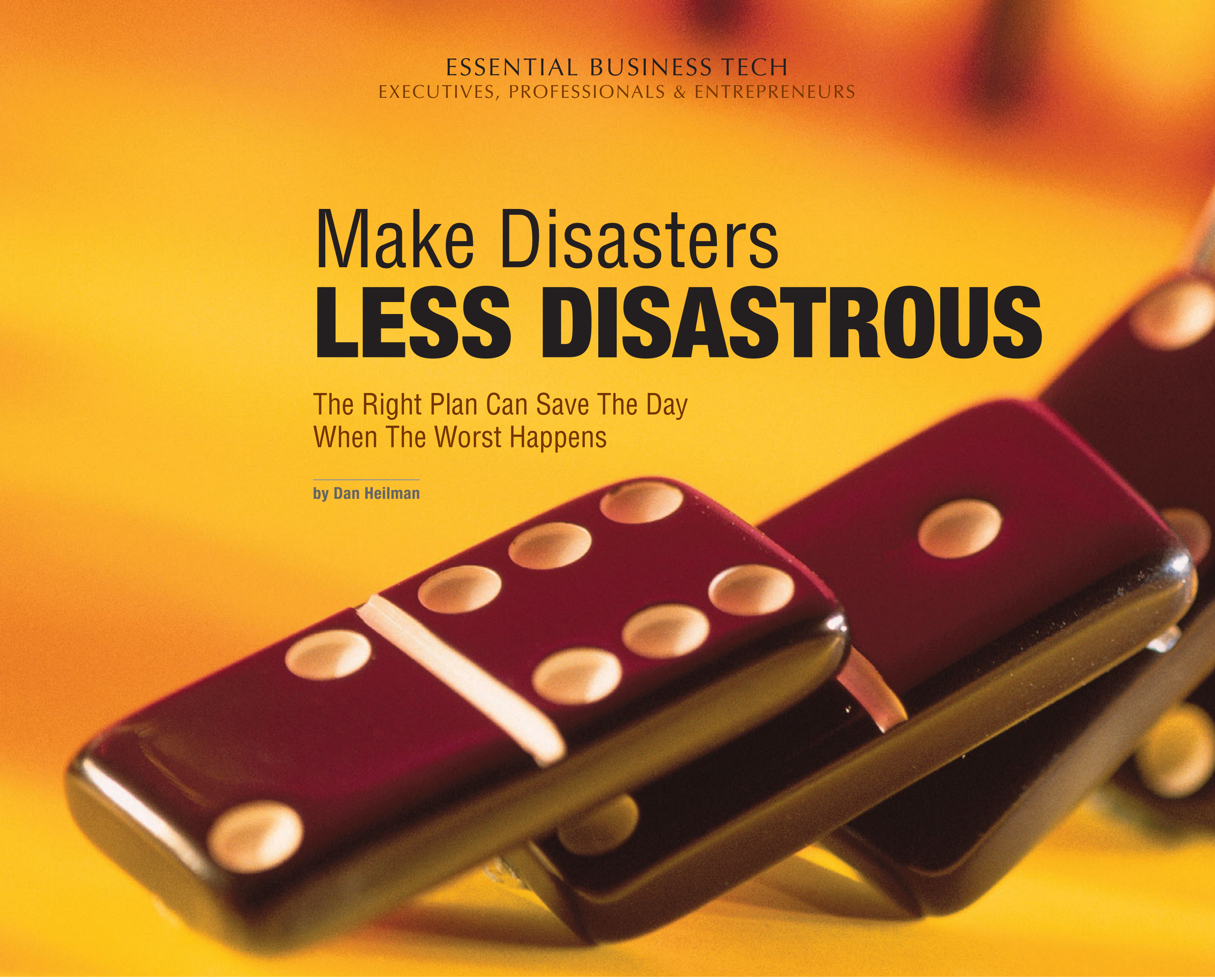
ESSENTIAL BUSINESS TECH
EXECUTIVES, PROFESSIONALS & ENTREPRENEURS



Make Disasters LESS DISASTROUS

The Right Plan Can Save The Day When The Worst Happens

by Dan Heilman

KEY POINTS

- ▲ List, in order of importance to your company, the technologies you need to run your business, and how long you can get by without them.
- ▲ Decide what technology you're going to use for your backup system.
- ▲ Make the formation of a disaster recovery plan a team effort, and make sure everyone knows what to do if disaster strikes.
- ▲ Once a plan is in place, test it regularly.

