Executive Guide to Enterprise Business Continuity

special report
several weeks ago, a senior business line executive asked during a capital presentation for his area, “What is resiliency, and can you really define the benefit for my organization and the enterprise?” My answer led me to develop the subject as an impetus for this article, and prompted the question, “Can we really demonstrate the value of resiliency in our business continuity (BC) programs?”

Our industry has adopted a term utilized in many other industries, including the psychological-behavioral sciences arena. Wikipedia defines “resiliency” in psycho-behavioral terms as the positive capacity of people to cope with stress and adversity. Resilience is understood as a process but often referred to as an individual’s traits or one’s “resiliency.” The concept of resiliency is an individual’s cumulative experience and protective mechanisms inherently developed to deal with many risk factors. Thus, resilience and risk are often referenced in the same context and are naturally at the root of BCP and DR terminology. This is primarily because we are an industry based in risk management.

The BCP and DR industry has re-branded itself and widely adopted this new terminology in our technologies, vendor products, vendor names, methodologies, organizational branding, program directions, and even management titles.

We continue to reference business continuity planning (BCP) and disaster recovery (DR) throughout our industry in the same domain, but they remain isolated topics. Is it any wonder, then, that the resiliency and BC program message can be confusing to business lines, management, and non-industry personnel? Even the nomenclature of the responsible areas change so frequently that one day it is called the BCP or DR organization, and the next day, via organizational transformation, the name is amended to be resiliency planning or resiliency operations. Important to note is that this confusion
creates obstacles to the justification of capital funding expenditures and also the identification of the real value in BC programs. This message can be even more difficult to decipher in a down economy.

Develop a Unified Message and Vision

Many corporations have embraced the re-branding of this BCP and DR “resiliency bottle,” but for the most part have not restructured their organization, mission, vision, processes, or even technologies into a holistic enterprise BC program to support this new branding. Corporations often maintain multiple organizational silos as well as isolated technology and risk assessment frameworks, training, compliance tracking, and notification protocols. These organizations then attempt to bring these physical areas together with technology or some consolidated measurement methodologies.

The history of BCP and DR has seen some remarkable technology changes and trends in the last 20 years. One trend increasingly seen in the financial, insurance, and brokerage industries is the understanding that the disaster recovery program is only one major service element in a unified business continuity program. It is also a key aspect to the resiliency strategy of the enterprise.

As a result, traditional individual BCP, DR, and incident organizations have been consolidated to present an integrated framework. This trend in some industries is beginning to give rise to the understanding that the creation of consolidated programs is key to embedding the message of resilience into corporate strategy.

The focus of organizational consolidation is one of corporate governance and transparency within each enterprise. The industry recognizes the legacy of organizational silos which have existed for many years across technology, information security, facilities, human resources, and enterprise risk management areas. The resiliency framework direction,
Beginning with a unified program policy. Ensure your vision and mission have clear and articulate scope and strategies, accountabilities, and program components to senior executives and your stakeholders. Develop detailed guidance that is linked to policy, processes, and technologies and, finally, reporting. Sending multiple messages and organizational reporting in terms of readiness, preparedness, compliance, exercises, and program risk are not conducive in the eyes of senior executive management or the board, to supporting the resiliency value proposition for the enterprise.

Structure and Align Technology, Tools, and Processes

Oftentimes, the organizational structure of the program may dictate isolated or silo-based processes, technologies, and frameworks. To support a unified message, BC programs require integrated activities and technology that ensure and demonstrate the ability to maintain the resiliency of the organization.

In order to accomplish this, BC program processes should be structured to promote BC, DR, and incident policy integration; guidance; and risk assessment frameworks. Too often policies are not grounded or linked by common governance, risk assessment, performance, or management. Stakeholders are often split between organizations and lack the interdependence and visibility between business areas and technology environments to effectively plan and perform dependency risk assessment.

A key tenet in the BC program has been, and will always be, the overall risk determination factors for ensuring an appropriate risk mitigation approach to planning and recovery. One of the more critical elements of a strong resiliency program is not only the risk factors for the business, but also the overall impact to the value proposition for resiliency.

Where risk methodology focuses on the overall impact to the corporation, the key resiliency business drivers should be aligned with risk and the required technology and availability requirements necessary to both mitigate the risk and avoid impact to the key business drivers. If the focus is only on risk, the enterprise misses its opportunity to ensure message continuity and the linkage to preventative and high-availability methodologies.

Programs should focus on people, process, and technology throughout events and post-recovery. They should also introduce key preventative dependency technologies such as fault-tolerance, high availability, virtualization, stand-by, and extreme replication environments. Working concurrently with these technologies should be the guidance by IT infrastructure and BC professionals to avoid or reduce the impact of an event to the enterprise.

