books24x7®

ExecBlueprints™

in partnership with Aspatore Books

Action Points

I. **When Planning for Business Continuity, What Issues Can IT Face?**
Although your company may be located in an area that is at risk for certain natural disasters, you still don't know if it will ever be hit, or what precise problems that event will cause. Given the inherent difficulty in planning for the unknown, important questions include: Which systems are critical? How will you function without public services? Without key personnel?

II. **The Bottom Line**
Because you don't know if disaster-recovery plans will ever be implemented, leadership will need to decide what problems to prepare for, and how much to spend, after determining: What are the standards for your industry? How long can you afford to be down before suffering other consequences? How did you perform the last time the lights went out?

III. **Must-Have Approaches to Testing Back-up Systems and Processes**
Conducting regular tests of your business continuity and disaster-response plans can be expensive and intrusive, but it is essential to ensure you are protected. Moreover, these tests should not only involve systems, but also serve to inform personnel about their roles. Finally, results should be reviewed by the appropriate governance committee.

IV. **The Golden Rules for Partnering with Users and Vendors**
No IT department is an island when it comes to disaster-response planning. Instead, you must plan to constantly collaborate with the company's business units to ensure you share priorities, and with vendors to leverage their expertise. In addition, invite everyone to participate in brainstorming sessions to plan for different scenarios.

V. **Essential Take-Aways**
The first step in planning for business continuity during a disaster is to establish priorities for recovery that are based on realistic business needs and budget. Then you will need to ensure that the right infrastructure will be available and train (ideally) the entire staff on a proper response. Finally, include a plan for restoring main systems once the threat passes.

Contents

The technology leaders from Greenleaf Trust, LION, Martignetti Companies, and Jensen Distribution Services on:

Disaster Recovery Planning: Ensuring Your IT Department Is Prepared to Keep the Company Running

Brian S. Loken
Executive Vice President, Chief Information Officer, and Director of the Business Information Services Division, Greenleaf Trust

Mark Boyed
Chief Information Officer, LION

Alfred Mendes
Senior Vice President, Information Technology, Martignetti Companies

Mike Lamb
Former Vice President and Chief Information Officer
Jensen Distribution Services

A core challenge to disaster planning is that you can never really be sure what you're planning for: Flood? Tornado? Cyber-attack? Each type of disruption will cause different problems — including those that you have not anticipated. Of course, you may also encounter nothing at all for many years, which, while fortunate, could cultivate complacency — and reduced budgets — for future disaster-response efforts. Given these unknowns, this ExecBlueprint offers IT strategies for maintaining business continuity if and when disaster does strike. They will require first partnering with company leadership to establish priorities and the appropriate balance between being prepared and conserving resources. IT's responsibilities will then focus on developing and testing redundancies for essential systems and processes and deciding if these will require separate facilities. In the midst of all this planning, it's essential to also include the people that will be affected. They need to know that a plan is in place. Then, they should be trained on the execution of that plan so that they will know what to do should that day ever come. ■

About the Authors

Brian S. Loken

Executive Vice President, Chief Information Officer, and Director of the Business Information Services Division, Greenleaf Trust

Brian Loken is an executive vice president, the chief information officer, and director of the business information services division for Michigan-based Greenleaf Trust, a privately held wealth management firm, with specialized disciplines in retirement plan services, personal trusts, and asset management. Mr. Loken's division is responsible for aligning technology, information security, and information use needs with the vision and growth of Greenleaf Trust.

Mr. Loken has over 17 years of industry experience, along with several industry technical and security certifications. He also serves on the board of Kalamazoo- and Battle Creek- based Family and Children's Services and volunteers with several community organizations. He is a graduate of Western Michigan University.

☛ *Read Brian's insights on Page 3*

Mark Boyed

Chief Information Officer, LION

Mark Boyed has led teams in sales, operations, supply chain, and information technology. His experience in the application of technology to exploit strategic business opportunities and his focus on business intelligence has helped him grow small businesses and expand the reach of large enterprises.

Mr. Boyed was named the 2008 Innovation Awards Executive of the Year and has written for magazines and news agencies about the topic of innovation for the last 15 years.

☛ *Read Mark's insights on Page 6*

Alfred Mendes

Senior Vice President, Information Technology, Martignetti Companies

Alfred Mendes is currently a member of the executive committee and responsible for the technical infrastructure and systems for the nation's seventh largest wine and spirits distributor.

