

The Data Dil

CONTINUITY INSIGHTS STAFF

Continuous data protection, high availability, data backup, data security...what does it all really mean? And what does it mean to business continuity professionals? We all know that business continuity has its roots in IT, springing from data center disaster recovery plans. And as business continuity has evolved and changed, it has, in many cases, moved out of IT. Today, the people who are responsible for business continuity, crisis management, security, and the like often don't have strong IT backgrounds. So how are they to know if their data is really protected, accessible, and valid?

Continuity Insights surveyed readers and talked with data protection experts to come up with some answers...or at least raise some important questions. Our survey shows that only 30 percent of respondents' job titles are specific to IT. And just 60 percent of respondents said that data protection is a top priority for their CIOs. So, if you're like most continuity professionals, and after your people, your data is your most valuable asset, read on to find out what you might be missing.

Coming to Terms

As an industry, we can't agree on standard definitions for our own terminology — business continuity, crisis management, resiliency, and so on. Now heap a big pile of data-related terms on the plate, and you've got jargon with a side of confusion. The problem is compounded by vendor marketing that creates, adopts, and spins buzzwords to match product and service offerings.

"What it really comes down to for a lot of companies is that they start looking at data protection and high availability and they get somewhat daunted by talking to different vendors and hearing different terminology," says David Aschmann of CA XOSoft. "They've read the magazine articles, and they really want you to boil down what do these things really mean. When they hear continuous data protection, what do you mean by it? Then they discover that this vendor defines it differently than that other vendor. It comes down to describing what the benefit is to them."

"Each supplier out there has the latest and greatest perspec-

tive on what data protection is and how it is achievable — usually by buying their solution," says SunGard's John Lindeman. "And as you start to pull away from the marketing and the positioning, you start to really get down to the core." The core? "Your business requirements for your data."

"The first important thing that we need to distinguish is what part of data protection they are talking about," says Tom Jensen of Brocade. "Is it security of data and risk? Is it making data highly available during normal business operations so that the failure of a device doesn't affect business function availability? Or are we talking about backup and recovery? That is typically what people are talking about when they talk about data protection — the ability to take copies of my data and recover it at some later time because some event has occurred that forces me to recover that data."

"What it really comes down to, is that the customer needs to figure out *first* what exactly they are trying to accomplish," Aschmann says. To do that, you need to ignore the terms and figure out that your needs really are. "It's not about terminology. If you start looking at the terminology, you are going to get really, really confused very quickly."

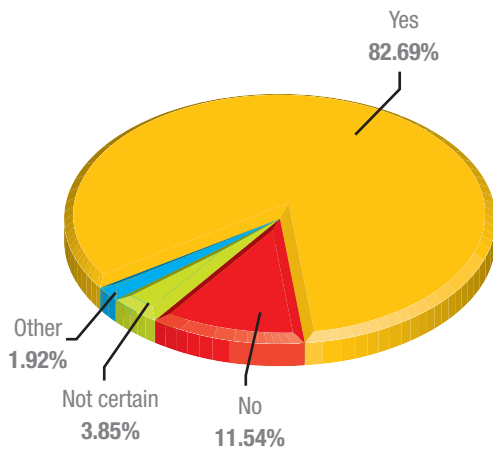
Defining Your Needs

"The key piece and one of the things that we find not well-defined and missing in the business process is what are our backup and recovery requirements?," Jensen says. "So before you can even think about solutions, you really have to know what your requirements are. Before anyone looks into specific technologies, they really need to understand those requirements for the business data. And I think that's a business process that is often missing. There is no process. There is no group responsible specifically for that, with the exception often of the disaster recovery scenario."

