XXXXXXXXX BUSINESS CONTINUITY SUPPORT SERVICES:

A REVIEW OF CURRENT PORTFOLIO AND MESSAGING

AND SUGGESTIONS FOR INCREASING MARKET SHARE

IN 2016

PRESENTED TO

XXXXXXXX XXXXXX

CHIEF MARKETING OFFICER

XXXXXXXXX, INC.

BY

JON W. TOIGO

MANAGING PRINCIPAL

TOIGO PARTNERS INTERNATIONAL LLC

DRAFT

12-17-2015

CONFIDENTIAL

SUMMARY

On December 17, XXXXXXXXX Chief Marketing Officer forwarded to Toigo Partners International a set of questions via email to which he was seeking objective and knowledgeable responses. Following an interview with XXXXXXXXXX personnel and management, this document contains the preliminary responses to the question list. Embedded in some responses are requests for additional information from XXXXXXXX. This is a draft document.

SPECIFIC QUESTIONS AND RESPONSES

- *What is the current satisfaction level with legacy DR and SAN to SAN replication?*

  Disaster recovery planning has never been a preferred activity of business organizations. In surveys conducted over a ten year period, the results have been fairly consistent: fewer than 50% of organizations develop disaster recovery plans for their IT operations, and of those who do, fewer than 50% test their plans, which is tantamount to having no plan at all.

  Key reasons for not planning include lack of on-staff skills or confidence in the ability of staff to complete a plan successfully, lack of resources, time or budget, and the urgency/priority of other operational activities. Management buy-in is key, but budgets are rarely allocated even after management has decided to create a plan.

  At a minimum, most IT organizations seek to protect their data. Data copy (or backup) is the least daunting hedge against catastrophe and numerous software and service products exist to aid in the effort. Unfortunately, storage infrastructure can be complex and proprietary, making simple backup/restore or data copy tasks more challenging to implement than expected. This is generally the case with SANs and other traditional storage infrastructure. Vendors have engineered SANs with sufficient proprietary attributes that they often require identical or mostly-identical gear and configurations to make routine data copying successful. Technical challenges often stymie the development, implementation and management of an ongoing data protection strategy of any sort.

  Recently, discussions of software-defined storage and hyper-converged infrastructure have tended to underscore the foibles of SANs and to villainize vendors of monolithic storage arrays. Hypervisor vendors are pressing into service “new” storage models leveraging direct-attached media in multi-nodal cluster configurations with on-going inter-nodal replication. These configurations, however, are proving to be very expensive to implement and challenging to maintain over time, in addition to having the unexpected consequence of slowing the performance of hosted virtual machines. Much work will be required to develop a stable software-defined platform that features ease of operation and cost-efficiency. As experimentation proceeds, there has never been a greater need

for data protection, but there is also considerable marketecture around the “high availability” that storage node clustering presumably provides to confuse operators or to console them with difficult-to-validate promises about built-in data protection and operational resilience.

For small to medium firms, the lack of confidence in on-staff capabilities to undertake data protection or disaster recovery planning is often contextualized in terms of the lack of resources to spend on obtaining the right tools – “enterprise class” backup or replication software is too expensive for the firm or two complex to implement and operate. This holds true in both small staff data centers and even in the remote office or branch office environments of medium and enterprise firms.

These issues are helping to drive interest in the idea of outsourcing data protection and disaster recovery planning to external, cloud-based service providers.

- *What problems are companies and their IT teams really trying / struggling to solve as it pertains to BC/DR, especially in the mid-market and enterprise?*

  The biggest issues confronting IT teams in the firms I consult for today involve maintaining service levels sufficient to prevent management from outsourcing IT altogether. Disaster recovery and business continuity are only prioritized in companies where legal or regulatory mandates require data protection, operations continuity or data governance and stewardship.

  Generally speaking, most publicly traded firms (regardless of industry segment) must act to protect their financial systems and data at a minimum in conformance with SEC requirements. Heath care and banking sector firms have a more compelling and comprehensive regime of data protection and operational continuity regulations and mandates to which they must conform. Other industries, especially data-centric enterprises such as media and broadcast firms, perceive their digital assets as the value of their businesses and tend to be more inclined to take measures to protect them – though many fail to do so.

  By and large, the biggest hurdle confronting most firms is a lack of management sponsorship of DR/BCP planning activity. Senior management rarely shows interest in plans and strategies unless an adverse audit finding or legal action – or an actual disaster -- exposes a significant risk.