Mr. Mendes previously spent 20 years at UNICOM, a valued-added reseller where, as a member of the senior management team, he was charged with setting the strategic direction of the network services and application development practices. In this role, he led the team responsible for the processes and systems that supported UNICOM's internal operations. Mr. Mendes managed a group of architects, consultants, system engineers, application developers, DBAs, and project managers, and also managed the technical and business relationships with Cisco, Citrix, HP and EMC.

☛ *Read Alfred's insights on Page 9*

Mike Lamb

Former Vice President and Chief Information Officer, Jensen Distribution Services

Through Mike Lamb's work experience in multiple industries (manufacturing, distribution, health care, financial, and utilities), he has acquired a wide range of experience in information technology leadership, mentoring, coaching, training, and strategic planning abilities.

Mr. Lamb has over 16 years of professional business management experience. As a former vice president/chief information officer for a distribution services company, his experience has included determining the scope of projects and managing these projects so that they adhere to their budget, scope, and industry regulatory requirements. In addition, he has expertise in design and implementation of information management technology solutions as well as extensive experience in managing technology day-to-day operations and strategic initiatives.

☛ *Read Mike's insights on Page 11*

Brian S. Loken

Executive Vice President, Chief Information Officer, and Director of the Business Information Services Division, Greenleaf Trust

Roles of the Technology Team

Plan, train, test, review, then repeat. In its simplest form, these are the keys to making sure we are prepared to keep our company running. Our Information Security Steering Committee (ISSC) is ultimately responsible for the disaster recovery (DR) plan, and ensuring alignment with our business continuity plan (BCP).

The importance of this function is best illustrated by a story an acquaintance of mine told me a few years ago when working on a project. A company's IT department he was consulting with spent a few years revamping their disaster recovery plan while the company was updating its business recovery plan. When the big day came to do their first full disruption test, the IT department very successfully recovered all of their systems and data to a location about 400 miles away from where the business continuity plan called for it be. In other words, that company clearly did not ensure alignment between their DRP and BCP.

It is important for us to ensure that we have the ability to recover our data and information systems in the priority order that they are needed, and provide access when and where needed. It is also important to prioritize what is most important from a client's perspective. For example, several years ago we started developing a DR plan based on the systems and information we decided were needed to get our critical systems up and running. Makes sense, right? However, what we found after much discussion (including with some clients) and internal debate, is that one of our most important needs is the ability to place trades when the market is open. That ability had initially been placed a little lower in the priority order than it ended up being in the final plan.

In order to have an effective disaster recovery plan, you must gain clarity on recovery priorities and a clear understanding of recovery time and objectives.

Brian S. Loken
Executive Vice President, Chief Information Officer,
and Director of the Business Information Services Division
Greenleaf Trust

Physical Vulnerabilities

From a DR perspective, our vulnerabilities stem from physical geography. If we had a local disaster, our employees could potentially be affected the most. We know, for example, that tornados are a possibility. In 1980 a tornado came through downtown Kalamazoo very close to where our offices are, and struck the building right next to us. Flooding is also a possibility because we are in a valley, and while we have no recent memory of flooding in downtown Kalamazoo, it is still something that we have to take into consideration. In addition, more traditional threats, such as fires, break-ins, and protests, are always a possibility at any site, so we focus on minimizing these types of risk, too.

A very successful strategy we have employed is to develop partnerships with first responders. Several years ago we hired the retiring Department of Public Safety chief as our director of corporate security. He has facilitated and maintains

Brian S. Loken
Executive Vice President,
Chief Information Officer, and Director of the
Business Information Services Division
Greenleaf Trust

"Every time we have gone through elements of our business continuity plan, someone has learned something new or identified an improvement opportunity area."

- *Over 17 years of IT experience*
- *Responsibilities include aligning IT, security, and information use to support company growth*
- *Graduate, Western Michigan University*

Mr. Loken can be e-mailed at brian.loken@execblueprints.com

many great law-enforcement and first-response partnerships, and has made many enhancements to our physical security operations to further mitigate the possibility of damage from the more traditional threats mentioned above. Whether you have retired law enforcement members on your security team or not, building and maintaining those relationships is important when it comes to your ability to respond to a disaster.

