Kodak

Disaster Recovery:
More Than Just Backing Up Data

By: Pat McGrew, M-EDP, CMP
Eastman Kodak Company
Data-driven Communication Evangelist

More than a few times in the last couple of decades, we have seen disasters that have impacted businesses of all sizes, sometimes for long periods. In the best of circumstances, those businesses have well-defined disaster recovery plans that help ensure business continuity. For every type of business those plans include considerations specific to the products, services and types of customers. For companies that communicate billing, statement, policy, benefit, and other types of financial information, a disaster recovery plan generally includes an ongoing data backup protocol and the ability to move the core data processing operations to an alternative location to ensure that business continues. Some learn, after a disaster occurs, that there were items missing from their business continuity plan, usually having to do with the ability to continue critical customer communication.

Remember that disasters come in all shapes and sizes. Some impact a wide swath of geography while others are specific to a small physical radius. It is no less a disaster when a truck takes out the power grid that serves your building, or a water main fails and floods your business, than when a hurricane or tornado takes out an entire community. Any disaster can impact your ability to communicate with customers.

Think back over the last 20 years of big disasters and catastrophes. Could your business have survived a hurricane, tornado, or earthquake? What about a small plane making an unexpected landing on your rooftop or a construction crew taking out utilities? No matter what plans you think you have, it's time to reevaluate your disaster recovery plans and your strategies for business continuity. It means looking at more than your data processing backup procedures or secure storage facilities; it means an in-depth look at your current document strategies, how information flows through your company, and what happens if you lose one or more of your mission-critical business processes, especially the print and mail operations.

Industry surveys tell us that widely reported disasters lead many unaffected companies to look at their recovery plans. A quick review to ensure that there are processes and protocols in place leaves everyone feeling comfortable and secure, but does that review truly identify the business continuity issues that can bring your business to a halt? If your plan does not include a clear set of objectives for handling everything from e-mail, to lost paper files, to print and mail, then you may be at more of a risk than you know.

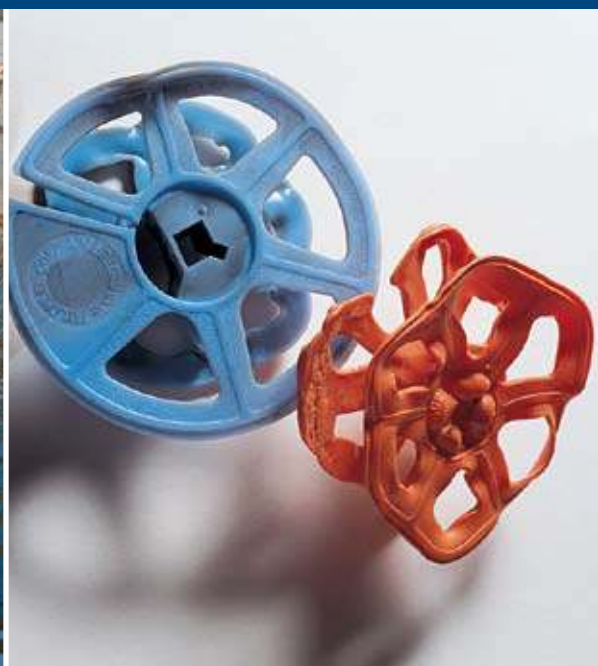
Even if you can move to an alternative hot site or to an internal company backup site, will business proceed? Even if you can get your data systems online, will you be able to communicate with your customers, send bills, statements, claims checks, refunds, or other regulatory communication through the mail? Have you seriously considered the impact of a disaster on the communication output of your data systems and the ad hoc role of communication on paper and via e-mail in the daily business process?

The role of paper in disaster recovery

It might seem like an odd place to start, but let's talk about paper for a moment. There are two considerations: the paper you store and the paper you use to communicate. Let's start with the paper you store.

Paper you keep

Not every process is covered in most recovery or contingency plans. Documents stored in on-site file rooms and sitting on desktops are often overlooked. Few companies consider the possibility that they will not know where their paper documents are, who has them, who might be reading them, and who might be using the information gained from them.



After disasters over the last 20 years, confidential documents have been caught up in the wind, and in those situations anything on paper is potentially at risk of being in public view, no matter what your normal business safeguards may be.

After an F2 tornado hit downtown Ft. Worth Texas in 2000, 27 buildings suffered damage and several were completely destroyed. The downtown area was off limits for days. Business papers littered the streets, including brokerage trade reports, retirement portfolios, and competitive analysis documents. E-mail held on personal hard drives was largely lost as PCs were sucked from buildings and smashed to the ground. E-mail containing customer requests, transaction data, and other business information was not part of most real-time backup cycles. Law firms, government offices, brokerages, and dozens of other businesses lost days, months, and years of data. Many learned that they had no backup for incoming paper correspondence or data on hard drives.

