing mail. Whether you choose to set up your own off-site facility or take advantage of one of Pitney Bowes facilities, we can provide a full range of advanced mail screening solutions to enhance the security and continuity of your business.

### **Employee screening and training**

As part of our Mail Center Management, we conduct the most rigorous employee screening process in the industry. Our initial training is also unparalleled, with continual updates on the latest guidelines and procedures. We can train your employees to better

secure their mail environment, including the identification of potentially hazardous letters and packages and protocols for handling suspicious mail. We also have effective strategies to retain highly competent and knowledgeable employees.

### **Customized mail center security procedures**

Every company has its own specific business needs. We design specialized security procedures to meet each of them. We can also help you select and integrate the best security technologies for your particular requirements.

### **Ergonomics to minimize mail handling**

We have developed techniques and equipment to help companies optimize and reduce the number of procedures involved with handling mail, increasing the efficiency of their operations.

## **Imaging and Document Management Services**

### **Secure document imaging**

For efficient and secure distribution of your incoming mail and internal documents, Pitney Bowes can digitize and distribute your information throughout your network. Our document security measures help ensure that your data remains protected, whether it's accessed from within your organization or from outside your network. Imaging also reduces on-site storage costs.

### **Document production and distribution**

Implementing an effective document strategy can help your business process and deliver documents at a moment's notice — when, where and in the quantity and quality required. With our experience in document processing, we can evaluate and recommend secure, cost-effective solutions, including print-on-demand, reprographics, e-mail and fax networks to improve your corporate communications.

## **Business Continuity & Recovery Services**

In the event of a disaster, Pitney Bowes can provide you with a backup "hot site" to ensure that your key business operations continue. Our 50,000-square-foot,

state-of-the-art Business Recovery Center (BRC) in Shelton, Connecticut is one of the largest in the world.

With capacity for a million mail pieces and 5 million print images, this dedicated facility offers high-speed variable print-on-demand capacity to route electronic data streams and print and send invoices, statements and other high-volume correspondence.

In addition to advanced print and mailing technologies, the BRC is manned by highly qualified technicians who can implement a recovery plan with full-service print, mail and finishing. We can help you avoid the costly penalties and regulatory actions that can result when critical documents don't reach your customers in time. Working together with your team, we conduct risk assessments and impact analyses covering financial loss, loss of customer confidence and damage to reputation, as well as worst-case scenarios.

One call activates your plan and Pitney Bowes goes to work:

- Preparing the site for you
- Configuring the equipment for your applications
- Establishing data communications
- Coordinating supplemental staffing
- Notifying U.S. Postal Service officials.

## Mail Processing Systems

Pitney Bowes mail processing systems are the most sophisticated in the world, completely automating the mail process to print, address, feed, weigh, seal, meter and stack mail in one continuous stream.

Mail security processes are built into many of our systems to minimize human exposure to mail operations. Mail tracking and customized reporting provide reassurance to recipients through the use of metering and seals that protect the contents of an envelope. We can consult with you on the products and services that will best serve your needs — for efficiency, productivity, cost reduction and, of critical interest today, security.

### Metering for identification

Our meters, licensed by the U.S. Postal Service, are

on file. Since every meter indicia contains the licensee number, you can identify the point of mailing for every piece of mail. We were the first to develop "intelligent" digital metering that provides sophisticated, targeted and encrypted information about each mail piece.

### Tracking and delivery management solutions

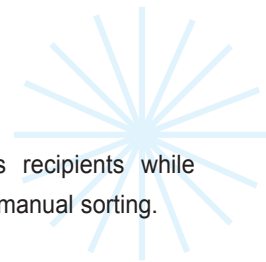
Having information about your delivery is key. Pitney Bowes DeliverAbility™ Enterprise Package Management is a desktop shipping tool that lets your employees complete shipments without mail center assistance. It enforces carrier-use rules while controlling costs across the enterprise with time-saving tools that provide shipment visibility and policy compliance.

Pitney Bowes Arrival™ software automates internal routing from point of delivery to final recipient, tracking a package through every stage with electronic signature confirmation.

No matter what you ship, Ascent™ mail center management software can send it quickly and more cost-effectively, with total accountability that includes e-mail and fax shipment notification, as well as retrieval of package delivery status from carrier Web sites. Account and Mail Management Systems help you track operations and provide postage security through password protection, including a "Meter Discrepancy Report."

Combining our DM™ Mailing System with your Internet connection, you can connect to Pitney Bowes Confirmation Services Network. It gives you electronic access to USPS Certified Mail Delivery and Signature Confirmation Services, so you can track and confirm your mail's journey from sender to receiver.

We also offer mail processing solutions for incoming and outgoing mail, sorting through an innovative and flexible software-based product offering of Multi-Line Optical Character Recognition (MLOCR) sorters, encoding and voice recognition systems, as well as Internet-based track and trace applications.



### Sealing technologies

Pitney Bowes has patented a number of tight, secure seal processes. These include our Nomex process, which lets you create a positive, even seal while you meter and stack 60 to 80 pieces a minute. Secure sealing has been integrated into our analog and digital machines.