Greenleaf's Current Business Continuity Plan

We have been fortunate in that we have only had to address individual system-level disasters in the recent past. And, I am happy to report, we were able to recover those systems within the time frames they were needed. We have not yet experienced any larger-scale disasters that required people to relocate. Some of the rolling black-outs that occurred a few years ago on the East Coast came as close as Detroit but didn't affect us.

Many years ago we were a much smaller company and one of our growing pains was that a lot of institutional knowledge was not written down. So we began developing our current business continuity plan by asking all the departments to document their processes and procedures. We then worked with a consultant who facilitated the BCP discussions by bringing in representatives from all areas of the company to conduct table-top exercises. We discussed potential threats, such as the loss of key personnel, and what we should do to handle such a loss. We also focused on what we determined are our highest recovery priorities, and who our spokesperson would be for communicating with the press. This was a great exercise for our company in general and we continue to do it on a recurring basis.

Ensuring Business Continuity: The 4 Essential Steps to Disaster Recovery

1. Establish recovery priorities and consensus on acceptable recovery times and objectives – in other words, determine which needs are truly immediate.

2. Regularly test the plan using table-top and disruption testing exercises:
   - Ensure that everybody knows their roles and understands what they need to do and when they need to do it.
   - Develop contingency plans for many different scenarios, including responses to losing leaders and staff.
   - Identify future leaders, i.e., those who will step up and take charge.
   - Determine potential leadership structures.

3. Ensure that the proper infrastructure exists to recover all of the necessary systems:
   - Proper security is in place
   - Disaster recovery is incorporated into change management processes
   - Project management practices include BCP and DR planning for new applications and systems

4. Build BCP and DR plan reviews into the responsibilities of the appropriate corporate governance committee.

The Importance of Clarity, Testing, Backing Up, and Securing an Infrastructure

In order to have an effective disaster recovery plan, you must gain

clarity on recovery priorities and a clear understanding of recovery time and recovery point objectives. From early on, the most common answer we would receive to the question of how quickly a system needed to be recovered was "immediately." However, when we looked at and demonstrated the financial ramifications of "immediately," the answer would often change to one that made more fiscal sense for the business.

Years ago, one of our key systems went down and we discovered that we could work around it for much longer than we had originally thought. This was one of those systems that "we have to have up and running immediately in a disaster" according to the users of that system. But it turned out that we were able to function without that system for a while with no adverse client impact or complaints. That was a great lesson for us when it came to setting realistic recovery time objectives and recovery point objectives.

Next, the plan needs to be tested. This involves going through table-top and disruption testing exercises and making sure that everybody knows their roles and understands what they need to do and when they need to do it. You also need to work through contingency plans for many different scenarios. One of the scenarios we worked through several years ago was loss of key personnel. We looked at loss of leaders as well as of any members of our staff. For this series of exercises, everyone signed up to attend one of three meetings. This provided us with a somewhat representative set of staff from all of our divisions at each meeting. We met in a large room and, after everyone arrived, we randomly selected about a third of the people, always including key leaders, and had them move to a corner, or told them they could not talk. This was the group that "died" in the disaster and whose institutional knowledge was lost. The exercise made everyone really think through what they would do, what information they would need, and even helped us identify some future leaders — the ones who stepped up and took charge when everyone else floundered.

To be truly effective any BCP and DR plan must work through answers to the questions: What happens if the people that understand the plan the best or if key leadership positions are no longer with us? Who steps in and takes over? What would the leadership structure be?

Third, you must ensure that the proper infrastructure exists to recover all of the necessary systems, that the proper security is in place for this infrastructure, and that the infrastructure is available. It is very important that you ensure DR is incorporated into your change management processes and that your project management practices include DR and BCP planning for new applications and systems.

Last, recurring BCP and DR plan reviews must be built into the responsibilities of the proper corporate governance committee or group (which, in our case, is the ISSC), testing of the BCP and DR plans and recovery infrastructure needs to happen on a regular basis, and those results must be reviewed by the appropriate leadership committees or groups. ■

Expert Advice

Appropriate Benchmarks Initially, business continuity and disaster recovery plan benchmarking was done by consultants who were hired to help us put our initial plans in place. Once plans were implemented, benchmarking activities transitioned into gaining knowledge and best practice information through research and attendance at seminars and conferences. In addition, we are audited by state and external auditors who we hire to determine whether our plans meet the business recovery needs of our clients and to give us their opinions on our procedures, including ideas for improvement based on current best practices.