After a fire in a Dallas high-rise in 1999, one law firm lost filing cabinets full of legal documents as they were blown out of broken windows. Some industrious folks on the street below began collecting the paper and sold it back to the law firm!

So, let's consider paper.

Does your current disaster plan include a strategy for what happens if you lose all of the paper sitting on all of the desks throughout your office? Businesses handle incoming customer correspondence, internal audit reports, notes on claims and cases, research notes, competitive analysis documents, and all manner of other paper to accomplish our daily business tasks. Many of these documents can be regenerated from system backup files or re-derived, but what about original inbound correspondence sitting in someone's in basket or in the mail room?

Now consider what happens if those documents start blowing in the wind, to be picked up by anyone. If you don't have a plan, this is a good time to work on one.

Suggestion: consider adding an item to your disaster plan document strategy reevaluation: the type of information printed on documents prepared for mailing and kept in paper form in the office environment.

Paper you use to communicate

Now let's turn to outbound paper. Does your communication with your customers require any special papers? Preprinted checks? Preprinted shells? Do you know if your hot site has them in stock? How will you handle check stock? ID card stock?

Do your alternative print centers have access to all of the types of paper you need to continue business communication? Customers will understand if a logo appears suddenly in black instead of in color, but what about the ability to print checks and ID cards? In many industries legal regulations govern how long a business has to issue a refund, send a claim check, or provide identification cards. Can you meet those requirements if you are printing in another location?

A DR strategy makes sense

Kevin Craine, author of *Designing a Document Strategy*, faced just such a disaster while writing his book. Originally conceived as a book about creating a comprehensive document-based corporate strategy to ensure consistency across the business process, it turns out that the same elements are essential to building a sound disaster recovery strategy. The requirement is to ensure that the entire document environment – not just the IT, data-oriented process – is covered. His book provides the "how to" if you need a place to start in your review of the corporate disaster recovery

plan, with a step-by-step guide to understanding what documents you have, who uses them, and which are mission-critical.

At the time he was writing the book, Kevin worked for a large health insurance provider in the northwestern United States. He had a disaster recovery awakening after a series of earthquakes in the northwest.

Kevin said, "For me, the first gut check was during the earthquake in Seattle. I managed two shops, one in Seattle and one in Portland. Both were affected, Seattle obviously to a larger degree. The building was in downtown Seattle, and for a day or so, it looked like we were not going to be allowed back into the building. I lost plenty of sleep when I realized that we had a data center recovery plan ... but nothing to recover print and mail. As a result, I led a team to design a disaster recovery plan for both states."

Part of the team's efforts used concepts from Kevin's book to identify the document constituencies and the vital documents. He was surprised to learn that many of the documents he believed were critical were not. This is where developing a strategy that includes a review with document constituents is worth its weight in gold. They might have been putting resources into recovering documents that were not critical, while other truly critical documents languished. Kevin says he learned a lot about getting the right paper stocks into the alternative print locations and made sure that became part of the strategy.

The hard part is getting the budget for implementing these types of strategies. Kevin had to include a six-figure allotment in his budget to expand and enhance their disaster recovery ability as the result of their experience after the earthquakes. He worried about that part of the budget surviving, but despite many cutbacks in the budget, using the document strategy approach, the budget remained intact.

Expectations

Over the years. there have been many magazine polls asking readers to identify disaster recovery plans. In a post 9/11 poll, a leading trade publication asked:

What types of disasters does your disaster/contingency plan account for?

- Software viruses
- Application failure
- Server failure
- Network failure
- Power outage
- Service provider failure
- Computer security breaches – external (e.g. hackers)
- Computer security breaches – internal (malicious employee activity)
- Natural disaster
- Physical attacks (e.g. war, acts of terrorism)

Note that there is nothing specific in here about print and mail. You could try to include it as a server, application, or network failure, but the loss of print and mail facilities is really a different problem. And, it is apparently not on the radar for the people who crafted the polls.

They did ask another interesting question: how long would it be before the company noticed that its mission-critical systems were compromised? They gave a range that began at under an hour to greater than a month. Think about not being able to detect a problem in your print and mail facility or your e-mail servers for more than a month!

Then they asked how long it would take to reconstitute the mission-critical environment. They gave a range of under twenty-four hours to greater than a month. Imagine not being able to get your print and mail facilities back on-line for more than a month!

The final question in the survey asked how often disaster recovery plans were reviewed. They started with the optimistic daily and moved through a range that included weekly, monthly, quarterly, two to three times a year, annually, and never.

While you are in "review" mode, take a careful look at the documents being printed, both for customer delivery and internal use. Start by looking at your own desk and your own home mailbox and think about what you are seeing there. Are you getting statements with your Social Security number on them? Do you have documents on your desk with client data that includes complete account numbers and financial data? How much of that information is really necessary, and how much is just convenience? The next time you have a document review session, bring up the question of what happens in the event of a disaster if the information on the document escapes the confines of the building and goes floating away.