If you're a business owner, chances are you have at least one file drawer full of insurance papers: insurance for your facilities, insurance for your assets, insurance for your workers.

What about insurance for your data? If that's something you've overlooked, you're not alone: According to Stamford, Conn.,-based IT industry analyst Gartner, only about half of medium-sized businesses and 25% of small businesses have a comprehensive disaster recovery plan in place.

That's partly because many small-business owners are so busy that planning for a disaster rests perpetually on their "to-do" lists, and partly because business owners are no different from the rest of us: They presume it won't happen to them, whether "it" is a server crash or a flood.

But having policies and procedures in place in case the worst happens isn't just prudent; it can potentially save your business. A DR plan can take on many forms, and can be customized to give your business the ability to bounce back quickly from disasters ranging from a server outage to a natural disaster that wipes out a data center.

One Size Doesn't Fit All

There's no one-size-fits-all way to develop a disaster recovery plan, but experts in the field agree on a number of steps you should take. A natural first step is to take stock of your IT-related assets, including data-based applications such as email, and determine how crucial each of those elements is to helping your business run.

"You can literally write that out on a piece of paper," says Heinan Landa, CEO of Optimal Networks (www.optimalnetworks.com), a network support company based in Rockville, Md. "It doesn't have to be a fancy exercise. Think through two questions for each type of data, whether it's email, client contacts, marketing database, accounting systems, or documents: How long can I

tolerate being without this information? And, how much of this data can I afford to lose?"

To paint a broader picture of how your DR plan should look, spend some time identifying your company's primary goals and the systems that must stay up for you to reach those goals, says Chris Moschovitis, CEO of New York-based TMG-Emedia (www.tmg-emedia.com).

"Create a simple scorecard," says Moschovitis. "Do you need to have your email server up and running at all times? Grade that 'A.' If you're OK with your accounting system being down for a couple of days, grade that 'B.'"

The most crucial elements of your company's technology will vary by industry, of course. If you have a Web site that is used mostly for marketing purposes, it might not matter if it's down for a day or two. But if you're a retailer or a business-to-business seller, an outage like that can mean significant lost revenue. What has to have the most uptime at your company: Email? Your accounting system? Specialized software, such as the litigation support packages used by many law firms?

"If part of your system goes down, figure out what the consequences would be to your business," says Gayle Rose, CEO of Electronic Vaulting Services (www.evscorporation.com) in Memphis, Tenn. "Will there be a loss of revenue? How much? Loss of reputation? At this point you can actually put some numbers to your thinking. If your email goes down, you have to be able to define how much that would cost you on a daily basis. [It's also important] to get agreement among your leadership about what constitutes an intolerable consequence for your business."

Better Shop Around

Once you have a list of your technology assets in prioritized order, you need to decide what form your disaster planning will take technologically. There are numerous varieties of technologies available to back up your systems and data, some more bulletproof than others. Some companies still back up their data on tapes, but many experts consider that a faulty, unreliable way to ensure safe data.

Quickly supplanting tape backup is off-site data storage, which assures that all your data files are preserved in case of disaster or hardware failure. With offsite backup, data can be saved and transferred manually or automatically over the Internet. What sort of a backup schedule you adopt is up to you; some businesses can get by with daily or even semiweekly backups, while more data-intensive companies require several backups per hour.

Less frequent backups automatically contain compromises, according to Landa. "If you do a daily backup, you're saying that it's OK if you lose 24 hours' worth of data," he says. "You're also saying that if your server crashes and you have yesterday's backup, it's OK to wait two or three days until the server is running and your data is restored."