Mark Boyed

Chief Information Officer, LION

Recovering from Disaster

At LION, our systems are well protected with a very strong disaster plan. As a manufacturing company, the real cost of disaster recovery is at the operational level. If some event were to wipe out one of our manufacturing sites, the cost of recovery would dwarf the cost to recover data.

The tornados that hit West Liberty, Kentucky, in 2011 were devastating to the town. The people of West Liberty are to be commended for their bravery and perseverance during and after those storms. LION was fortunate in that our manufacturing facility located there was not more critically affected. When the tornado struck nearby, the team for the plant notified our leadership team and we were able to immediately implement our disaster recovery plan. The IT systems were online and ready for operations within eight hours after the tornado touched down. Our operational systems were up and running and ready for people to return to work in the plant within 24 hours. It may have been a Herculean effort, but we were much more fortunate than other companies in the area. As a result, we looked at our plan and asked what we could have done better.

We want to ensure that we are more proactive about planning so that our business continuity plan does not have to focus on disaster recovery.

Mark Boyed
Chief Information Officer
LION

Developing a Business Continuity Plan

FEMA provides downloadable lists of all the steps a company needs to take to effectively overcome a disaster. I believe that the first and most important step is focusing on IT systems as a whole. The second is functionality. Will public services

Mark Boyed
Chief Information Officer
LION

"As CIO, I also believe that I am responsible for coming up with sound solutions for the enterprise outside of IT to be able to continue operations."

- *Demonstrated leadership experience includes operations, supply chain, and technology*
- *Has used business intelligence to grow small businesses and expand reach of large enterprises*
- *2008 Innovation Awards Executive of the Year*

Mr. Boyed can be e-mailed at mark.boyed@execblueprints.com

After a Disaster: Key Considerations for Getting a Company Up and Running

1. Are public services, such as water, available?
2. Can trained staff come to work? If not, how quickly can others be trained on necessary functions?
3. Do you have a back-up location if your main site goes down?

be available? If you are in a municipality without water, then basic hygiene needs cannot be met. In the bigger picture, if you don't have access to water, you could lose your entire company if there's a fire. If trained staff will not be able to make it to work, how quickly can you train others on necessary services? The third step is location. If your central location is affected, is there a backup location?

Those are the first three steps to getting a company up and running: IT, service, and location. Once you have a place to go, services to provide, and people to provide them, then you can start to focus on connecting to servers, maintaining services, and keeping the service capability equal to the systems.

Every 12 months, we make sure our plan is updated and we run quarterly checks in case it is not. We also run regular maintenance checks to ensure that systems that aren't always on are available and ready. Think of it as the equivalent of checking the batteries in the flashlight before a storm. We never want to find that our batteries have run out. We also want to ensure that we are more proactive about planning so that our business continuity does not have to focus on disaster recovery. The goal is to take action prior to outages.

Vendors and consultants can play a huge role in disaster recovery planning. The reason is simple: while my companies can only know what they have been through, consultants have seen hundreds of companies in multiple industries go through just about everything. They have so much more expertise. In fact, we recently worked with people at Ohio State University to evaluate our operations flexibility and disaster recovery. They evaluated our plan against those of other companies regionally as well as nationally. The work helped us better see our vulnerabilities and decide what areas need to be strengthened. Then we were able to take these external benchmarks and go to the board with a realistic idea of specific measures we could put into place.

Expert Advice

Every year we modify our business continuity plan. The disaster plan and business continuity team includes members from every business unit. The current plan has incorporated lessons that we learned in West Liberty to allow for added redundancy in the operational model that did not exist previously. In the past, we had facility operators at just one facility; now, however, we have multiple teams at geographically separated facilities. Additionally, equipment critical to operations now exists in multiple locations should there be a need to restore operations.

West Liberty, Kentucky after 2011 tornadoes

Role of CIO

As the CIO, I own the technology planning, including the disaster recovery plan for technical systems — and also for the enterprise outside of IT. For example, in most companies IT has uninterruptable power supply (UPS) for its systems and generators, but most do not extend this UPS capability to operations. In our case, we have site generators feeding data centers as well as the buildings where people are working. This cross-utilization of resources prevents duplicating costs and provides greater flexibility. The goal is to remove risk at the lowest viable cost.

