

DISASTER PREPAREDNESS GUIDE

Even small companies seeking to protect data

By David Ortiz,
PBN Staff Writer

UNICOM, a Woonsocket-based computer technology consulting company, was recently approached by a client concerned about the costs it would incur if its e-mail communications were brought to an extended halt by a terrorist attack or computer network meltdown.

So UNICOM forged a data backup solution for the client, a manufacturer headquartered in Boston, which involved replicating the client's exchange server at a satellite facility in New Hampshire.

"In the event of a catastrophic failure in the geographic location of their main site, what will happen is in a couple of moments' time, all mail traffic would then be re-routed to the backup location, and mail would start flowing just as it would prior to the disaster," said Chris Powers, a systems engineer for UNICOM.

The job was a routine example of work being performed daily by a growing number of firms in Rhode Island and across the nation. The data protection and recovery field has exploded in recent years, as companies and organizations of all sizes seek to protect disruptions caused by natural and man-made disasters, and to comply with more stringent government regulation of electronic data.

The field is seen as offering so much potential that some computer technology companies that once offered many

services are now focusing exclusively on data protection and recovery. One such firm is SafeData LLC, a Warwick-based firm in business since 1995 that two years ago shut down its hardware and software sales divisions to focus exclusively on data services.

Today, the company is a managed service provider that offers subscription-based data protection services.

"We've doubled the business in the past year, and we're about as busy as you could possibly be without having a heart attack," said Peter Briggs, SafeData's president.

The data protection and recovery field has taken off as more and more businesses and organizations grow their computer networks and allow employees to work remotely, Briggs said. At the same time, the business world has become increasingly concerned about the financial impact of lost time in the event of a disruption, Briggs said.

"There's no more tolerance for downtime," he said. "I think where companies used to be able to say, you know, if we back up to our tape, and we store it in a safe somewhere and our building burns down, we can rebuild the business in three or four or five days – that's adequate. And what's happening today is because of the competitive nature of business and the

service that [companies] have to provide to their own customers, their systems cannot be down as long.”

Companies and organizations in industries that have become increasingly regulated in recent years are generating a significant amount of business for data protection and recovery firms as well.

Lincoln-based Lighthouse Computer Services’ booming data protection business is being driven largely by clients in the banking, accounting and medical industries that need to comply with Sarbanes-Oxley, and other federal laws and regulations, said Jerry Hughes, the company’s director of IT governance, auditing and regulatory compliance.

‘We’re about as business as you could possibly be without having a heart attack.’

PETER BRIGGS
SafeData president

“It is really a requirement – more than just best practices now – that organizations that store private information off-site, that these backups are encrypted,” Hughes said. “My team is able to go in, assess the client’s environment and what the regulating agencies in their industry require of the information that they save.”

In particular, many of Lighthouse’s clients are banks and other financial institutions that turn to the firm for its expertise in that industry’s data compliance laws,” Hughes said.

“We serve all industries; however, there’s been a lot of traction in the banking industry and really the financial industry as a whole, including the SEC world with Sarbanes-Oxley,” he said. “So we’re

doing a lot of work with those folks to ensure that their environments are secure.”

For local data centers that provide physical storage of their clients’ computer systems, Rhode Island’s size and geographic location offers a strategic advantage, said Casimir Kolaski, owner of HostTech Communications, which has a 40,000-square-foot data center in Providence.

Increasingly, companies in large cities are seeing to store their computer systems in remote locations to prevent disruptions in the event of a natural disaster or terrorist attack. Many of HostTech’s clients are from Boston and New York City and want to maintain their computer systems outside their large metro areas but close enough that their engineers can easily travel to their machines, Kolaski said.

“It’s far enough away to be safe, but close enough to be able to get at it,” Kolaski said.

Until recently, only large companies could afford systems that continuously protected their data and ensured the data would be quickly retrieved in the event of a catastrophe. But today many smaller businesses and organizations are moving to protect their data, aided by lower prices and an array of solutions tailored to smaller enterprises as the data protection field matures.

In today’s business climate, everyone needs to protect their data, Kolaski said.

“Even something as simple as a pizza shop needs to track the amount of pizzas they do an hour – so that’s important data – all the way up to a bank [dealing with] credit cards and social security numbers. So there are different fault tolerant levels for companies,” he said.