The checklist

If you spend the money to ensure that you are doing real-time backups of your corporate data, and you've negotiated with key vendors to provide hot site access in the event of a disaster, then be sure that you have done everything you need to do to ensure that you will be able to recover from a disaster.

Start with the basics:

☑ Can you clearly identify your mission-critical documents?

Everyone has an opinion of what is critical, but have you taken the extra step of defining the constituents for all of your documents and discussing their needs if a disaster happens? It should be a part of any document strategy exercise, but that part of the discussion is generally overlooked. Remember that the documents that are critical on a daily basis may not be the documents that are critical in crisis mode. Talk it over with the owners of the documents and processes to determine where to put document recovery resources.

☑ Does your company have a *comprehensive* disaster recovery plan, contingency plan, or business continuity plan?

Over the past 20 years the names have changed, but the general idea is that every business, regardless of size, should have a plan for what to do in the event of a disaster. For most companies this involves what to do in the event of a hurricane, tornado, earthquake, or fire that disrupts business. Once the employees are safe, the key concern is the preservation of the data and application programs that drive daily business.

☑ Can your current plan stand up to the challenges posed by a catastrophic event?

Think outside of the box that contains your data backup procedures. Do a checkup on the health of your e-mail, and print and mail processes and protocols. Scrutinize your current document strategies. If your current plans fail to include concrete objectives for handling everything from e-mail to lost paper files, to print and mail, you may be wasting company time and money, and putting your company at risk.

☑ How fast can you recover key e-mail containing customer requests, transaction data, and other business information?

☑ What is your plan if you lose all of the paper sitting on all of the desks throughout your office?

☑ What is your plan if your mailroom is destroyed?

☑ Do you have a plan to get print and mail functions back into full operation?

Why is this important? Cash flow is a big reason. And when your print and mail operation drives your revenue, that can be the difference between survival and financial collapse.

☑ Do you have a working and tested hot or cold site?

Even if you get print and mail out the door every day, you may have lost track of the amount of equipment in place to move your applications through the print and mail process. From the systems that generate the data and develop the print, to the print devices, and then on down the line to bursters, trimmers, stackers, bar code markers and readers, stuffers, sorters, and the rest of the odd-looking machines that occupy the floor space, there is a cavalcade of technologies that go into the average print and mail operation. And, if your print and mail environment is leading edge, you may have even more complex equipment for handling the mail sorting and packaging. Does your hot or cold site mirror what you do today?

☑ What are your print streams?

AFP? **Xerox** DJDE? **Xerox** Metacode? **Adobe** PDF or PostScript? Line Data? You may be surprised to learn that you have all of them, as well as applications that post-process the original print streams. Each of the print streams has its own file format, its own resources that control the jobs, its own font issues, graphic formats, and electronic forms formats. Having the data available to print without having the required forms, graphics and fonts is as good as not having the data to print at all.

☑ Do you know where your resources are and if they would be available at a backup site? Do you use custom fonts, unusual paper, preprinted forms? Any of these can make it difficult to migrate your print to an alternative facility in the event of an emergency, unless you prepare in advance.

You may find that resources created using older versions of the applications will not migrate to a site that is completely up-to-date. Conversely, if you are a cutting-edge shop, your applications may be too new to run successfully at your alternative facility. Testing is imperative.

☑ Beyond the print files there are the support issues, including all of the post processing, sorting, and stuffing equipment; much of which relies on bar codes, edgemarks, or similar technology to make the right decisions about how to create the appropriate mail packages. Can your alternative facility handle your needs as they are currently coded? Will they be able to stuff your envelopes, insert your preprints, and verify your zip codes as you do in your facility?

Use your internal experts

This is a lot to think about, and we're not quite done yet. Once you have had a chance to review your current plans, including print and mailroom recovery, it's time to have a long talk with the business continuity group in the organization. If you don't have one, it's time to form one.

Business continuity experts look at the business with a completely different set of objectives than the application developers, workflow managers, and other process owners. Their mission is to develop the procedures that ensure that business can continue in the event of any type of business disruption. The needs of a bank are different from those of a manufacturing plant. The needs of a print and mail-service bureau are different from those of an aircraft manufacturer. There will be many common elements, but every business is different. Even two insurance companies may have different requirements as they build their approaches to business continuity.

You will also need executive buy-in.

The moral to the story is that disaster recovery planning means different things to different organizations. For some, it means complete, constant hot backup of all data in the enterprise and the demonstrated ability to recover every iota of information in the event of a disaster. For others, it means keeping the business up and running and maintaining an ability to re-derive any lost data. Regardless of where your enterprise falls, you should have a comprehensive plan in place that includes customer communications.

To learn more about **Kodak** Products, Disaster Recovery Services or Preservation Services and Solutions Agents, call 1-800-944-6171.

Produced using **Kodak** Technologies.

Eastman Kodak Company
343 State Street
Rochester, NY 14650

Kodak