Building redundancy into disaster recovery systems means doubling the money spent on the same systems. But we don't want to have to buy two of everything. Instead, we prefer to look at alternatives. For example, instead of buying two buildings, one for current use, and one for potential use in a disaster, we instead pay a monthly fee to rent mobile command centers in case of emergency. The fee is nominal compared to that of a new location, but the end result is the same: operations continue regardless of the storm. ■

Alfred Mendes

Senior Vice President, Information Technology, Martignetti Companies

Areas of Vulnerability in the Face of a Disaster

Frankly, there are few areas in our business that are not vulnerable in the face of disaster. We need to be able to take orders and process those orders. We need to be able to put them through our system; process them; send item, order, and demand information to the warehouses; and we need to be able to ship and deliver those products. In addition, we also need to be able to reorder products, so any interruptions to our supply chain would be detrimental. Having said that, if something does happen, we have plans in place to mitigate the problems, depending on the scenario.

It is my role to maintain IT functions in the face of a disaster. We need to make sure that our warehouse systems are up and running along with most of our technology. We need to have our enterprise resource planning system working, we need e-mail, we need to have working phones, and our warehouse systems need to work — we are greatly dependent on them. We have two separate warehouses and they are unique with respect to the products that they carry. However, if something happened to one, we could redirect inbound product to the other warehouse.

As we rotate production servers, we take the previous systems and repurpose them as disaster recovery equipment.

Alfred Mendes
Senior Vice President, Information Technology
Martignetti Companies

The most common type of event we plan for is a sustained power outage. Due to the amount of materials-handling automation in our warehouse, it is not practical (due to the electrical load required) to have backup power in place. However, outages do happen from time to time and we have tuned our processes and systems to quickly recover, even from extended outages.

Disaster Recovery Planning and Challenges

Without getting too specific, when preparing and testing our systems to ensure they will function effectively in the event of a disaster, we do what I think most people do. We conduct various scheduled tests to make sure functions that are supposed to happen regularly and routinely are actually happening. For example, while many organizations engage in data replication, when is the last time they actually ran for a day off the replicated data? Or replicated this data back to their production system after running on the replicated data/disaster recovery site? These tests are expensive, intrusive, and are not easy to run. Yet they are critical to perform in order to fully test your recovery plans. Disasters generally cause unforeseen problems as well as those that you planned for.

We face numerous challenges when trying to develop the right strategy for disaster recovery because we have so many systems. As tight as we are, systems are interconnected, so it is hard to plan for a disaster if you are not exactly sure what you are planning for. In some ways, it is actually easier to plan for a complete disaster where everything has to be replaced. It is far more difficult to reassemble