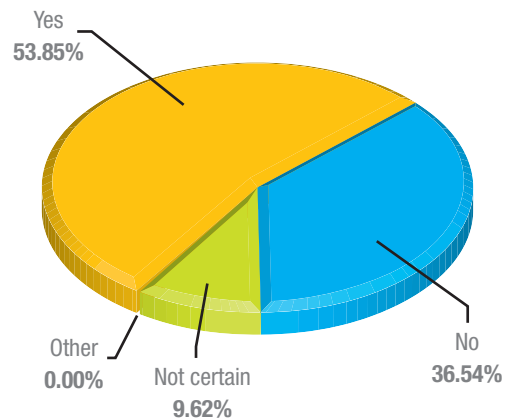
"Business continuity is often associated with DR and often there is somebody who is responsible for disaster recovery and maybe the recovery objectives are understood in a disaster scenario. But there are a whole lot of other, what we call data recovery events, that aren't associated with a site disaster and these need to be looked at too and

emma

Do you believe that your organization has an adequate level of data protection to prevent data loss during normal operations?



Do you believe that your organization has an adequate level of data protection to prevent data loss during a disaster or other major disruption?



recovery requirements need to be defined for them.”

“So I think the biggest thing we find is that there’s not a process for gathering and understanding those recovery requirements through the broad spectrum of events — including the smoking hole event that is the lost a data center. But there is a broad set of operations recovery requirements that don’t get defined and therefore it is difficult to put together a cost-effective solution to meet those requirements because you don’t really know what they are.”

Why isn’t this taking place? “It’s hard thing to do,” Jensen continues. “You have to communicate to the lines of business, after you educate them on what you’re talking about. Then you have to get them to sit down and realistically think about what their real business requirements are. Because, if you ask them, they will tell you they need a full back up of everything every day and they need to keep it forever. That’s a real costly recovery requirement to meet. And so you have to try to get the lines of business to understand what it is you are talking

about and then get them to buy in as a stakeholder.”

And it’s complicated, says Lindeman. “One size doesn’t fit all and one application. One set of information may not need the same sort of protection that another set of information needs. That’s when the end user really needs to look at data classification. They need to understand the value of the data as it relates to their organization. This has always been easily solved in the past by saying let’s just back everything up to tape on a Friday night and we know that is our starting point for whatever happens. But now in the world we live in, Friday night data becomes aged very quickly. And that’s why some companies are looking now, first, to try to classify their information.”

“The most important thing is the business impact of not having information available,” Lindeman says. “That *can* be quantified and that’s where some of the data classification algorithms help a company start sorting through this. If you look at some of the terms that came out in the last three

White paper:

Business Continuity and the SMB Market

A business outage is an SMB's worst nightmare. Whether due to natural disaster, a blackout or a software change that takes down a critical server, SMBs can't afford to lose customers or revenue to an outage.

While most organizations save data to disk or tape, simple backup isn't the same as business continuity. A true business continuity solution minimizes or eliminates downtime of key applications and services, and enables employees to continue performing business-critical job functions.

Traditional business continuity services typically include redundant data centers, alternate workspaces, and on-site delivery of equipment and materials. Such services are aimed at large enterprises — and carry a large-enterprise price tag. But SMBs have a growing number of options to choose from, including hosted applications, online backup and restore offerings, and managed services. Each has a differing level of business continuity associated with it from simple data protection and archiving to full scale high availability aimed specifically at the SMB marketplace.

Visit www.geminare.com to download a copy.



years — information lifecycle management and data classification — they point to the same things. All information is not created equal and information changes in its value over its lifecycle. So there are different tools and different approaches that can be put in place to help a company protect that information during its lifespan. Some of those tools are the tried and true tape back up. That may be the best tool and the best approach for information that is aged or easily recreated; whereas continuous data protection may be the approach that is mandated for that transactional, high-volume, high-value piece of information.”

What the Numbers Mean

Our survey shows that about one quarter of respondents have no process for classifying data. But yet, respondents seem fairly confident about their data. Some 83 percent say

they are confident that their organizations have adequate data protection to prevent data loss during normal business operations. However, only 54 percent say they have adequate data protection to prevent data loss during a disaster or other major disruption. And in tests, only 27 percent meet their recovery point objectives (RPOs) all the time; 21 percent meet the recovery time objectives (RTOs) all the time.

