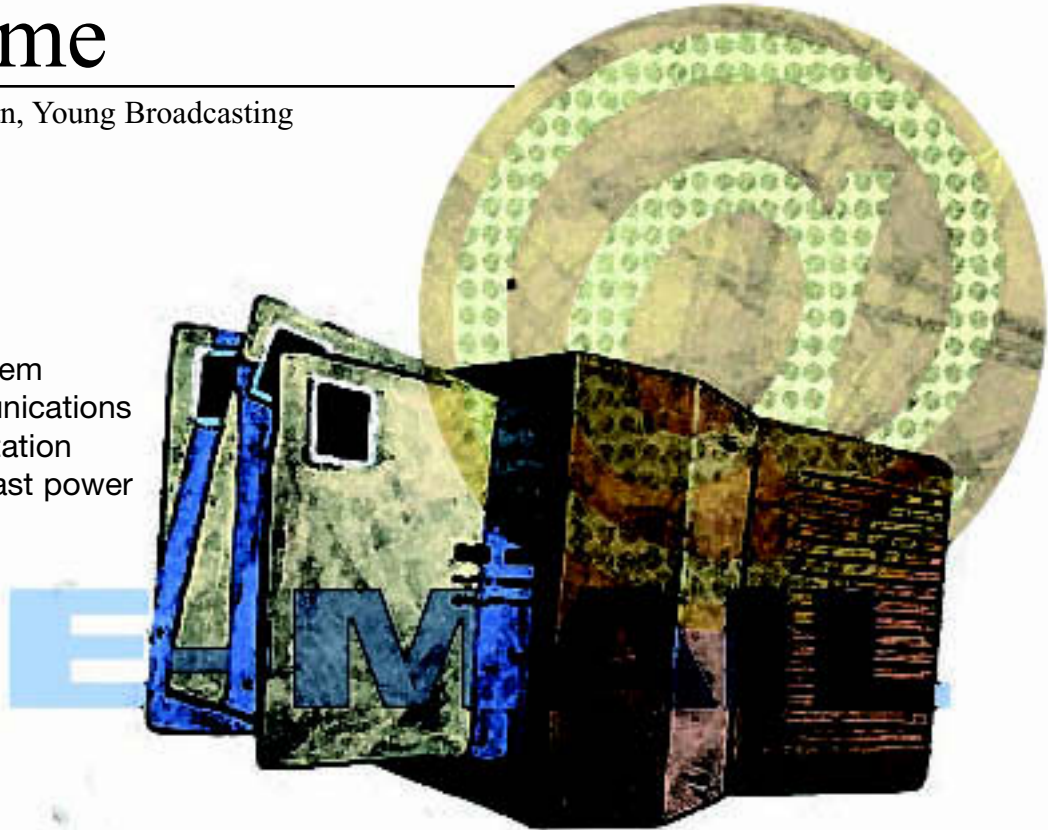


Case Study

Strategic Pre-Planning Yields An E-mail Recovery Solution Just in Time

Peter Grazioli and Dan Ryan, Young Broadcasting

An e-mail continuity system maintains critical communications link for a broadcasting station group during the Northeast power outage.



Executive Summary

The loss of e-mail can severely impact revenue, productivity, reputation and the ability to communicate and facilitate the communication process in the wake of a disaster. With strategic pre-planning, Young Broadcasting was prepared with an e-mail continuity service when the Northeast power outage hit last summer. The outage knocked out its New York City headquarters and several of its TV stations nationwide, yet Young was able to recover quickly and maintain communications with its backup e-mail continuity service.

YOUNG BROADCASTING, ONE OF THE LARGEST AND fastest growing broadcast station groups in the United States, owns and operates 11 television stations in geographically diverse markets from San Francisco to Green Bay, and operates the national television representation firm, Adam Young. The responsibilities for the BC rest with VP/CIO Peter Grazioli and Systems

IT/Manager Dan Ryan, experienced IT veterans who are based in Young Broadcasting's New York City headquarters.

With the company and its television stations increasing dependence on e-mail, they knew that they had to ensure that e-mail continued even during an outage, or it could cripple the stations, from news reporting to advertising sales efforts for the business. The New York City headquarters was key, because if its data center e-mail capabilities were to become incapacitated, inbound e-mail would not be able to flow to the staff of television stations across the U.S.

For the IT department at Young Broadcasting, strategic pre-planning with technology consultants put them in the enviable position last summer of having a reliable and affordable e-mail recovery solution in place when the MS Blaster virus and the Northeast power outage crippled businesses across the country.

