SECURE HORIZONS

DISASTER PLANNING IS OFTEN OVERLOOKED AND DONE HAPHAZARDLY. FORMALIZING POLICIES AND FORGING PARTNERSHIPS CAN WARD OFF DOWNTIME.

WRITTEN BY ESTHER SHEIN | ILLUSTRATED BY WILLIAM DUKE

JOSH BAUER HAS NO intentions of letting an IT disaster cripple the systems of Daymon Worldwide while he's on the clock. Bauer, network administrator for the private labeling and branding firm, has taken multiple steps to prevent any kind of crash and burn. First, there was an audit to check for deficiencies in the data backup plan. Second, there was an upgrade to new backup software that could better handle the needs of Daymon's growing remote population. As icing on the cake, Bauer put the new capabilities to the test during the company's annual off-site disaster drill. As part of this exercise, Bauer and his IT staff took the most recent backup tapes and installed them on test servers at a remote site in Philadelphia to prove system resilience. "Everything came right up—exactly the data we'd need to operate from a new location—and very quickly," says Bauer, in Stamford, CT.

Daymon Worldwide is in the minority when it comes to small- and mid-sized businesses adequately and appropriately preparing for IT disasters before they strike. Data storage experts say most SMBs, hamstrung by either limited or no on-site IT staff, generally don't make data backup and recovery a priority and do little to no advanced preparation. Even if they have a system in place, oftentimes there's no one in charge of regularly backing up and testing the data. Even the simple things, like making sure there is a tape in the drive, often get lost in the cracks.

"Companies at the smaller end are doing it themselves, so they try and figure out what to back up—if they remember to do it at all," says Fred Broussard, a research manager at International Data Corp., in Framingham, MA.

Dealing with data security and recovery haphazardly, though, is a disaster no business can afford, regardless of its size. Small and large companies need to make both a top priority, at the very least, putting products in place to protect them at a most basic level and, even better, formalizing policies and forging partnerships—to help ward off any disaster that could lead to downtime.

The first step to disaster recovery planning is to answer some basic questions that can help determine what kind of products and what scope of policies are necessary for your business. Start by determining your business requirements and business continuity needs since those most impact the tools you'll use. Also figure out who will be in charge of backing up the data and how often they need to do backups and testing; institute those choices as formal policies, with penalties if they're not adhered to. Companies should also designate an offsite location to store backup tapes—for example, a bank vault—and potentially find a data center where tapes can be brought in the event of a catastrophe, minimizing downtime for the business. Some experts even suggest prioritizing

A 10-STEP PROTECTION PLAN

Most small businesses don t deal with disaster until disaster strikes. But that can end up being a huge mistake in terms of cost and downtime. You don't have to make major changes; even small measures can help.

INFOGRAPHICS BY JOHN GRIMWADE

COVERING THE BASES: Sonny Labrie of the Federation of Canadian Municipalities employs a multi-faceted backup plan.

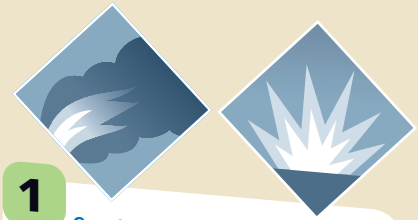
PHOTOGRAPH BY TONY FOUHSE

data and backing up what's deemed critical on a more frequent basis.

Another thing to consider is that backup and recovery isn't just about protecting data. When formalizing a plan, companies also need to think about their applications, especially proprietary ones, and make sure those are factored into the process as well. And if a business operates 24/7, it should consider installing software that backs up open files and applications that employees use late into the night or around the clock, in addition to what's closed out at the end of the workday, when network backups typically occur, experts say.

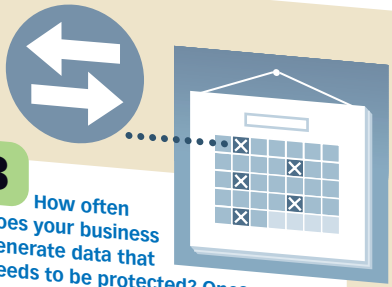
"It's not enough to have the software—you need the discipline to do the backup, make sure [tapes] are being taken off-site, and test the recovery [plan] so you make sure what you've taken off-site can recover your business," advises Mickey Baker, a senior consultant at GlassHouse, an independent storage service provider, in Framingham, MA.