Why? It's a product of the different mindsets and missions of data center personnel and business continuity professionals, experts say.

“They have very different views,” says Aschmann. Data center types are focused on the day-to-day concerns their jobs entail; business continuity people are concerned with “what if.”

“To a great extent — and this is probably changing — the business continuity guys typically focusing on the smoking hole event, the site disaster, if I lose this data center, how do I recover? The IT director's most pressing problems are the recoveries that happen every day,” says Jensen. “There are six, eight, ten of those every day and succeeding in those events is the big challenge for the IT director. Yeah, the smoking hole disaster recovery scenario, we've got to think about, but that's the insurance thing. And it doesn't happen too often and nobody can really measure me as to whether I can really meet that requirement because we don't do it. But if every day I have to perform 10 or 12 recoveries and people measure me on those things.”

Aschmann says he sees a trend in IT people digging deeper into business continuity, however. “I am surprised at how many of the IT administrators, the more technical folks, have become more and more up to speed on business continuity as a whole.” He says shrinking RTOs and RPOs have “really forced them to look at business aspects and people and processes, whereas before they had a 24- or 48-hour window to be back up and running. Now they are told, ‘You've got 15 minutes and that's it. We don't care if we lose the site. We want e-mail and this critical Web portal back up and running in 15 minutes.’ IT administrators are not going to be able to put a solution together until they step back and for a minute and determine if it need to be accessible in 15 minutes, how do users access the system. It's a trend in IT that I am seeing a lot more now: IT administrators tend to be less and less kind of just tech geeks and are really getting more into the business. That is starting to be a real requirement of the role now. They need to be aware of the threats that are out there as they help evaluate the technologies. They can't just be looking at technology only anymore.”

Jensen says he sees a “spectrum of data recovery events” with a file or application recovery on one end and a lost data center on the other. He says while IT and business continuity people are often on opposite ends of the spectrum, there should

White paper:

Data Backup and SAN Security

In today's ultra-competitive business environment, data has become an increasingly valuable corporate asset. As such, you need to make every effort to ensure that your data is safe, secure, and highly available in order to meet both your business objectives and your compliance requirements. Part of this challenge is identifying your key business needs and developing a reliable data protection strategy.

To learn more about the various facets of data protection and areas you might need to consider in regard to your current strategies, be sure to download the following white papers:

- Data Protection: Understanding the Benefits of Various Data Backup and Recovery Techniques (www.brocade.com/dataprotection)
- The Growing Need for SAN Security (www.brocade.com/SANsecurity)

Brocade Services can help you better understand your data protection requirements, show you how to augment your existing infrastructure, and help you implement a reliable data protection strategy. To learn more, visit www.brocade.com/services.



BROCADE

be “one coordinated group that collects the requirements and keeps them consistent across that whole spectrum.”

Jensen explains: “In operational recovery for a particular application during normal business operations, you may not be allowed to lose more than five minutes worth of transactions *and* you have to have that application up within ten minutes because it is revenue generating. But maybe in a disaster scenario you have different requirements and you may have different technologies to meet those requirements. That’s important. It may not be, and often isn’t, one single technology across all applications across the whole spectrum of data recovery events that can that can meet cost-effectively the business requirements for recovery.”

What You Don’t Know...

None of the experts interviewed was surprised that most businesses believe they are in good shape when it comes to daily data protection. But they say reported successes might be hiding potential failures.

The Search for Meaning

There are resources to help you cut through the vendor “noise” and determine what all those technical terms actually mean.

David Aschmann of CA XOssoft suggests Storage Networking Industry Association (SNIA) Web site, www.snia.org. The SNIA dictionary is a “really good resource,” says Aschmann, as it defines common IT terms, including:

High Availability: The ability of a system to perform its function continuously (without interruption) for a significantly longer period of time than the reliabilities of its individual components would suggest. High availability is most often achieved through failure tolerance. High availability is not an easily quantifiable term. Both the bounds of a system that is called highly available and the degree to which its availability is extraordinary must be clearly understood on a case-by-case basis.