Leveraging any of the BCP, DR, and incident management vendor software platforms available in the market today enhances the planning, tracking, and alignment of major BC program components for many corporations. These products provide the ability to not only plan for and manage events but also provide a platform, when integrated with other enterprise knowledge bases, for supporting measurement of the value proposition to senior executives. The information housed in these products, when properly aligned across business processes, technology, and personnel, supports both the resiliency program and creates value as a knowledge base for the enterprise.

Develop Integrated Resiliency Measurements

Several of the measurements that can be utilized in assessing the value proposition for an enterprise BC program include the dimensioning of key strategic program domains (such as financials, customers, reputation, availability, assets, stakeholders, partners, employees, operations, regulations, compliance, and guidance.)

When assessing the many program domain data points, it is important to analyze the value of these data points not only in terms of inherent and residual risk impacts or exposure, but also in terms of the costs associated with not meeting predefined operational, process, and customer service levels and other data point threshold values.

Utilizing the data point elements of aligned technology for planning, monitoring, tracking, and recovery allows the enterprise BC program to enjoy a base of trusted information to the corporation. The data in the BC program can, through alignment of processes and technologies, federate other trusted single sources of corporate information. The BC program knowledge base elements then become a primary source for...
measuring the value of an enterprise BC program.

Additionally, the integrated BC program, in conjunction with other organizational information, becomes a key corporate asset and part of the value proposition.

Developing the integrated information base as part of the value proposition often requires specific technology and capital investment decisions but can, ultimately, generate a return on investment to the program and the corporation. It is also a valuable exercise to demonstrate the impact to the value chain.

**Promote the Value Proposition**

Propagate to the corporation the resiliency message with a basis in readiness, availability, and risk exposure to prevent and manage events. Our industry has an overarching tendency to focus on the risk framework only, using that as the message to senior management (and rightly so), as our paramount focus has been based predominantly on risk mitigation.

The justification for a capital funding request inevitably leads to a risk-based or return on risk investment analysis. While risk mitigation is an important component of our funding requests, value proposition, and executive management acceptance, it requires both transitional programs to promote the readiness, availability, and resiliency of the enterprise to withstand threats as well as the necessary preventative technology and processes within an integrated risk framework.

This requires solid framework and the principles discussed in this article to be repeatable and promoted to management. The real key to success for selling this proposition is to educate senior executives on what it means to be ready and resilient. The enterprise BC program must convey the corporate resiliency message in terms of the enterprise’s ability to maintain their competitive and customer-driven positions and brand identity with a focus on our people, processes, and technology, not only before but also through and after any event, major or nominal in nature.

One prospective way to demonstrate the value of enterprise resiliency is to structure a 3-to-5-year resiliency strategy roadmap and briefing with required capital and expense base to executives. Each of the capital elements should have an associated business driver with the correlated value to the overall business and/or business lines. This is a critical success factor for any resiliency program message.

Building upon your program features, utilize your key business drivers to demonstrate the core values of the program through ongoing measurements.

The marketplace has transitioned over the last 10 to 15 years from a glass-housed, operational-centric service metaphor to a ubiquitous, mobile, and 7-by-24 customer demand metaphor. This transformation has driven the rise of new directions in technologies, methodologies, and program structures as the basis for funding. Our industry, as a whole, has begun stepping up to this challenge. In response to this trend, your customer demand, availability, and resiliency need to become central components of the message you present to executive management.

The past industry messages of promoting BC and DR as isolated solutions for ensuring continuity will inevitably miss the target. BC/DR strategy has evolved into an enterprise resiliency strategy and focus. This message needs to firmly embrace the readiness, availability, and risk of people, processes, and technologies, thus enabling the enterprise to provide flexible services to customers and stakeholders on a continuous basis.

Major concepts in your value proposition message for resiliency are depicted in the value chain model (above).

Geno Pandolfi is a senior vice president and director of enterprise readiness services at U.S. Bank. He has more than 30 years of industry experience in IT, readiness, and risk assessment areas. Prior to joining U.S. Bank, he was president/CEO of Group Info-Tech and CENSOFT, Inc. The firms provided operational readiness and risk assessment technologies, assessment methodology, and consulting services to the financial industry. Pandolfi holds an MBA from Fordham University in management science and a BBA from Pace University in computer science.
process by scripting a business discussion designed to identify single points of failure or large concentrations of critical work. To focus the process further, we identified six general types of risk sources to consider:

1. Kraft-owned manufacturing facilities;
2. Co-manufacturers;
3. Suppliers;
4. Critical logistics infrastructure (ports, borders, rails, roads);
5. IT services and;
6. Corporate and shared services entities in each of these areas had the potential to have a significant business impact.