Sonny Labrie does all that and more after learning the hard way about the price you pay for not formalizing a disaster-recovery plan. Years ago, in a previous post, Labrie experienced a data-backup



1 Consider the possible hazards your business could face. These can range from natural disasters and human error, such as floods or fires to terrorism, hackers, or disgruntled employees. Also consider potential exposure from surrounding businesses.

2 Make a business decision on what level of recovery is required for your business. Does your company generate critical data?



3 How often does your business generate data that needs to be protected? Once you understand why, what, and how often your company needs to back up, you can make a decision on what backup plan best fits your business.

"Companies at the smaller end are doing it themselves, so they try and figure out what to back up—if they remember to do it at all."

failure—now he covers his bases with a range of products and backup procedures.

Labrie, manager of information systems for the Federation of Canadian Municipalities, a lobbying group in Ottawa, employs basic backup and recovery software supplemented by another application. That program migrates data the federation hasn't used in a while to another drive based on policies that Labrie sets. The impetus for this piece of the backup strategy came about because the federation was holding on to too much information that wasn't being accessed every day, making it a challenge to run backups on a single tape drive. "This reduces the amount of data we back up every night and the amount of time it would take to recover the data," Labrie explains. It also precludes them from having to purchase a larger tape library, which the federation couldn't afford.

Labrie has a number of other disaster-prevention maneuvers up his sleeve. An application assessment helps him prioritize backups. The federation has 115 employees and runs 18 servers, all of which require backup. Thanks to the assessment, though, Labrie has prioritized backup for the federation's accounting program as well as any member-centric databases, he says. There is also an information storage provider partner, Iron Mountain, which, for a monthly fee, picks up and stores the federation's tapes off-site. The other critical measure is to rent co-location space from an Internet Service Provider, where the federation installed some Web servers that will be tapped in the event of a network failure. "I could just take our tapes and go to the ISP's site and restore the data, and have our users operational either within hours or days," he explains. "It can save your business."

Unlike Labrie, Carol Hynes has never personally suffered the pain of losing company data, yet she takes the threat just as seriously. While Hynes handles basic technology setup and support at FloraTech, a small manufacturer of jojoba oil and cosmetics products, she's brought in some outside assistance to handle disaster-recovery planning.

Basic backup, tasks like workstation setups, server backups, and shuttling tapes to a secure location is Hynes's responsibility. The heavy lifting, including coming up with a formal game plan, selecting products, and instituting best practices, is the domain of FloraTech's partner, Bryan Vincent Associates, an IT consulting company in Chandler, AZ. "A company our size needs someone else to ... administer the system so I don't have to know everything about everything," says Hynes, vice president of business management, who is also the de facto go-to technology person for the 34-person FloraTech in Gilbert, AZ.

Daymon Worldwide's Bauer also enlisted partners to whip the firm's data backup program into shape. Previously, Daymon's backup policy required users to back up their own data locally on a regular basis. The company also expected its several hundred remote users to upload data to a central server for

4 Create a contingency plan to remain in operation if your office becomes unusable. Notify your employees of this plan and provide regular updates. Also consider contracting with your local ISP or hire a data center for backup. Another option is to form a partnership with a like business in order to get up and running quickly. Conduct a disaster simulation to see if the plan works.

5 Identify critical files such as accounting records, customer lists, production formulas, inventory, payroll, etc. Store at least one copy of this information on-site (your working files) and one full backup copy off-site.

STORAGE FOR THE MASSES

Network Attached Storage appliances offer attractive features for SMBs.

Network Attached Storage (NAS) appliances are dedicated servers that provide file services to different client machines. They do what general-purpose servers do: Store and serve up files quickly and efficiently. But while other servers can also be used to access e-mail, printers, and the Internet, NAS has a sole purpose in life—to store and serve up files. NAS appliances range in price from $500 to $1,000.

If a business finds itself cramming too many functions onto one server as its needs grow, a NAS appliance is an attractive alternative. "By deploying a NAS server next to a general-purpose server, you're offloading the file sharing function onto the NAS appliance, and it frees up resources onto the general-purpose server more efficiently," explains Brad Nisbet, a program manager at research firm International Data Corp., in Framingham, MA.

Often, NAS appliances can be filled with very-large-capacity hard drives, which is critical for growing businesses. They also offer data protection more easily than general-purpose servers, adds Nisbet. NAS appliances typically use RAID (Redundant Array of Independent Disks), which are multiple disk drives working together to protect the data so that if one disk drive fails, it can be recouped by another.

