



## Lost in the Mail?

# Why You Should Plan for Print-to-Mail Recovery

*by: Nicole Ross*

**Pages: 17-20; March, 2002**

文章简介: 本文介绍了丧失打印转发邮件能力可能给机构造成的影响, 深入分析了评估该风险和恢复该能力所需考虑的问题和可能采用的方法。



[华安信达](http://ChinaCISSP.com)

After 40 years of being in business, K-Mart — now facing \$10 billion in debt, hundreds of store closings, and throngs of unhappy customers — has become the largest retailer to ever file for bankruptcy protection. An Msn.com column states that in October 2001, as part of CEO Chuck Conaway's enterprisewide plan to turn K-Mart into an everyday low-cost destination, advertising was cut by as much as 50 percent. The result? Sales dropped by as much as 5 percent almost immediately, according to DSN Retailing Today, because K-Mart relinquished their Sunday newspaper circulars. Although traffic during the week improved somewhat, weekend customers stayed away.



“They cut back mass advertising too quickly,” says Frank Badillo, senior retail economist at Retail Forward (Columbus, OH). “Customers were expecting advertising circulars every week and reacting to them. K-Mart needed to overlap strategies for a longer time.”

This example illustrates the financial catastrophe that can result when a company fails to reach its consumer base, which relies heavily on paper-based mail pieces.

High-volume paper documentation — in the form of invoices, marketing materials, statements, policy notices, and payroll — is generally associated with health care institutions, insurance companies, financial or credit establishments, utility companies, and government agencies. Yet, virtually every company sends out invoices, statements, and other critical documents that communicate information to current or potential customers and stakeholders.

Critical mail applications can be interrupted for many reasons — inability to access a facility, print-to-mail equipment failure, power outages, loss of document-dependent data — and, in the meantime, financial stability, employee productivity, and reputation can be damaged as a result of that interruption. Not only must organizations back up their data, but they also must ensure the continuity of their print-to-mail operations.

### **Why Print-to-Mail Recovery?**

A business' cash flow mostly relies on paper processing — accounts receivable invoices, accounts payable checks, and employee payroll checks — for financial stability. Also, as organizations are subject to state and federal regulations — insurance cancellations; bank, tax, and investment statements; transactions with utility companies; as well as best practices, due diligence requirements, and stakeholder protection precautions — there must be plans in place to ensure these vital services are carried out.

“When print-to-mail operations do not perform and statements and checks are not delivered on time, businesses not only face interruptions to their cash flow, but expose themselves to fines and penalties from regulatory agencies, such as the SEC or state-controlled insurance regulators,” says Nick Kopernik, director of Pitney Bowes Business Recovery Services (Stamford, Conn.). “For large operations that have 10 or 20 million dollars in the billing stream, any delay in getting the information out on time can result in financial losses of hundreds of thousands of dollars.”

In addition, many daily business processes — such as financial and production reports, training manuals, explanation of benefits and corporate procedures, and routine business correspondence — ensure a continuity of operations. As businesses continue to rely heavily on the mail piece as their primary communications tool to reach current and potential customers, the inability to do so can easily create a negative perception in the minds of stakeholders who demand

operational superiority, says Kopernik.

If an organization experiences a business interruption — from extensive facility damage, to a power outage, to print-to-mail equipment failure — customers, business partners, and shareholders still expect product output to remain the same, regular business functions to continue, and documents to be printed and delivered. In short, organizations are expected to back up their business-critical operations so that production remains watertight.

For the business continuity team at PFPC Inc.'s Advanced Output Solution division (Lynnfield, Mass.), losing their print-to-mail capabilities is not an option. PFPC provides services for mutual funds companies, including print-to-mail services, digital archive, Internet presentment solutions, transaction processing, compliance, tax accounting, and customer support.

"Clients expect PFPC to satisfy all of their distribution requirements, regardless of events that could prevent this. For us to be competitive, it's necessary to have an effective continuity plan," states Barry Crawford, vice president of operations. "In the sensitive mutual funds, financial services, e-banking, and e-commerce industries, our company and clients expect us to operate without any obstacles or degradation of services. At all times we're trying to maintain continuity because of our reputation, legal requirements, and the sensitivity of the documents [we produce]. Operations should be seamless to the customer."

### **Assessing Risk**

The development of an effective print-to-mail recovery plan is an individual and strategic one for each organization, and often, recovery costs will play a key role in determining what plans are put in place.

Companies must first determine which print-to-mail applications should be backed up. Since this will vary from industry to industry, and from organization to organization, companies should complete a thorough business impact analysis (BIA)

to identify business-critical applications, evaluate and allocate values to the risks associated with those applications, and then discern the level of protection needed. According to Gerald Montella, vice president of sales and marketing at Mail-Gard Concepts Inc. (Warminster, Pa.), all relevant departments — such as payroll, accounts payable and receivable, legal, auditing, human resources, public relations, security, etc. — should be involved to evaluate impact and set recovery priorities and RTOs for each potential application.