Expert Advice

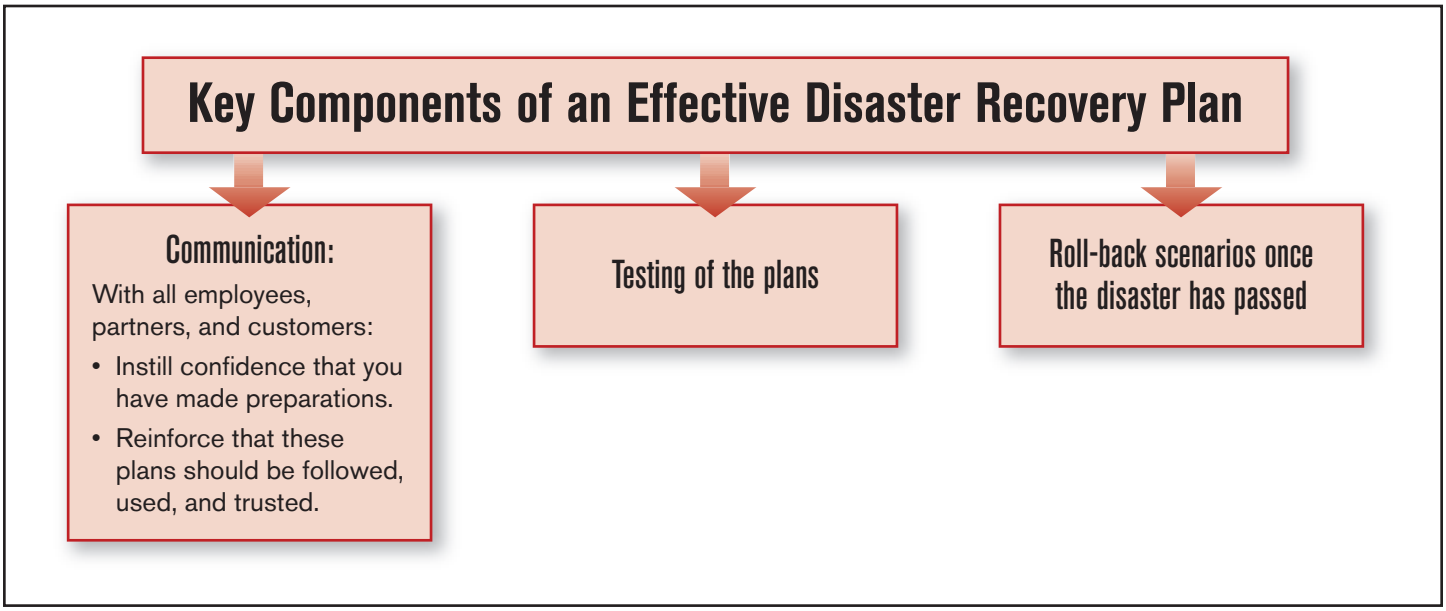
We used a consultant to help us put our disaster plan together, and they remain engaged with us as we often have updates. Our vendors play a key role in our operations every day and others would play key roles in the event of a disaster, all the way from facilities to technologies. We use the word "vendor" loosely because we also like to use the word "partner" to refer to some vendors; we have vendors that are partners and we have vendors that are vendors. The vendors that are partners are an integral part of our disaster recovery plan.

Alfred Mendes
Senior Vice President, Information Technology
Martignetti Companies

"We have very clear plans that cover every department should an event occur."

- *Previously set strategic direction for network services at UNICOM*
- *Responsibilities included managing system engineers, application developers, and project managers*
- *B.S., Technical Management, DeVry University*
- *M.B.A., Keller Graduate School of Management, DeVry University*

Mr. Mendes can be e-mailed at alfred.mendes@execblueprints.com



missing pieces. Like most companies, we rotate our technology on a regular basis, but we need to question whether or not we could get something that is a couple of years old in crunch time. Our plan needs to take this into account. Again, it is so important to have a good backup plan.

Best Practices for Managing Costs

There is no way to make a disaster recovery plan inexpensive. At the end of the day, it is about balancing our tolerance for business interruption against our need to service our customers. Employing a multi-layered approach, we can use backup systems for certain periods of time. In the event that something happens that is not covered by the plan, or if it is not possible to follow the plan, then we need to balance the amount of effort required to remediate the problem versus the time delay before business interruption insurance takes over.

Few organizations affected by the events of 9/11 had plans that covered a catastrophic event of that scale. Quite honestly, we are probably not adequately prepared for an event of this nature, but we have done all of the reasonable preparation that we can do within our means. This is really where the consultants helped us. They told us when we were over-thinking issues and that we could not attempt to prepare for every possible event. They made us focus. You need to pick what you are going to be prepared for and how much you are going to spend on insurance.

One thing that came out of our planning was the way we invest in backup equipment. As we rotate production servers, we take the previous systems and repurpose them as disaster recovery equipment. As we typically rotate equipment before we experience performance issues, we can repurpose the retired equipment for DR functions. ■

Mike Lamb

Former Vice President and Chief Information Officer, Jensen Distribution Services

Areas of Vulnerability

All company areas are at risk in the case of a disaster, including both the physical and the virtual technology worlds. Physical locations are subject to the widest variety of threats. The threats could be posed by a fire, flood, or any other environmental situation. On the technology side, the virtual world is at risk of getting hacked, which is becoming more and more common. Until recently I worked in distribution services, which is not in one of the hackers' high-target industries like banking or utilities. That industry is probably fairly safe for now, but could be heavily targeted in the future by hackers who are getting smarter, more sophisticated, and more likely to go after smaller targets all of the time. There are always threats out there.