  In many firms, management nonchalance is actually reinforced by IT hardware or software vendors who use exaggerated resiliency promises as part of their sales effort (“with our virtual servers everything is replicated, so disaster recovery is built in – there is nothing else to do or buy”). Editorial (and sneakily framed advertorials) in leading business publications often help to disseminate and reinforce such claims.

In light of the above, the “business-savvy” IT planner seeks to develop a data protection capability that

- Doesn’t require additional staff to operate or manage, and/or that can be automated to the greatest possible extent, and/or that doesn’t require the deployment of extraneous hardware or training-heavy software…

- Delivers enterprise-class data protection without the effort or skills requirement, and/or that doesn’t require significant levels of up-front planning or data analysis, and/or that doesn’t entail the software licensing costs…

- Doesn’t require time-consuming or disruptive testing…

- That works for the 90% of disasters that do not involve facility level outages or regional outages…

Such solutions are difficult to find, validate, or acquire, of course. They tend not to be comprehensive solutions since they don’t offer protection against facility or regional outage threats. Instead, they represent minimal level responses to vulnerabilities such as localized data errors, application software faults, discrete hardware failures, and user errors that account for roughly 90 to 95% of annual downtime events in the US.

Moreover, the solutions are rarely “tuned” to the actual needs of the business. Rarely, do strategies take into account the relative value or importance of business processes, the applications that serve them and the data produced by and used by those applications. Strategies tend to be “one size fits most” data, which rarely fits the actual restore priorities, often stated in estimated recovery time objectives, of the organization.

And, as stated above, such strategies are rarely tested for their solvency, mitigating their actual value as emergency responses to unplanned interruption events.

To the “sincere” planner (the IT operator who truly desires to protect the operational and data integrity and availability of IT for the company), the lack of management support, the lack of budget/resource availability and the impenetrable amount of marketecture that shrouds the architecture of both the technology products themselves and the service providers who are appearing “out of the woodwork” claiming to be expert at data protection and DR are typically cited as key impediments to doing a good job.

- *How are these companies currently addressing these problems?*

Large and medium size companies tend to pursue DR/BCP as a set of small or incremental projects aimed at safeguarding specific business processes, specific applications or specific entities (branch offices, for example). Often, DR or data protection strategies can be implemented as part of the hardware kit rolled out to support

the specific BP, app or environment. The problem with such an incrementalist approach is that, without very careful scrutiny, it can create the problem of multiple isolated islands of technology and data that need to be managed using whatever tools and procedures that have been implemented for each specific island.

Increasingly, departmental-level business managers are making a decision to move to an internet- or cloud-based DR service provider to protect "their" IT assets and data, especially in organizations where centralized or corporate IT management discipline has been weakened or is otherwise preoccupied. This is both good and bad news for DRaaS providers. It may simplify sales, but only if the right business manager can be identified to sell to.

- *What DR needs are being met and by whom?*

  As indicated above, DR/BCP in medium and larger organizations may be a centrally managed activity, or it may be decentralized and handled by departmental business managers.

  A centralized management approach has the advantage of delivering a universal set of resources and services at an affordable cost to the organization -- courtesy of economies of scale realized from bulk purchases of software licenses and/or service contracts.

  In a centralized management model, there is usually a team of DR planners, led by a strategy administrator. The administrator may be located in the IT department or he/she may be part of the corporate risk, governance and compliance organization, if such an entity exists. The team

  - Performs, or engages a consultant to perform, a business impact analysis that establishes the relative importance of business processes, their interdependencies, and their recovery objectives (RTOs and RPOs)

  - Assesses risks and assigns restore priorities to business processes

  - Inventories applications and data by the business process served and prioritizes recovery

  - Identifies strategies and technologies for data protection and researches the efficacy of those strategies and technologies in order to recommend adoption of a particular strategy and its associated technology or service

  - Identifies strategies and technologies for application re-hosting and recommends a strategy/technology

- Identifies strategies and technologies for network recovery and recommends a strategy/technology/service

- Implements approved technologies and services and tests strategy

- Develops schedules for ongoing maintenance and testing of the program, sets up a change management process to track changes to business processes, applications, infrastructure and data

By contrast, a distributed management model often introduces a potentially greater ability to design customized strategies for specific business processes, apps or environments. Departments do not need to conform to a common corporate standard or set of technologies or services: they each create their own, typically via a team of business staff, technology support staff and/or consultants.

However, a distributed model also entails potential problems in the form of multiple strategies that are difficult to coordinate in response to a disaster effecting multiple business units. Distributed approaches also result in overlapping recovery capabilities or redundant protective processes that can drive up the cost of DR planning.