When examining each critical application — most likely documents that affect cash flow or are bound by specific requirements, penalties, or government regulations — companies must determine the expertise required to complete the job, as well as the volume and timing requirements for each. However, Kopernick stresses that volume should not be the determining factor in deciding what recovery services are required. For example, it may be necessary for a utility company to process statements to be mailed to customers who have pending discontinuances of service. Even though the volume of these may be extremely small, there are penalties for not mailing them in a timely manner.

The BIA should be instrumental in choosing the appropriate print-to-mail recovery solution. Weighing the potential risks against the recovery resources available will allow a company to see if the selected plan will be sufficient.

### **Flexible Recovery**

Fortunately, as organizations give print-to-mail a higher priority, the options for flexible plans have increased as well. According to Montella, 20 to 30 years ago the concept of print-to-mail recovery was almost nonexistent, and the recovery process consisted of creating a 'temporary facility' — locating available floor space, hiring temporary labor, and installing similar equipment. The introduction of continuous-form printing and inserting, two-wide and duplex printing, as well as roll paper feeders and rewinders streamlined the print-to-mail process and greatly reduced "per envelope" costs.

Complex print software products and intelligent barcode technology allowed corporations to downsize staff and facilities, automate print management, and track documents. However, these great strides brought about more changes: the need for specialized print-to-mail facilities, customized equipment, highly trained technical staff, longer lead-time telecommunications, and advanced software. Companies today are therefore faced with the same volumes of print-to-mail applications, but with less equipment to complete production, and no backup equipment in case of an emergency.

The availability of proven print-to-mail recovery facilities aids organizations as they combine solutions for sophisticated data backup and recovery with the continuance of print-to-mail applications. Below are options for companies to consider.

#### *Dedicated Print-to-Mail Recovery Sites*

These hot sites can offer high-tech equipment that's ready to be used as soon as companies start the recovery process. Such sites can potentially avoid disruptive lead times of up to six months, typical when replacing specialized mail-inserting equipment. Subscriber fees cover availability, space, equipment, and services of fully operational facilities maintained by independent providers. Kopernick recommends that companies visit potential sites to ensure that in fact the facility is a true dedicated disaster recovery hot site, one that is continually up and running — this guarantees that the site is capable of being operational on short notice to meet clients' requirements.

#### *Excess Capacity Offerings*

Print-to-mail facilities offer operational resources and time beyond their normal workload in order to accommodate disaster recovery. This type of offering can be dependent on a "first come, first served" basis, though, so if the region is hit by a natural disaster or massive power outage, other customers may receive a higher priority. In addition, some vendors offer partial recovery options, in which

companies back up only some of their recovery needs. Less expensive than a hot site arrangement, this solution may fit well with a company's budgetary or production requirements.

### *Reciprocal Agreements*

Companies with similar print-to-mail requirements and equipment can form contracts to support each other in disaster recovery. However, according to Montella, potential problems associated with this option include differing equipment and workloads and the inability to incorporate the additional production.

### **Comparing Vendors**

Expertise and experience in the areas of communications, print platforms (i.e., mainframe, midrange, server environments), print formats (AFP, Metacode, PCL, postscript), all printing systems (cut sheet, continuous MICR, and color), and inserting and finishing systems (barcodes, select and standard inserting systems) are essential when choosing a vendor, stresses Montella.

"Many people not familiar with print-to-mail operations tend to underestimate the level of complexity involved in things like IBM-AFP streams versus Xerox-Metacode, font sizes and types, signature block requirements, or finishing the mail piece with folds, inserts, perforations, et cetera," says Bill Rider, disaster recovery coordinator at Johns Hopkins Hospital (Baltimore, Md.) and a member of CPM's Editorial Advisory Board. "The print-to-mail side of the business represents an 'operations' environment very distinct from the traditional data center environment, but one that is just as important and complex."

A vendor should be equipped with up-to-date technology and equipment that can efficiently replicate their clients' specific environments. As companies' operational needs change, successful vendors should be able to provide a flexible printing and inserting platform.

In considering an alternate site's proximity to your facility, Rider notes that it

usually will not pose a problem if the vendor can accept e-transferred data. It's still important to inquire if the vendor has the telecom equipment and bandwidth to accept high-volume file transmissions. Of course, there may be instances in which a company will want members of their BC team to oversee the print-to-mail operations, in which proximity will factor in the decision. In addition, the vendor should have access to major data hot site providers so that data can be successfully transmitted to the facility.

When considering location, it's important to assess the risks posed by regional hazards — flooding, earthquakes, tornadoes, etc. — as well as sites that are served by the same electrical power grid or communications services as the primary facility.

Choosing a vendor well versed in postal regulations and procedures is a must. In addition, check the vendor's proximity to the post office and postal service inspectors. Ensure that the vendor's local post office can process a sudden, high volume of mail.

A vendor should also be equipped with uninterruptible power supplies in case of a power outage at the alternate site; climate control and fire detection/suppression systems; adequate telecommunications support; storage space to warehouse printed stock on site; and a high level of onsite security, including key access, camera systems, and bonded personnel.