With clear executive direction on risk tolerance and crisp definition of the risk sources we were focusing on, we engineered a Web-based survey process tied directly into a management database to help focus the data collection and ensure consistent and complete feedback from all parties. We were able to conduct facilitated Web meetings with the business units to get their input effectively and efficiently, resulting in the creation of comprehensive risk profiles. We were able to conduct the process through pre-read preparation and facilitated Web meetings without incurring any travel expenses. Facilitated “live meeting” workshops provided flexibility for our mobile and virtual workforce that increased participation and scheduling flexibility. We executed the entire process for our North American business in less than six months while efficiently engaging all facets of our business in the input process.

The facilitated Web meeting approach not only saved us time and a lot of money, it produced far superior data. The process was a giant step forward for the program and was instrumental in helping our business leaders understand and take ownership for business continuity risk in their business units. By making efficient use of their time, we got them actively engaged and got the data we needed to make important decisions.

The data gathering was part science and part art. In our case, the questioning process was designed to keep the focus on the most important issues and not get distracted by the less important ones. There was room for disagreement and a method to handle gaps that might not be fully addressed in the first meeting. By establishing risk profiles in an easy-to-use database we were able to instantly analyze the data in real time dashboards and reports. We used the analyses to help us refine and improve the quality of the information as we reviewed our findings with each level of management.

The result was a project that produced exactly the information we needed to make business decisions about our most important risks and which came in under budget on a very aggressive schedule. The initial project addressed our North American business units which are now well on their way to mitigating continuity risks, making improvements, identifying alternatives, and building actionable business continuity plans.

We are leveraging proven technology and methods to maintain and improve our program in North America while we extend the program to the rest of the world. Once again, we are executing the project with little to no travel expense, operating on five continents across all of our global brands. The methods and systems we deployed are proving even more important in our international work as we are challenged with language barriers, time zones, and a highly mobile and diverse workforce and partner network.

The upside for Kraft comes from a simple recipe.

- Start by determining risk tolerance.
- Form and empower a steering committee.
- Define risk sources.
- Develop and refine a data gathering process that will produce the reporting needed for decision-making.
- Run facilitated workshops using experts who can guide and focus the meetings.
- Compile reports and dashboards that frame the business decisions effectively and efficiently.
- Use technology to keep things simple and focused.

The secret sauce comes from the cross-functional BCP steering committee, the innovative use of technology, and expert facilitation that has helped us economically execute a comprehensive and ambitious plan. With the right framework we not only have successfully launched our program, but we have also set the foundation for a program that is simple and easy to sustain.

It is notable that during this entire process we did not add staff or incur significant incremental operating costs. We simply used technology and process to harness information that was once broadly dispersed to enable our company to effectively address continuity. Our program is now connected from the very top of our company out to the people who manage those risks day to day.

We now have an effective, efficient, economical, and sustainable program. As part of Kraft Foods’ broader ERM program, BCP risk management initiatives are now more clearly understood and are being addressed as part of comprehensive plan to manage business risk.

Claudia Temple, assistant treasurer, global risk management and insurance; Leslie Borders, CBCP, manager business continuity and disaster recovery. Temple and Borders are members of the Kraft BCP Steering Committee which has accountability for managing the business continuity process at Kraft Foods.
IT Service Continuity Programs

Everyone has heard the pitches on risk-based benefits for building and sustaining good service continuity and disaster recovery (SC/DR) programs. We can reduce our risk by shortening the time it would take to recover in the event of a data center disaster or a major system meltdown. Fear, uncertainty, and doubt (FUD) are the typical drivers for coaxing out precious enterprise investment dollars for SC/DR. After all, SC/DR is just an insurance policy.

This discussion is not about the standard pitch. Instead, it is a description of several hidden benefits to the CIO for building a strong SC/DR exercise program.

Even if adequate funding and recovery tools are available to IT from the enterprise, there is often little support within IT’s technology teams to provide resources for consistent and proper testing of critical systems. People in IT are so busy with the daily burdens of development, incident response, performance tuning, and general firefighting activities that they often push back on doing even minor activities related to SC/DR plans and exercises.

A CIO might see the value of a strong SC/DR program, mandate with an iron fist, and run unannounced or routine table-top reviews, partial or even full-scale recovery tests. Alternatively, they might take a softer approach and give everyone SC/DR personal goals for the year. Either way, pain and angst will be felt. And yes, of course, everyone wants highly available systems with redundancy and auto-failover which could eliminate the need for a substantive SC/DR program. But the costs of deploying highly available systems can be far beyond the ever-tightening pocket book.