> "A disaster plan doesn't have to be a fancy exercise."
>
> **Heinan Landa,**
> *CEO, Optimal Networks*

More modern DR solutions take snapshots of servers every 15 minutes and store them locally on a disk, giving you the ability to virtualize a server from that backup set within an hour or two. "You won't lose more than 15 minutes of data," says Landa, "and you can be back up and running within two hours."

> "As long as your IT infrastructure is generic and inexpensive, you can use cheap, simple disaster recovery solutions."
>
> **Jeffrey Bolden,**
> *partner, Blue Lotus Systems Integration and Data Conversion*

If you own a company that relies heavily on a Web site for its revenue, such as a retail business, consider a backup site: an online location where an organization can easily relocate its business following a disaster. The most reliable (and expensive) type of backup site, called a hot site, is a duplicate of your original Web site, with near-complete backups of all your user data.

"It's worth asking if you need a hot site or real-time replication of data and transactions," says Ed Coram, an IT consultant with Systems Alliance in Hunt Valley, Md. "You can fail over pretty much in real time, but of course there's costs related to that. You can also pay for space or accommodations as you need it instead of on an ongoing basis, which is a cheaper option if you feel your company can stand a data outage of a couple of days."

Jeff Bolden, a partner with Blue Lotus SIDC (Systems Integration and Data Conversion; www.bluelotussidc.com) in Princeton Junction, N.J., agrees that while it might be tempting to get a top-of-the-line backup solution, it's not necessary for many businesses.

> "If your email goes down, you have to be able to define how much that would cost you on a daily basis."
>
> **Gayle Rose,**
> *principal owner and CEO, Electronic Vaulting Services*

"In the case of a lot of businesses, there really isn't that much important data on their actual computers," Bolden says. "Often, even some important functions, like accounting, are outsourced. As long as your IT infrastructure is generic and inexpensive, you can use cheap, simple disaster recovery solutions."

Make It A Team Effort

Many small-business owners subscribe to the credo that if they want something done right, they must do it themselves. That can be a bad idea when developing a disaster recovery plan. If you're the only one who knows the plan, what are your employees supposed to do when it's time to put the plan in action?

It pays to not only have a team of key internal players help you develop your DR plan, but to also have specific assignments for everyone in the company if and when disaster strikes. A communication plan will enable people to quickly rally the troops and help get your IT system back on its feet.

"Every small business has one or two people who are highly knowledgeable about what makes the business run in case of a disaster," says Bolden. "Take advantage of that knowledge."

Making a DR plan into a team effort can even involve bringing in people outside the company, such as suppliers and other vendors. While big businesses usually have complicated internal infrastructures, most small businesses outsource that infrastructure. But something small businesses often fail to do is keep an up-to-date list of all their vendors and what roles they play.

"Let's say there's a disaster and your company has to move to a new location 30 miles away," says Bolden. "You have to know who does what for you. Otherwise you can end up in a situation where you've forgotten how to make your own processes run. Let your vendors and their technology help you regain your technology."

Testing, One-Two

Having a disaster recovery plan in place won't help you sleep much better at night if you're not sure it's working. Testing on a regular schedule is a crucial component of even the most modest DR plan, according to Landa.

"Once every six months is a good interval," he says. "You don't have to do a complete, disruptive test where you rip down your entire network. If you can see your latest backup, you can be 99% sure everything's running OK."

Even with a seemingly airtight backup system—let's say a disk-to-disk-to-tape backup, in which a server backs up to an external hard drive, which is backed up to tape, which is sent to a vault—should be subjected to an occasional pop quiz, according to Moschovitis. "Once a month, you should randomly pick a file from that backup and try to restore it—from the server and from one of your tapes," he says. "It's a simple way to do a quick test."

Whether you test your DR system once a week or once a year, the main thing is that you have such a system, and that it suits both the priorities and pocketbook of your company.

"We always tell our consultants that in IT, failing to back up is a career-ending mistake," says Moschovitis. "That's how companies need to think: Failing to plan adequately for a disaster is a career-ending mistake." ▲