Continuous Data Protection (CDP): A data protection service that captures changes to data to a separate storage location. There are multiple methods for capturing the continuous changes involving different technologies that serve different needs. CDP-based solutions can provide fine granularities of restorable objects ranging from crash-consistent images to logical objects such as files, mail boxes, messages, etc.

Rebecca Levesque of 21st Century Software points out that analysts also provide valuable information for those trying to keep up with IT terms. “Analyst organizations like Forrester and Gartner are currently talking a lot about continuous data protection (CDP) and high availability, so they can be incredibly helpful in offering an objective view that distinguishes between marketing spin and fact,” she says.

“Gartner notes that while many technologies have provided snapshot copies, CDP offers additional flexibility and reliability by creating snapshots at logical or critical times, such as every time a new write function is done (“True-CDP”) or during file closing or other specific policy-driven timelines (“Near-CDP”). With Continuous Data Protection (CDP), data modifications are tracked and stored independently of primary data so CDP can provide excellent performance, flexibility, reliability, while providing additional protection capabilities that eliminate backup windows. In addition, the phrase high availability (generally associated with hardware solutions) communicates a certain absolute degree of operational continuity during a given measurement period. As such, CDP and High Availability are complementary,” according to Levesque.

White paper:

Five Assets of an Effective Data Recovery Strategy

In crafting your data recovery strategies, you're likely focused on contributing to operational efficiencies, while helping to shrink recovery windows. Also important is finding a data recovery solution that contributes to greater availability,



reduces risks, lowers overall costs of recovery management, provides a window into actual application and data usage — and aligns intelligently with real-world business challenges.

With the increasing costs associated with securing a successful backup and recovery, accomplishing an ironclad data recovery strategy is more difficult than ever. Developing an intelligent business continuity strategy is made easier when you consider the critical elements of an effective data recovery solution. Namely, that it is responsive, application-driven, actionable, verifiable...and maximizes your current assets. When your approach — and chosen solutions — sync with these five essential characteristics, the result is intelligent data protection.

In a recent whitepaper, "Five Assets of an Effective Data Recovery Strategy," 21st Century Software explains the key considerations that help ensure your continuity strategy is in sync with these characteristics. The paper details the three phases of recovery management — planning, data management, and reporting — and the possible strategies and methods to follow within each step to ensure an effective business continuity strategy.

Finally, we explain how our intelligent data protection solutions help ensure that your data recovery strategy — and solution — maximizes your current assets, while being responsive, application-drive, actionable, and verifiable. To access this whitepaper, e-mail sales@21stcenturysoftware.com.

"From an operational recovery standpoint, a business believes it has sufficient capacity to meet its objectives if it can just get its backups done every day. I think that's kind of a mindset," says Jensen. "So if I'm able to run my backup jobs and I get a 98 percent success rate on a

daily basis, then we're getting the job done."

"The problem is that just getting your backup jobs completed, does not mean for specific business functions, applications, file servers, that you can meet the recovery requirements of those specific areas. Even if you have service levels defined for a particular business application, because you don't recover on a daily basis, you don't really know if you are still able to meet the requirement you defined 18 or 36 months ago and your data base has grown in size and maybe you're running on a different platform. There are a lot of things that change over time. You really don't know if you are meeting requirements."

Much like BCP, backup is not a revenue generating application and IT groups often have a tough time justifying investment in that technology. When sufficient funding isn't there, that's when shortcuts and work-arounds happen — seemingly innocuous occurrences of business continuity people are typically unaware.