In the case of a disaster, it is essential to control the chaos and have a plan in place to bring order to the chaos. A company must identify potential risks and hazards ahead of time. You want to preplan for those things and go through those scenarios with training and dry runs. The plan and information also must be available when a disaster happens, to allow everyone to know their role and what they need to do.

[Another key consideration is] to not only plan but also conduct training around different disaster scenarios and make sure that backups and restarts are working before you need them.

Mike Lamb
Former Vice President and Chief Information Officer
Jensen Distribution Services

Role in Ensuring Information Technology is Running in the Event of a Disaster

I always make sure that plans are in place and that my company has disaster recovery capabilities for our core systems. In the event of a disaster, the CIO is responsible for identifying physical, virtual, and logical items that the company needs. The other key thing that I have learned throughout my career is to not only plan but also conduct training around different disaster scenarios and make sure that backups and restarts are working before you need them. Another way to mitigate a disaster is by utilizing technology and tools that are available such as virtual server environments that can give you added redundancy and the ability to restore capabilities to prevent loss.

Role of Vendors and Consultants in Disaster Recovery Planning

Vendors and consultants play a huge role in disaster recovery planning. A smart company, even if it has an information technology department, will rely on external third parties to provide additional

Expert Advice

I try to follow the Information Technology Infrastructure Library (ITIL) strategy for company systems. Using change management practices, I identify areas that require backups that will run in the event of a disaster, as well as ways to generate these backups. Various scenarios should be considered from the corruption of a partial system to the destruction of an entire server. It is essential to be able to recover the data.

Mike Lamb
Former Vice President and Chief Information Officer
Jensen Distribution Services

"When everyone knows that there is a plan in place and that there is a possible positive result, they are not as likely to panic when a disaster does occur."

- *Industry experience includes manufacturing, distribution, health care, financial, and utilities*
- *Over 16 years of management experience, including day-to-day IT operations and strategic initiatives*
- *Former VP/CIO for a distribution services company*

Mr. Lamb can be e-mailed at mike.lamb@execblueprints.com

support in some areas. Having multiple providers ensures that backup is available when staff is on vacation. Another thing that is essential is to have your own redundancy within the IT department. This capability enables your staff to deal with day-to-day processes to keep the business moving as efficiently as possible.

However, when dealing with unusual, demanding situations, it is beneficial to not get your staff too heavily involved. By relying on a third party to take care of those occasional, difficult tasks, we create long-term relationships with a third party that is enforced with a maintenance or disaster agreement. An example is the core virtual environment that we maintained at my last company: we were in frequent contact with the vendor regarding new trends, upgrades, and best-practice approaches. In addition, we kept them informed of changes or challenges we were having so if we had issues that we could not resolve ourselves we could leverage their expertise.

Challenges Faced When Developing Disaster Recovery Strategy for Information Technology

When developing a disaster recovery strategy for information technology, it is essential to expose the team to the strategy to ensure that everybody understands its importance. Also, sometimes disaster recovery is a huge expense, so it is important to identify the rewards of the strategy to ensure that the money being spent for disaster recovery is appropriate. This also applies to your service-level agreements with different application or business system owners around the company that actually own the system from a business perspective. ■

Ideas to Build Upon & Action Points

I. When Planning for Business Continuity, What Issues Can IT Face?

While you should probably anticipate that your company will experience power outages from time to time, the truth is that you cannot know the nature of every single threat to operations that your company will experience in the coming months and years. What's more, you cannot predict all of the problems that such threats will cause. Given all this uncertainty, key considerations for disaster planning are:

- What systems and processes are absolutely critical for the transaction of business? Which can be offline for certain periods without serious consequences?
- What will happen if x leader or employee is suddenly unavailable? Who will step in? What will the new leadership structure look like?
- What will you do if public services, such as power and water, become unavailable for extended periods?
- What institutional knowledge are employees and leaders still holding in their heads?
- Does it make sense for your company to develop backup locations?

II. The Bottom Line

While you hope you will never need to implement a disaster recovery plan, financial considerations are inevitable. How much money should your company spend on such a plan? What systems and processes can your company afford to lose? What length of business interruption can you endure? What kind of insurance should be bought? While some of these dilemmas may lie outside the domain of IT, methods for assessing the value and appropriateness of your disaster planning to the organization are:

- Determining your company's customers' needs relating to your products and services: what are the consequences for not meeting these needs during a disruption?
- Benchmarking your plans against comparable companies in your industry: where do you stand?
- Analyzing cost savings of alternative approaches to duplicating systems: instead of buying another building, how much is saved by renting mobile command centers? How much is saved by repurposing older systems into back-up equipment?
- Evaluating your response to past disruptions: how long did it take for critical functionality to be restored?