When Young Broadcasting's e-mail continuity solution kicked into gear, it saved critical business downtime and helped them recover smoothly with key communication channels in place.

CHECKLIST FOR EVALUATING AND SELECTING AN E-MAIL CONTINUITY SOLUTION

Hosted versus self-hosted approaches.

It comes down to risk mitigation. With a self-hosted approach, physical and man-made threats may take down your primary system as well as a self-hosted backup e-mail system (e.g. a hurricane or power outage). Using a hosted continuity solution mitigates a single point of failure and can reduce overall risk.

Look for the easiest to deploy and manage systems.

It should be relatively quick and painless for an IT department to get a business up and running with an e-mail continuity solution—in many cases in less than 24 hours. In addition, the IT department should not have to expend manpower managing and overseeing the system.

Focus on recovery time objective.

An e-mail continuity solution should be ready and able to be activated at a moment's notice to ensure vital communications. Services such as EMS from MessageOne can be activated in less than 60 seconds via a Web console or a phone call.

Consider solutions that support multiple messaging platforms.

Systems that support the most popular environments, such as Microsoft Outlook/Exchange, Lotus Notes, Novell GroupWise and others, will give your business the flexibility to add additional environments and still be protected against an e-mail outage.

Follow basic command and control doctrine.

Look for systems that are functionally equivalent to the primary, but with a structurally different architecture. For example, if your organization uses Microsoft Exchange or Lotus Notes, choose a continuity solution built on an open source code such as Linux, which will provide an extra layer of protection from brand-specific viruses or worms.

| Strategic Pre-Planning |



Mission-Critical E-mail Could Not Fail

As one of the fastest-growing broadcast ownership groups in the U.S., Young Broadcasting was rapidly multiplying with people, properties and partners across the country. Trying to get a handle on the IT challenges of serving such a far-flung enterprise with 24/7 business requirements was not an easy task.

After conducting an enterprise-wide business impact analysis (BIA), it was clear that maintaining key communications across the offices was a mission critical endeavor for Young Broadcasting's business. The loss of e-mail to some or all of the organization could severely impact revenue, productivity, reputation and the ability to communicate and facilitate a recovery process in the wake of a disaster.

Like most firms, Young Broadcasting has a handful of close partners and consultants they've worked with over the years. One of the firms Young Broadcasting has a long history with is New York City-based Domino Computing—a full systems VAR and systems integrator that had helped set up and manage Young Broadcasting's messaging infrastructure. In working closely with Domino Computing on architecting a highly available e-mail system, they ultimately recommended an emergency messaging system (EMS) that they recently discovered and already tested and deployed for their own use.

This new EMS, from MessageOne (Austin, TX) was not like any of the previously considered solutions, which were expensive, difficult to deploy, hard to manage and not completely thorough in covering the widest range of possible threats. It offers enterprise-wide, self-administered deployment in less than one hour—a feature of great importance to Young Broadcasting's lean IT department. A unique bonus was an emergency notification and escalation process to help ensure business communications were in place and could be strategically used for business recovery in the event of a disaster. And the EMS was significantly less than the cost of other e-mail continuity solutions.

New Emergency Messaging System Deployed

After recognizing the strong value proposition of this new e-mail continuity solution, Young Broadcasting moved forward with Domino Computing to deploy the new service in their New York City headquarters and data center. This location was a high priority since it houses the company's Internet SMTP gateway for all Internet-bound e-mail.

The EMS was deployed in less than a day and quickly sent e-mails to all Young Broadcasting staff around the country, asking them to enroll and register on the system with their emergency contact information (including alternate e-mail addresses and all telephone contacts) in the event of an emergency in which the firm needed to reach them.

Once deployed, EMS required very little maintenance for the IT department. Working closely with Domino Computing, a simple series of desktop, Web-enabled tests of the EMS were conducted to ensure that the system was armed and ready in the event of a potential outage or disaster. Daily e-mails, notifying the company that the EMS system was working properly, also were sent out to assure the company was protected against the worst-case scenario. This required no day-to-day proactive management from the IT staff, but allowed Young Broadcasting's team to know they were always prepared.

NE Blackout Shuts Down Headquarters

After implementing the EMS, a few months went by with business as usual. That changed dramatically in early August of 2003 when the first significant worldwide computer virus was running rampant—the MS Blaster RPC worm. The threat to enterprise computing systems was significant and having the ability to turn over its e-mail system to the EMS could protect the company while it had time to determine the internal course of action and conduct check-ups and install reactive patch upgrades to its systems if they had not already done so. Although Young Broadcasting was not impacted by that particular threat—its turn was definitely coming.