Perhaps the CIO could take a different view toward validation exercises in a strong SC/DR program. There are three flavors of potential hidden benefits locked up inside of SC/DR exercises: IT to IT interaction; IT to business interaction; and executive awareness.

IT to IT Interaction Benefits

In many IT organizations, divergent camps or towers emerge and create a hindrance to delivering services efficiently to the business. Oftentimes huge barrier walls are created between these camps. At times it may appear that gladiators have stepped in the coliseum to slug it out to the death. This is a natural tendency of many operational units, so IT is no different. For example, look at the military. Even though they are all on the same team, the Marines are down on the Army and vice versa. Within the Army the tankers conflict with the infantry which conflicts with the artillery which is in conflict with the rear echelons. Yet, they all have to work together to get the job done. IT is a unique little battleground in its own right.

Over the years, an entire service industry subsequently developed to help business leaders tear down these walls. These “organizational consultants” charge CIOs phenomenal service fees to improve collaboration, advocate team building, and nurture partnerships between teams. A great deal of time, effort and money go into tearing down those walls. The consultants engage the CIO’s leaders in sometimes silly activities such as walking on hot coals or falling off of picnic tables blindfolded into the arms of their colleagues. Many of the scenarios used in the exercises are fabricated crisis situations to accelerate exercises so people can learn more in a short period of time. These exercises are not the routine, day-to-day IT experiences of “death by a million pin pricks,” which sometimes seems to be an enterprise sport.

CIOs will drop $20K, $40K, or even $50K and lose entire leadership teams for multi-day to week-long off-site events to squeeze out what could be marginal improvements in team collaboration. These artificial exercises cannot possibly mirror the team’s real working environment. It is difficult to relate the exercises to the team’s real jobs because they are simply playing roles.

But what if the CIO were to throw out the team-building consultants and leverage SC/DR exercises to do the same thing? SC/DR exercises could be planned as a team-building activity that put people in their actual working roles. The scenarios could be a simulated crisis scenario that is very relevant to their actual job. They would be forced to work in crisis under stressful recovery time objectives (RTOs), side-by-side with the gladiators that they were battling just last week. They have to get these systems back up and put their business customers back online. And they can only do it by working together.

In a previous global position, I physically monitored or audited exercises on five separate continents. The most entertaining part of that job was to “kill” key operations people at the beginning of the exercise. Panic would flush across IT managers’ faces when they realized they had no access to their most important people. No team-building exercise or relationship-ship consultant could build a more relevant, effective scenario. Those managers were forced to reach across the tower walls to muster resources to meet their recovery objectives. The teams had to learn how to work together to get the systems back up. That cooperation oftentimes carried back into the day-to-day arena, nurturing a sense of cooperation between the gladiators.

It’s a most fulfilling sensation to watch server, database, applications, and network teams suddenly pulling the rope in the same direction. Now that their data center and IT office building was destroyed in a tornado; flood; chemical disaster; or car, train, or plane crash, each team sitting side by side in a war-room-like scenario in an off-site recovery location suddenly become one team. I have seen where routinely adver-
serial teams suddenly merge into one highly functional team because they were forced to solve their own real life IT problems under pressure. The key to gaining value for IT to IT interactions from these exercises is in packaging the optimal scenarios for getting the desired results. If a CIO feels compelled to use a consultant, use them here. There is a caveat to this postulate. If all of your systems are built with fully redundant, highly available, auto roll-over capability, then you might just have to bring those consultants in to help tear down the tower walls. If the CIO is fortunate enough to have enough business support to fund such advanced capability, they should feel fortunate from a SC/DR perspective. In that case, just pay the team-building consultants, walk on the hot coals, and don’t complain.

IT to Business Benefits

No one knows more about the pain of system downtime than business leaders. Although ironically, during business impact assessments (BIAs) with business units, I have seen many managers say, “Oh, we can live without that system for days or weeks before we really hurt, financially.” However, if that system goes down on Tuesday afternoon for 45 minutes, the escalated phone calls would have the CIO believe that the Earth was just invaded by aliens attempting to take over the planet. The business unit feels intense pain, regardless of the true financial impact.

But those same business managers who yell the loudest do not always understand the complexity and sensitivity of aging systems running on obsolete, unsupported hardware, systems of which they are often unwilling to fund upgrades or enhancements. They just don’t seem to understand the pain that IT operations and application teams feel trying to keep their business systems running. But if some business people could see firsthand the trouble in trying to recover those systems in a simulated disaster, their whole perspective might change. Having business observers of SC/DR exercises could build empathy to daily IT challenges. This could translate to more funding or less resistance when it comes to supporting improved system designs, upgrades, and investments. Maybe they will even fund some highly available systems, eliminating the need for SC/DR tests.