Finally, vendors should have sound internal business recovery plans of their own. Pre-testing at the vendor site can ensure that their recovery plans and operations are well designed and reliable. This will also clear up any issues with data transmission, printer format, inserter barcode issues, etc. Experts recommend testing at the recovery site at least four times a year.

### **What to Tell Vendors**

Vendors will need to know the specifics of a company's critical applications: the

results of the BIA; monthly print volume and number of documents rendered; number of pages per envelope; number of computer program applications and their sizes; how many employees work on each application; peak process and turnaround times associated with production; and the typical mailing cycle, including how the mail is shipped (i.e., first or second class).

To effectively mirror or acceptably modify a potential client's print-to-mail process, a vendor will ask what the client's normal print-to-mail production process is, the type and quantity of equipment used, and any processing requirements, controls, or auditing trails associated with each application. In addition, vendors recommend that clients maintain a print-ready data stream to ensure a higher level of security and to prevent errors when processing the data. Vendors will ask which, if any, third-party service providers manage potential clients' data recovery.

An organization will need to supply the vendor with a sample mail piece, determining beforehand the minimum requirement for its appearance (i.e., color requirements, number of inserts, font sizes and types, document size). As a guideline, Rider suggests asking the question: Does appearance matter as long as the piece gets out, or does the mail piece have to conform to the company's regular correspondence (i.e., colored logo, inserts) to avoid the risk of sending the wrong message to the customer?

### **What to Ask Vendors**

The first question a company should ask a potential vendor, according to Montella, is: Are you a dedicated print-to-mail service provider, and what percentage of your service does disaster recovery account for? Though many companies offer recovery as a sideline to their normal production output, during a disaster they may be unable to provide the outsourced support in addition to their regular workload.

In addition to asking about a vendor's level of experience and industry qualifications, companies should investigate how many customers are contracted at

that particular site; how many customers the vendor can simultaneously support; and if recovery time is assigned on a first-come, first-served basis. When a business interruption occurs, the last thing a company wants to worry about is if their disaster recovery site can support their workload.

Before comparing vendors, companies should visit each vendor site. Their disaster recovery or security specialist should conduct onsite surveys, and their production manager should inspect the vendor's equipment and evaluate operations. Consulting with vendor references can also provide tangible examples for better comparison, including: why a particular vendor was chosen; what the selection process entailed; vendor strengths and weaknesses; their experiences with site activation and testing; if the service has been consistent; and if costs exceeded the original estimates.

### **The Bottom Line**

Though we may be moving in the direction of becoming a paperless society, chances are it won't be any time soon. Paper documentation — in the form of mail pieces or internal communications — remains the chief method of reaching corporate customers, employees, and shareholders. In the same way that the window for acceptable downtime has become virtually nonexistent, the window for not being able to print and distribute messages in a timely manner has also virtually disappeared.

"If you want to maintain a client base and stay competitive," says Crawford, "print-to-mail recovery is more of a should-do than a requirement. Every new business opportunity comes with the question of how you'll handle business continuity. If you don't have a viable solution and, in many cases, produce physical proof of this capability, you're not going to compete for [new] business."

### **Print-to-Mail Recovery Assessment**

Print-to-mail disaster recovery provider Mail-Gard Concepts Inc. recommends the following questions be used in developing a basic proposal for print-to-mail disaster recovery.

- Do you have a data recovery plan?
- Does that data represent a printed document?
- Do you have a recovery plan for your printed documents?
- What critical applications do you need to recover at the print-to-mail recovery facility?
- How will you transfer data to your print-to-mail recovery vendor?
- What type of print streams will you use (i.e., AFP, Metacode, PCL, Postscript)?
- What type of printers will need to be recovered (i.e., cut sheet, continuous, MICR, highlight color, full color, etc.)?
- What finishing equipment is required to complete your applications (i.e., folder, accumulate, insert)? What types of barcodes are used?
- How will the print-to-mail applications be distributed (i.e., USPS, FedEx, internal distribution, etc.)?

### Print-to-Mail Issues to Consider

Print-to-mail disaster recovery provider Pitney Bowes suggests that companies consider the following issues when implementing print-to-mail recovery plans.

- *Supply Line* — Is your vendor compliant with your organization's business continuity plans?
- *USPS* — Have you contacted postal representatives to discuss the acceptance of mail at alternate locations?
- *Internal Customers (marketing, sales, finance, etc.)* — Are they aware of your business continuity plan, and is there buy-in on the process?
- *Recovery Team* — Does a recovery team exist? Do they have their roles and responsibilities spelled out? If the team cannot reach the vendor site, is the vendor prepared to function with little or no input?
- *Change Management* — Have you prepared to keep your business continuity provider in tune with all activities that affect critical applications backed up in the recovery process?
- *DR mode* — Do you plan to function as you would in normal processing, or will you streamline processes to meet key objectives, such as maintaining cash flow, regulatory issues, investment community concerns, etc.?
- *Quality Assurance* — Do the vendor's processes mirror your internal controls? Are the vendor's controls sufficient to meet audit requirements? Are any special provisions required?
- *Critical Testing* — Do you test? Have you visited the facility? Is it an active hot site or just a production facility with limited capacity availability?