On August 14, 2003 the Northeast U.S. was hit with a major blackout that spanned the Great Lakes area to the East Coast. Young Broadcasting's NYC headquarters, in mid-town Manhattan, was not immune. Within minutes, building evacuations began and the staff was forced to power down the data center, including the central MS Exchange servers. Just 20

minutes after the outage hit, IT was able to place a call from a physical, landline phone to their EMS vendor's network operations center to declare an emergency. Working through a quick, pre-arranged authentication pass phrase—designed to authenticate IT staff identity—Young Broadcasting IT staff instructed the activation of EMS for the firm immediately—and in just seconds the e-mail backup system was up and running.

“The problem at the time of the blackout was that senior management had no way of knowing either the extent of or the potential duration of the outage,” says Grazioli. “This left the affected managers without an effective way to communicate with their employees and partners in the field offices to let them know their business status.”

He added, “By using EMS, Young executives were able to restart the flow of e-mail (both to and from the Internet) to continue to enable those sales offices in Atlanta and Dallas that were not even geographically impacted by the blackout. Once Young Broadcasting's EMS was activated, all the e-mail users were notified (to both their primary e-mail addresses and their emergency contact addresses) to let them know that Young Broadcasting headquarters had been affected by the blackout and that the data center was not operational.”

Young Broadcasting IT staff also informed affected employees that the EMS was in place and gave them simple instructions (a URL address) from which they could go from anywhere to access, send and receive their corporate e-mail. Had they not been notified, the users across the country would have spent considerable time trying to reach Young Broadcasting's evacuated corporate IT desk seeking help with their now disabled e-mail system.

EMS Keeps E-mail Flowing

According to Ryan, “When our staff logged into the EMS system, they were greeted with a simple interface and could find and have access to all critical corporate and personal information they used on a day-to-day basis (contact lists, corporate directory, distribution lists, etc.). Most importantly, they could continue to send and receive e-mail without the outside world knowing that they were no longer operating through their usual business e-mail system.”

Even though their NYC office remained without power for four days, many of the New York City-based staff members were able to get power earlier at their homes outside the city and were able to work remotely through EMS. One of Young Broadcasting's IT managers was even able to use a fully charged notebook computer with an unaffected POTS (plain-

old-telephone-system) landline to dial up to his ISP, connect to EMS and then send out e-mail updates to the entire enterprise.

When Young Broadcasting did finally get power back in NYC, they were able to bring their MS Exchange server up—but not without incident. As a consequence of the power-down sequence, it had suffered a database corruption that took hours to repair. Once again, they were protected as they maintained the EMS system for e-mail until they had the server ready to go. When they did bring the primary MS Exchange system back up, the process of returning users to the primary e-mail system was straightforward and easy. The EMS automatically recovered all transacted messages sent or received on the EMS and transferred them back into the primary e-mail system.

“For our users, it was if they had never left the primary e-mail system and to our outside partners, vendors and customers as well—enabling us to continue to communicate reliably even during the outage,” explains Ryan.

It's Good to Be Prepared

According to Grazioli, “We are thankful and fortunate that we had the foresight to embark on contingency planning and risk mitigation, which paid off for our organization. Not only did it enable us to continue to communicate with our other offices/stations and clients, but it enabled us to recover, by providing us with reliable e-mail communications during the outage.”

The results with this new EMS were so impressive that Young Broadcasting has already purchased it for all of its TV stations across the country and is in the process of deploying those now.

According to Ryan, “It was nice to have our efforts recognized for a few days around our company, but as business went back to usual it will be the unexpected that makes our job truly appreciated.”

As Young Broadcasting's strategic plan calls for a continuation of an aggressive acquisition program to further build its broadcast group, placing added demands on the IT infrastructure, the IT team will continue to be prepared for the unexpected with its backup e-mail service, enabling Young Broadcasting employees to continue with business as usual.

CI

Peter Grazioli is vice president and CIO of Young Broadcasting, Inc. (New York, NY). He can be reached at pgrazioli@young-broadcasting.com.

Dan Ryan is the systems/IT manager for Young Broadcasting, Inc. He can be reached at dryan@youngbroadcasting.com.

©2004 Communication Technologies, Inc., All Rights Reserved.

Reprinted from *Continuity Insights* magazine. Contents cannot be reprinted without permission from the publisher.

STRATEGIES TO ASSURE INTEGRITY, AVAILABILITY AND SECURITY
[CLICK HERE TO SUBSCRIBE, WWW.CONTINUITYINSIGHTS.COM](http://WWW.CONTINUITYINSIGHTS.COM)