### Encryption technology

Pitney Bowes DM™ mailing systems offer encryption technology through digital printing of postage imprints. Digitally encrypted meter indicia satisfy all current postal regulations while ensuring flexibility and adaptability for the future.

### Addressing and production quality

AddressRight™ products print addresses on envelopes, creating a professional look that builds confidence with your customers and make your marketing mailings more effective. It also helps ensure that your mail will reach the right recipient, correcting addresses against the 110 million address-range United States Postal Service regulations while ensuring flexibility and adaptability for the future.

SmartMailer™ software, which helps ensure the correct address and bar coding, produces a professional look to inspire the recipient to open your envelope.

Our newest inserters include sophisticated Optical Mark Recognition (OMR) scanning capabilities that read most OMR marks. PB FIRST™ Document Processing Software also provides OMR capabilities that help companies deliver the right information to the right addresses — particularly important in the production of bank statements, security packages, medical information, etc. Seamless integration of our folding and inserting equipment with our sophisticated software solutions helps automate processes to insure optimum security and integrity of your flow of communication.

The Mixed Mail Manager (M3™) solution automates your incoming mail process, providing increased productivity, efficiency and security. Information from powerful reporting software maintains tight control

of costs and accurately identifies recipients while reducing delivery time by replacing manual sorting.

### Enhancing the quality of direct mail

Pitney Bowes production mail products and services, such as Advanced Production Systems (APS), meet the needs of high-volume transaction-based documents such as invoices, statements and targeted 1-to-1 marketing messages. We provide hardware, software, professional services and system integration and related maintenance support and financing options. And OnRoute tracks and traces the entire document management process from point of job receipt to distribution.

### Electronic document delivery

For businesses considering combining digital document delivery in with physical documents, Pitney Bowes offers advanced solutions through our Group 1 offering. This solution enables companies to deliver bills and statements electronically without disrupting or rewriting existing applications and fosters greater employee and consumer physical safety at a lower cost than additional safety/security measures in mail centers.

### Financial services

With operations and facilities now being scrutinized, audited and restructured, you may need to upgrade your technologies or other mission-critical equipment. Many of our customers are asking Pitney Bowes for financing solutions to help them acquire the equipment, facilities, products and services they need. Our sophisticated financial services group can provide flexible financing options for large enterprises, municipalities and small and mid-sized businesses.

To learn more about how these solutions can benefit your organization, please visit [www.pb.com/security](http://www.pb.com/security) or e-mail us at [pivotalthoughts@pb.com](mailto:pivotalthoughts@pb.com).



**BEYOND**

**THE**

**ENVELOPE**

**AN ONGOING SERIES**

**OF EVENTS FOR**

**SENIOR-LEVEL EXECUTIVES**

# BEYOND THE ENVELOPE

## AN ONGOING SERIES OF EVENTS FOR SENIOR-LEVEL EXECUTIVES

*Pitney Bowes "Beyond the Envelope" events bring together senior-level executives with America's business thought leaders to explore today's most timely business topics. Here are some recent and upcoming events. To learn more about these and other Beyond the Envelope events, log on to [www.pb.com/executiveview](http://www.pb.com/executiveview).*

### **The Importance of Global Communication: Forbes Dinner and Conversation**

Businesses around the globe need solutions that enable them to cut costs, improve productivity, manage funds more securely and, most importantly, build customer loyalty. Reducing the risk of turnover for high-value customers has become mission-critical, and more and more organizations are turning to Pitney Bowes for answers.

Pitney Bowes and *Forbes* magazine recently co-hosted a dinner for senior-level executives around the country. Discussing the importance of global communication was a distinguished group of panelists, including: Steve Forbes, President and Chief Executive Officer, Forbes Inc.; Murray D. Martin, President and Chief Operating Officer, Pitney Bowes Inc.; and Brian M. Baxendale, Senior Vice President and President, Enterprise Relationship Development, Pitney Bowes Inc.

### **Marketing Has the Right NOT To Remain Silent: Webinar with Peppers & Rogers Group**

CAN-SPAM. Do Not Call lists. TIVO. E-mail filters. In an environment of barriers, how can companies best communicate with their customers? A recent Webinar, "Marketing Has the Right NOT to Remain Silent," focused on the importance of the mail channel and best practices of leading companies who are effectively using direct mail, integrated marketing and advanced metrics to achieve better communications flow.

The Webinar featured a roundtable of leading experts, including: Don Peppers, Founding Partner, Peppers & Rogers; Michele Bottomley, Chief CRM Strategist, OgilvyOne; and Neil Metviner, President, Pitney Bowes Direct.

You can view an archived version of this Webinar at [www.pb.com/voice](http://www.pb.com/voice).



### **Driving Corporate Innovation: Fortune Innovation Forum Breakfast**

The Fortune Innovation Forum will mark the culmination to the year-long celebration of the Fortune 500®. The program will offer an in-depth look at the innovative corporation from three perspectives:

- Leading innovation at the top, featuring CEOs' views on leadership, management and people issues related to fostering innovation.
- Implementing innovation on the front lines, featuring C-level experiences from product, process and marketing areas.
- The impact of globalization, international and national policies on innovation.