"Often operations will make concessions in the way they do things just to get those back up jobs done," Jensen says. "For example, in a shop that is using tape cartridges to store their media, ideally they want to have a tape library that has enough slots and media in it so that operators don't have to manually interface with the physical cartridges. At some point in time, though, they may run out of slots in the library. What they do is start to eject full cartridges out of the library and put them on a shelf somewhere. Then they put in some new scratch cartridges so that the night's jobs can actually run. Well, having those cartridges out of the library has just defeated the purpose of having an automated tape library and the efficiencies that are gained by having an automated tape library.

"It doesn't look like its costing anything to the business other than some new cartridges, yet it is has now started to degrade the operational efficiency of backup and recovery on the whole," Jensen continues. "Yet the business doesn't really see it until they have to do a recovery and the cartridge isn't in the library. Behind the scenes things start to happen if there is insufficient infrastructure and what we find is that IT does these things behind the scenes to make it look like everything is okay and keep the backup jobs running at a 98 percent success rate. But now there's a lot of abnormal things happening in the background to keep this appearance up. Business people and business continuity people don't find out, until they have a serious recovery issue, what the data center people may be doing."

Down to Size

While big businesses certainly are vulnerable to data disaster by shortcut, small to medium-size businesses (SMBs) are especially so.

White paper:

Guidelines for Successfully Migrating Data Centers

From mergers and acquisitions to cost-driven consolidation, there are many reasons organizations undertake data center migrations. Moving data center resources is an important project with little margin for error. Without proper planning and expert execution, migrations can have catastrophic, if not disaster-like results.

But, unlike hurricanes, fires or power outages, this is a “disaster” that can be planned for and managed proactively. With thorough preparation and a detailed information availability plan that integrates IT and facilities, organizations can avoid common pitfalls — such as budget overruns, missed deadlines, excessive downtime, people challenges and scope creep. Proper planning and preparation can help keep a data center move on time and on budget, with minimal disruption to day-to-day operations.

In this white paper by SunGard Availability Services, readers will learn:

- Risks associated with data center migration including logistical and interdependency risks
- The four phases of a successful move: assessment and strategy, detailed planning, preparation, and move execution
- Tips for success including: focus on planning, building a toolkit, engaging the right resources, communicating proactively and regularly, and anticipating failure

Moving IT systems — which house valuable data and power critical business processes — is not to be taken lightly. Such projects require coordination across multiple locations with multiple hardware and software vendors. A lot is at stake — and a lot can go wrong.

By using a proven information availability approach — one founded on in-depth planning well in advance of the move — an organization can execute a smooth, successful data center migration. For more information, please visit <http://www.availability.sungard.com/>

SUNGARD® | Keeping People
Availability Services | and Information
Connected.®

Best Practices

What are best practices for preserving and retrieving critical data? 21st Century Software’s Rebecca Levesque recommends the following best practices for preserving and retrieving critical data:

- Knowing your data (what data is critical, what data requires fastest recovery) before making technology decisions
- Fully understanding your technology choices—both their strengths and weaknesses
- Augmenting your existing hardware with powerful software solutions that can demonstrate a proven track-record of success
- In considering your options, remembering that no one solution or vendor can solve ALL of your problems or meet EVERY objective
- Placing the priority on ensuring that the most critical data is available first (this helps to reduce tape and disk storage costs)
- Being willing to look outside the box and find alternative solutions that address your unique problems and challenges in order to make your organization as recoverable and restorable as possible

need for it but it becomes very large and scary,” he says.

Geist says SMBs must be especially careful because they have limited budgets and less tolerance for failure. “They have a different set of needs and a different set of requirements,” he says. “As far as their requirements for data protection for business continuity for high availability, not only do they have almost an identical requirement to enterprise-class businesses, in some cases they even have a higher requirement. We’re talking about professional service firms, law firms, small financial and manufacturing companies. When we talk about their operations going down or their operations being interrupted, there are significant business-changing impacts that can happen to them.