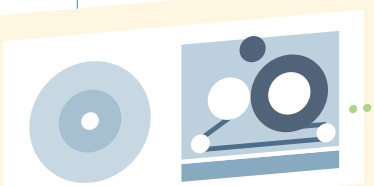
—*E.S.*

backup. The system worked well when the company was smaller, but as Daymon grew, compliance became spotty.

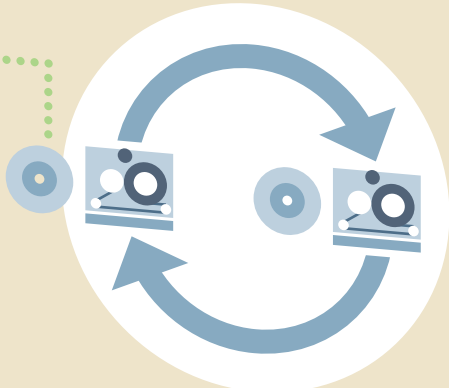
Step one was to swap out the old backup system with new software—Backup Exec from Veritas. Backup at all of Daymon's locations is done nightly, says Bauer, beginning at 5:30 p.m. and running through the night until 7 a.m. the next day, due to the large number of servers. The company also runs Backup Exec Desktop and Laptop to automatically back up Daymon's remote data, allowing the IT staff to spend 30 percent less time on backup and restores.

On top of the new-and-improved backup process, Daymon also enlists Iron Mountain to pick up the previous night's tapes from the Stamford, CT, location to be stored remotely on a daily basis. "Data protection has gone from a disaster waiting to happen to a solved problem," Bauer says.

6 Perform daily incremental or differential backups and weekly full backups. Most important, test your ability to restore data at least once a quarter. Designate someone to take tapes off-site to a safe location.



7 Always rotate and catalog tape cartridges or discs. Be sure to replace tapes or discs on a regular basis to maintain optimum performance. Designate a specific employee to periodically check the system and make sure there are at least a few tapes in the drive—and that they work.



"Sooner or later, everyone will be presented with the problem of a computer failure. When they are, it's a very poignant lesson to learn."

QUESTIONS AND ANSWERS

Beyond cost, here's what to ask when considering an outsourcing partner for backup and recovery:

HAS THE CONSULTANT/SYSTEMS INTEGRATOR DONE WORK IN SIMILAR INDUSTRIES TO YOURS? This may be important because some industries have different backup/recovery needs. For example, an e-business is not going to have the same requirements as a manufacturer.

DO THEY HAVE STRONG REFERRALS? It's critical that a potential partner have clients who can attest to the type of work they do in this specific area.

WITH WHOM DO THEY PARTNER? There are so many different products on the market, and consultants have their preferences. But some systems integrators may guide you to more cost-effective products that aren't necessarily well-known, but still do the job.

WHAT KIND OF SERVICE-LEVEL AGREEMENTS CAN YOU GET? Some systems integrators put everything together for you, but then don't provide good support services going forward. In that case, you're in trouble if you don't have a dedicated IT staff to deal with a technical issue.

SOURCE: International Data Corp.; Connect reporting

What happens, though, if a business can't afford a consulting partner or is precluded from reserving space in a data center? A cost-effective approach to disaster recovery is to partner with a similar company, says Arun Taneja, founder of the Taneja Group, an analyst and consultancy focused on storage-centric server technologies, in Hopkinton, MA. That way, both firms have a backup plan for running the core business applications in the event of an emergency.

Another alternative is to align with companies that will electronically store data. Companies such as LiveVault Corp., of Marlborough, MA, offer off-site storage, archiving, and guaranteed data recovery, an ideal data protection option for small and medium businesses and enterprises with remote offices.

If a company has unlimited resources, they can take data protection to the next level by purchasing a large disk system such as a Symmetrix or DMX from EMC Corp. Such systems can back up data faster and do data replication to another system.

Regardless of business size and the amount of bucks, the reality is no company is immune to disasters and everyone's data is important to them. "Sooner or later, everyone will be presented with the problem of a computer failure," says GlassHouse's Baker. And when they are, "it's a very poignant lesson to learn."

Esther Shein has been a freelance writer and editor, specializing in technology and business, for several years.