Executive Awareness Benefits

Most business executives view their IT systems as utilitarian, like an electric plug or a telephone. They want it there all the time, any time their teams or customers want it. They are so busy running the business line, they cannot possibly worry about the CIO’s problems with funding upgrades of their systems let alone building in more SC/DR capabilities. The CIO can make the FUD risk pitch during the annual budget bartering season, but chances are their requests will be pushed to the bottom of the business funding priority list.

However, running comprehensive business continuity/disaster recovery (BC/DR) tests, successful or not, can play out an entirely different scenario. In the end of a routine meeting between the CIO and a division president (post-BC/DR exercise), suppose the following conversation takes place:

CIO: “Oh, by the way, Madam President, last week our operations team ran a disaster recovery test with your people on your business systems. It did not go as well as expected. It took them over three days to recover full functionality.”

President: “Whoa, what happened and how do we fix that?”

CIO: “The post-exercise analysis showed that we need to make investments to cut the time down. If we invest $250K, they should be able to get the recovery down to one day of downtime. But with $1.1 million, they could make it fully redundant with high availability. That means the system would be rewritten to operate in two different data centers simultaneously. If one data center goes down, the other half continues to operate. The system should never go down in a single disaster.”

President: “You’re kidding, CIO Joe. If you guarantee me that it will never go down, I will budget for the highly available system in this upcoming budget cycle.”

A bad BC/DR exercise could be a “half-full glass” with the right view. This is not advocating the CIO to be a spin-doctor, but played right, exercise results could yield positive outcomes when dealing with business executives. After all, they will be glad to see that the CIO is doing her best to protect the business interests of the organization.

Caveat Emptor & Summary

All three of these hidden benefits are two-edged swords. The back blade could easily bounce back and cut deep.

IT to IT: Some people are just not team players. These people might actually be a root cause of tower walls and fortress building, hidden in routine day-to-day work interfaces. An intense SC/DR exercise may well expose them, making it easier for a CIO to deal with this type of person. Seldom will you find someone “written up” for not playing well in an off-site game playing exercise. But if they don’t play well in a BC/DR exercise, the leaders could be on their way to removing that person from the team. This may sound a bit draconian, but sometimes the king needs to stand on the throne at the coliseum skybox and put a thumbs-down on a weak gladiator. Conversely, during a challenging exercise, a CIO might just find some shining stars that would otherwise continue to be buried in the depths of IT operations.

IT to business: If an IT team is really “messed up” and they bring the business unit to watch them helplessly flounder through a recovery exercise, the relationship and image could suffer. In fact, the IT reputation could be irreparably damaged at least until major personnel changes took place, e.g., replacing the CIO. So if IT has significant issues with being able to adequately perform during an SC/DR exercise, there may be second thoughts about bringing the business too close to the exercise process. A CIO needs to think about the potential adverse reactions of this double-edged sword.

Executive Awareness: Ditto on the previous sword. If SC/DR exercises go well, then the CIO should raise the battle flag in glory and wave victory. But if the exercise bombs, extra caution should be used in how to best raise executive awareness. A failed test could be viewed as a CIO’s failure to adequately manage risk, regardless of the SC/DR budget cuts experienced over the years. To head off some criticism, it may be best to socialize the pre-emptive mantra “the best DR test is a failed test, so we can fix the problems before a real disaster.”

In summary, making an investment in a strong SC/DR test and exercise program could have paybacks that far outreach the classic risk-based benefits used to justify the expenditures. For the company, the CIO should leverage these SC/DR exercises as that proverbial insurance policy. As a CIO or business leader, a strong SC/DR program can be leverage to improve IT operations overall, IT to business relationships, and enterprise executive relationships with IT.

For a last recommendation as part of SC/DR exercises, take the technical teams, including business unit testers and managers, and treat them to a nice lunch or dinner after the exercise. Spend the dime to thank them for their support in reducing the risk to the business. Yes, go back and make the original FUD-risk pitch to these people who are helping the CIO meet the enterprises’ SC/DR risk reduction objectives. But they do not necessarily have to know about the hidden benefits the CIO is getting in return for their hard efforts.

Bob Frank, CISSP, is the vice president of service management at Apollo Group, the parent company of the University of Phoenix, the largest university in the world with nearly half a million students. Apollo Group also holds several other global universities servicing regional students in Europe, Asia, and Latin America. He also carries responsibilities as the chief information security officer for Apollo Group plus service continuity and disaster recovery processes for the core data center operations.