“They would typically have customers that are very reliant on them and very key customers that are essentially keeping the business floating,” he continues. “If they are not able to service those accounts, then they have a significant and real risk of going bankrupt or losing that customer. Enterprise-class businesses, although they would absolutely have these key customers, if they actually had an interruption, they would absolutely be able to bounce back a lot easier than the SMBs

“SMBs don’t have non-critical servers. All of their data is critical to them. Everything is critical to them,” says Geminare’s Joshua Geist. And smaller businesses typically do not have the level of IT or business continuity expertise that larger organizations do. “They absolutely recognize the

White paper:

Practical Disaster Recovery Planning

Everyone is talking about disaster recovery planning and how important it is to be prepared for any emergency that could impact business-critical operations. But how do you actually develop a sound DR plan? There's lots of information out there, but where do you actually begin?

The development of a comprehensive disaster readiness plan generally encompasses these three steps:

- Identify the processes and resources that are truly business critical.
- Develop realistic and necessary recovery objectives for those processes and resources.
- Determine how you can achieve your DR objectives as simply and cost-effectively as possible.

Download this white paper to get practical guidance on developing, implementing, and testing your DR plan. It clearly outlines the steps you should follow to ensure that your DR plan will work as you expect it to and that it will scale as your business and IT needs evolve. Learn more about designing a holistic approach to DR planning that combines available backup and recovery technologies. Download here: www.caxosoft.com/disasterrecoveryguide.shtml



because they have a lot more customers across the board. For them to lose a million dollar account, it would certainly have an impact, but it wouldn't have business changing impact. For an SMB customer to lose a million dollar account because their servers are offline for three days and the account has to go somewhere else — that is a business changing event.”

Geist suggests that SMBs should look for “packages that include the entire data center, bandwidth, software licensing, expertise, implementation, audits — the entire process around creating a high availability environment.”

Lindeman agrees that SMBs have unique challenges but cautions them that some vendors see them as “prime targets” and may offer them solutions that are critically limited in scope. “They're sold on it, but when they go to use it, they find

it is missing this point and this point and this point, and that the solution didn't come complete. They thought they were buying X, but in fact, they were buying much less than X.”

Geist further cautions SMBs to make sure vendors understand that they have “very specific technologies, and very, very defined budgets, and that they don't want to change” platforms or technologies. “And they don't want to run through an \$80,000 audit to tell them what needs to get done.”

Option Overload

Vendor selection is tough for any size business, says Lindeman. He cautions companies to look for solutions that are “repeatable” and “something that you could sustain and bring to your business with the same IT professionalism that you have in place now.” He warns that while cutting-edge technologies are great, they must be proven. “I think many people are captivated by these new things that hit the market, where many of the enterprise organizations have learned their lesson over the years and waited to see a little bit more success and market penetration.”

Lindeman says a vendor also should be able to “show what they've done in your industry. That starts to really reduce the number of suppliers down to a more manageable amount. Many of the tried and trues start to percolate to the top, but you may start to see some less innovative solutions. There is a trade-off there. You have to ask yourself, ‘Do I need it? Do I have to have it now?’ If the answer is ‘yes’, then you may have to assume a little more risk.”

Says Rebecca Levesque of 21st Century Software: Customers should consider both the effectiveness of the product under consideration, as well as the service and expertise that will be delivered in conjunction with that product. If the vendor in question has a track-record of success in working collaboratively with customers — as a partner — then you can expect to more easily and effectively meet your objectives. Also critical, does the company under consideration have a long-term client base that is happy with its solution?

And don't forget that vendors must be willing to work with each other, adds Aschmann. “From my perspective, it is my job to make sure our products are compatible with all the other backup vendors out there. Obviously, we don't have the only back-up solutions and customers are going to pick what is going to work best for them. We are not going to try to impose a 100 percent CA environment. We know that's not the reality out there. Customers do choose different vendors and you want to make sure your products are compatible

“Recently we have had conversations with some of our competing vendors to determine if our products will work together for a customer. It is in our best interests and our competitors to get on the phone with each other.” **CI**