

# Don't Put Your Company at

How leaving your printing  
and mailing systems  
unprotected hurts

The dramatic events of 2001 have made business continuity and disaster recovery planning top of mind within the American business community. The need for such planning is now not only a top priority for IT and risk managers, but corporate executives and investors alike have recognized how a solid continuity and recovery plan can be considered an asset to a company.

What's more, executives, management teams, boards, audit committees and other governing bodies today embrace business continuity planning as a "cost of doing business." They are challenged on an increasingly frequent basis to demonstrate proactive initiatives to minimize human and physical loss while mitigating financial risk to shareholders, investors, customers, employees and other influential audiences.

Companies whose revenue streams and critical business communications depend on printed documents yet lack an appropriate recovery strategy for such processes may be jeopardizing the enterprise's ability to sustain valuable customer relationships and short- and long-term profitability.

During a typical business day, American companies generate billions of invoices, financial statements, healthcare/insurance documents, payroll checks, payments, customer communications and critical internal communications and reports. Those documents are imaged, printed, sorted and mailed to customers, shareholders, employees and vendors.

But just one operational systems failure, whether it is caused by human error, power outage, natural disaster or even an



By Jerry Montella

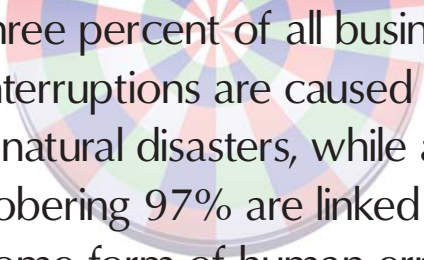
act of terrorism, can cost thousands if not millions of dollars to a company if a complete continuity or recovery plan is not in place. Without contingencies to guard against systems failures, the complex nature of print-to-mail operations can take weeks — even months — to resume fully.

## Is Your Company at Risk?

Industries that rely heavily on invoicing or daily payment cycles, such as utilities, telecommunications, insurance, financial services, credit card and brokerage services and healthcare, are at significant risk.

For utilities, telecommunications and insurance companies, each with potentially millions of individual customers, revenue models are based on daily statement generation and payment cycles. The inability to process and mail invoices, even for one day, can significantly interrupt cash flow. Claim payment cycle times are also often dictated by state regulations and contractual obligations. A delay in the ability to process and mail statements or claims, even for a short time, may force outside entities to levy penalties or take legal action.

Large retail chains process many rent checks, and some leasing contracts lock-in rental rates as long as rent is paid on time. Thus, one late rent payment for one retail location could result in a rate hike across all of the retailer's properties. And losing the ability to process payroll will not only create disgruntled employees, but it can also result in fines or penalties associated with breaches in union contracts and possibly lead to litigation.



Three percent of all business interruptions are caused by natural disasters, while a sobering 97% are linked to some form of human error.

While the events of September 2001 dramatically exposed the need for disaster recovery planning, such events do not historically fall among the predominant causes of business interruption. The U.S. Bureau of Labor reports that only about three percent of all business interruptions are caused by natural disasters, while a sobering 97% are linked to some form of human error. When asked by Disaster Recovery Journal through an online poll, continuity planning professionals indicated that the most prevalent causes of business interruption are human error (43%) and power outages (39%), followed by natural disasters (8%) and terrorism/sabotage (1%).

Business interruptions affect the majority of companies operating today. In fact, *Contingency Planning & Management* magazine found that nearly 75% of all US businesses have experienced some form of interruption.

Understanding the most prevalent causes of business interruptions and analyzing the kinds of operational failures most likely to impact a given business can help drive a systematic approach to disaster recovery planning. A company must then analyze and formulate viable contingency plans for its critical operations with a specific focus on those business applications that support its revenue stream and financial well-being.

A company should take the same steps to protect its print-to-mail operations as it does to protect any other corporate process vital to its day-to-day operation.

It must analyze exactly how long it can operate without the ability to disseminate its critical documents and assess the resulting impact of each hour or day that it is unable to generate, process, print and mail such documents.

The following elements of a Business Impact Analysis allow a company to expose the inherent risks of print-to-mail systems failure:

- Lost revenue per day in the event that invoices and other critical documents are not generated and mailed
- Costs associated with resuming operations, including temporary employees, equipment overtime costs and extra shipping costs
- Lost worker productivity during downtime
- Costs equivalent to the loss of business because service level agreements could not be met
- Monetary compensation owed to customers resulting from service level interruptions
- Fines or penalties imposed by regulatory agencies for failure to generate critical documents in a timely manner
- Estimated potential legal liability to a company, its executives and board of directors

Like most elements of a recovery plan, the return on one's investment in a print-to-mail plan can only be measured when and if a business interruption occurs.

### **Finding a Print-to-Mail Recovery Provider**

When you begin your search for a print-to-mail recovery

provider, be certain that print-to-mail recovery services are the company's primary business. Some companies sell excess capacity but may be committed to supporting one large account that has preemptive rights to their resources — potentially delaying all other customers' recovery implementations. Companies should instead seek access from providers demonstrating purposed recovery facilities in more than one locale. The following additional criteria can also be applied to service providers and support the development of a comprehensive print-to-mail recovery plan:

- Multiple, print-to-mail recovery facilities
- High-speed data communications and transfer
- State-of-the-art facilities that features diverse and well-maintained equipment
- Focused recovery team prepared to respond effectively
- Secure, 24/7 service
- Secondary back-up facilities;
- Qualified, dedicated and bonded production staff
- Capability to launch ancillary e-mail or telephone notifications to customers, vendors or shareholders that statement, payroll or invoice generation will not be disrupted
- On-site Postal Service office

Implementing a print-to-mail recovery strategy requires a pre-planning phase in which a company outlines specifications for replication of applications and processes and all necessary data requirements. Initial concept testing must then be conducted to ensure that the data and print image operations are mirrored to the specifications of a company's current processes. Periodic (annual or semi-annual) testing is also customary in order to accommodate and integrate any systems changes or alterations in data requirements.

A print-to-mail recovery initiative can be effectively incorporated into a broader recovery and business continuity plan with relative ease, with pre-planning and testing completed successfully in as little as several months. Should a print-to-mail plan need to be engaged, a company has the ability to quickly and systematically trigger full-scale duplicate operations in this alternative site. A company can shorten its total recovery time, reduce its risk and exposure to financial loss, permit compliance with regulatory and legal requirements and maintain fluid communications with critical audiences — all primary benchmarks of a successful recovery and business continuity strategy.

*Jerry Montella is the general manager of Mail-Gard, a CC3 company and provider of print-to-mail continuity and recovery services. For more information, please visit the Mail-Gard Web site at [www.mailgard.com](http://www.mailgard.com) or call 215-957-1007.*