III. Must-Have Approaches to Testing Back-up Systems and Processes

Disasters can bring on their own chaos, which is why the last thing you want is for your plan to fail because something basic was overlooked, i.e., the large-scale equivalent of dead batteries in your flashlight. To avoid such problems, it is critical to run regular maintenance checks of your business continuity and disaster-response plans that include:

- Working through contingency plans for many different scenarios
- Making sure everybody knows their roles, and understands what they need to do and when they need to do it
- Checking the integrity of backed-up data — and replicating it back to your main systems
- Building in recurring business continuity and disaster planning reviews into the responsibilities of the designated governance committee or group

IV. The Golden Rules for Partnering with Users and Vendors

When it comes to business continuity planning, IT cannot stay in its silo. For starters, you need to continually communicate with leaders throughout the company to ensure that your priorities are actually focused on business-critical functions. Then you should strongly consider leveraging vendor expertise; after all, while you may have had some experience with recovering from disasters, consultants have seen hundreds of companies go through just about everything. Communications relating to disaster planning must be carried out with your various constituent groups.

With employees and customers:

- Ask all departments to document their processes and procedures.
- Include members from every business unit in your business continuity planning processes.
- Engage all levels of the company in tabletop exercises that require people to think about strategies for coping with the sudden loss of specific leaders and staff.
- Gain trust by communicating your plan with all stakeholders: employees, partners, and customers.

With vendors:

- Solicit their observations regarding your company's specific vulnerabilities and advice on areas to be strengthened.
- Commission evaluations of your plan against those of comparable companies.
- Keep them informed of your changes and challenges.
- Ask them about new trends, upgrades, and best-practice approaches.
- As appropriate, plan to engage them in actual disaster-response activities.

V. Essential Take-Aways

Of course, if you ask business units when they need their systems up and running after a disruption, they will usually say, "immediately." But is this really the case? Because not every system is business-critical for every moment of the day, your first responsibility as IT leader is to achieve clarity on recovery priorities once you and company leadership have determined business recovery objectives and budget. Once priorities are established, best practices for preparing for a disaster include:

- Incorporate disaster recovery into your change-management and project-management processes.
- Ensure that the proper infrastructure (that is protected by adequate security) exists and is available to recover all of the necessary systems, utilizing separate locations or vendor-provided facilities, if appropriate.
- Continue to update plans to align with emerging needs and priorities.
- Develop relationships with first responders, such as local law enforcement.
- Designate a suitable company spokesperson to communicate with the press concerning recovery efforts.
- Undergo regular table-top and disruption testing, involving all leaders and employees in business-continuity training, if possible.
- Include plans for rolling back to main systems once the emergency situation abates. ■

10 Key Questions and Discussion Points

1. Which areas or functions at your company do you consider to be especially vulnerable in the face of a disaster? What types of disasters make these areas vulnerable? What factors drive this vulnerability?
2. What functions are essential to maintain during a disaster? What network resources or databases are located in vulnerable areas?
3. As CTO/CIO, what is your role in preparing the IT department to keep the company running in the event of disaster? How do you work with other areas of the business to ensure that the company is adequately prepared to respond to a disaster?
4. How was your company's current business continuity plan developed? How has it changed over the last three years? What formal documents, policies, and procedures exist?
5. What role can vendors and consultants play in disaster recovery planning? What are the advantages? What are the disadvantages?
6. What are the top five most important features of an effective disaster recovery plan? Why are these features necessary?
7. Have you had to address any disaster-related concerns in the past five years? Which systems were affected? How did you handle the situation? What could have been improved?
8. What preparation and testing do you do to ensure your systems are effectively prepared for disaster recovery? How often are these tests run? How often are emergency notification systems tested?
9. What are your best practices for managing costs associated with building redundancies and maintaining disaster recovery systems? What areas are typically the most expensive to maintain?
10. How do you measure the ROI for your continuity strategies? What does downtime cost your company? What does disrupted communications cost your company?