Pitney Bowes will host this private breakfast for senior-level executives attending the Forum on November 19, 2004. The event will feature James Euchner, Vice President of Advance Technology and Chief e-Business Officer for Pitney Bowes Inc., as well as Clay M. Christensen, renowned Harvard professor and speaker, who will showcase his new book, "Seeing What's Next: Using the Theories of Innovation to Predict Industry Change".



## **PITNEYBOWES:** **ENGINEERING THE FLOW OF COMMUNICATON**

Pitney Bowes is a world leader in integrated mail and document management, working with nearly all the FORTUNE 500 companies, developing processes and technologies for cost efficiency, security enhancement and improved customer communications.

By engineering the flow of communication, we provide solutions to two of the most important challenges facing management today: how to cut costs and boost productivity inside the organization, and how to grow revenue outside it. To these ends, we offer unique capabilities for engineering the processes, technologies and financing that help business-critical communication flow more efficiently within the organization — and work more effectively outside it.

Linking paper to digital formats, mail and transactional documents to customer response and relationships, our solutions continue to impact higher and higher value processes in the communication chain.

Helping companies simplify and manage their complex mail and document processes, Pitney Bowes can reduce costs, increase impact and enhance customer relationships. More than 80 years of technology leadership has produced many major innovations in the mail and document industry, as well as more than 3,500 active patents with applications in a variety of markets, including financial services, government, manufacturing, printing and marketing.

## About Dr. Robert F. Hahn II



Robert F. Hahn II is Vice President of Strategy & Secure Mail Solutions for Pitney Bowes Management Services (PBMS). He develops and implements the long-term global business strategy for PBMS, with a special emphasis on business process outsourcing solutions and vertical market applications. He also leads the Pitney Bowes team that creates and delivers a full range of secure mail solutions for government and commercial customers.

Prior to assuming his current position, Dr. Hahn was President of Pitney Bowes Government Solutions (PBGS), a wholly owned subsidiary of Pitney Bowes Inc., providing outsourced mail, document management, facilities management and distribution services to federal government customers throughout the United States.

In 2000, as Director of Futures Strategy, he was responsible for developing the company's understanding of the long-term business and technology trends shaping the future of the mail and document management industry. He has also served as Director of Accelerated Growth, Director of the company's Business Continuity Planning Group and Chairman of its Emergency Preparedness and Crisis Management Team. He also co-chaired the Security and Crisis Management Council for SACIA, the Business Council of Southwestern Connecticut, an organization that includes senior security officers of Fortune 1000/500 companies like GE, Xerox, UBS, Purdu Pharma, PWC, and others.

Prior to joining Pitney Bowes, Dr. Hahn served 22 years as an Infantry Officer in the U.S. Army, retiring in 2000 with the rank of Lieutenant Colonel. A 1979 graduate of West Point, he served in a variety of command and staff assignments in the U.S. and Europe. He was a counter-terrorism instructor, served on the NATO staff in Europe, taught American politics and defense policy at West Point, and managed the Army Strategist Training Program at Fort Leavenworth, Kansas. He completed his Army career as Senior Strategist with the Army After Next Project, where he focused on creating the operational concepts, military organizations, weapon systems and technological improvements needed to transform the Army for global operations beyond the year 2010.

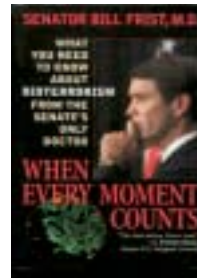
Dr. Hahn holds a Ph.D. in Government from Cornell University and a Master of Business Administration degree.

**TWO GREAT  
LIMITED-TIME OFFERS,  
COMPLIMENTS OF  
PITNEY BOWES**



*As a subscriber to Pivotal Thoughts, you're invited to receive a copy of two enlightening publications addressing corporate security, with our compliments.*

***When Every Moment Counts: What You Need to Know About Bioterrorism from the Senate's Only Doctor*** by U.S. Senator Bill Frist (R – Tenn.). Senator Frist brings his experience as a heart and lung surgeon and ranking member of the Senate Subcommittee on Public Health to this informative and approachable guide to coping with bioterrorism threats.



***Pitney Bowes/BusinessWeek Research Services Survey Security White Paper*** by Kevin R. Hopkins. This valuable White Paper delivers and interprets findings of the August 2004 survey of senior-level corporate executives, shedding new light on American business's views on corporate threats and how they're being dealt with.

*To receive these free publications, please visit [www.pb.com/pivotalthoughts](http://www.pb.com/pivotalthoughts) or call 1-866-DOC-FLOW today.*



*Engineering the flow of communication™*

Pitney Bowes Inc.  
World Headquarters  
1 Elmcroft Road  
Stamford, CT 06926-0700 US  
Telephone: 1-866-DOC-FLOW  
[www.pb.com/pivotalthoughts](http://www.pb.com/pivotalthoughts)