- *What DR needs are not yet being met? What gaps exist that* XXXXXXXXX *could fill?*

The outcome of DR/BCP can be conceived as a process that produces a strategy with three parts: data protection, application re-hosting and network redirection (so end users are able to re-connect with rehosted apps). XXXXXXXXXX needs to decide how it wants to plug into the process.

XXXXXXXXX could provide consulting assistance in data discovery and classification, identifying assets that need to be protected and recovered with the highest priority (RTO of less than 4 hours), those that have medium priority (recovery within 12 to 24 hours), and those that, while important, do not need priority recovery at all (greater than 24 hours). This business impact analysis sets the stage for plan success or failure from the start, though it is often overlooked or is taken as “a given” by vendors seeking to sell a protection or recovery product or service. Business impact analysis, with data classification, is a difficult task to undertake within a company since IT folk generally do not know the relative importance of business processes or which data is associated with which business process (and don’t want to know!) and business folk know nothing about the technology for storing, protecting, archiving or recovering data.

A data risk analysis service, as a precursor to other activities (archive, security/encryption, data hosting, data protection), might be well received in the market and would distinguish XXXXXXXXXX from most of the DRaaS providers in the market who are simply providing data replication software and services. This would be an even more effective offering if XXXXXXXXX could develop methodologies for data classification that map to the typical workflows of a given industry segment: media and broadcast, oil and gas, etc. have very specific workflows that create data, and well understood requirements for data retention and protection, providing an opportunity for XXXXXXXXXX to become the expert in data protection for that industry segment.

XXXXXXXXXX should also look at its own capabilities and decide how it wishes to be perceived by potential clients. Do you primarily want to enable data replication by placing software or hardware at the client site, tag certain production data for ongoing backup, and drive that data copy to XXXXXXXXXX hosting facilities? This appears to be the primary offering of XXXXXXXXX today. Unfortunately, it is an increasingly crowded market in which multiple vendors offering the same horizontal service differentiate themselves solely on the basis of client lists and which enterprise-class software product they are making available to the client company. That is a challenging market in which to thrive.

Does XXXXXXXXX also want to provide application re-hosting – delivering the equivalent of a "hot site" where clients can re-host their virtual machines and operate them remotely if their facility becomes untenable? That is another DRaaS scenario, but it entails more than just providing hosting platforms and connectivity. Provisions must also be made for testing the strategy on an occasional basis, in the case of a stand-by or active-passive clustering strategy, or on an on-going basis in the case of an active-active clustering strategy. Most managed hosting facility providers who are hanging out DRaaS shingles actually know very little about, or have few procedures for facilitating, client testing of the failover strategy. Most have no "fail back" strategy whatsoever. XXXXXXXXX could distinguish itself by having published procedures for these services, if this is their chosen direction.

Does XXXXXXXXXX want to provide network re-direction or user work facilities? These are also important services that require a certain degree of expertise and a predefined set of procedures to ensure consistent and reliable delivery. Providing such a service would certainly help the company differentiate itself from the preponderance of "backup clouds" in the market.

- *What is the general perception of DRaaS and Raas providers, especially among those with legacy DR or SAN to SAN solutions?*

  In my experience, the reception of DRaaS providers in the US is generally warm but somewhat skeptical. While most IT management bristles at the idea of outsourcing (the basic cloud model strikes them as an outsourcing play, like ASPs/SSPs in the late 1990s

and service bureau computing in the 1980s), they are more favorably predisposed to use an outside entity to facilitate data protection and disaster recovery and have been doing so successfully since the commercial hot site appeared in the market in the early 1980s.

Skepticism arises when the vendor oversimplifies the explanation of the protection/recovery process – which is commonplace when the vendor is pitching non-technical business management. It does violence to the sensibilities of the IT person who understands the impact of latency and jitter on data networking over distance and the challenges of working with a service provider to coordinate field testing. Depending on the audience, XXXXXXXXXXX needs to acknowledge benefits and challenges realistically and at a fine enough level of granularity to instill confidence that they know whereof they speak.

Most companies would not be considering DRaaS unless

1. They believe that they are not doing an adequate job to protect their data or operations integrity, or criticisms of their capabilities have been raised by internal audits, regulatory reviews, or recent disaster events
2. They believed that they did not have adequate on-staff skills, resources or budget to undertake such planning successfully on their own (this is especially the case with respect to SAN to SAN replication, which requires detailed knowledge of technology and vendor-proprietary technology implementation, difficult to perform testing regimens, and on-going cost of synchronizing remote SANs to correspond with changes made to local SANs)
3. They had budget to acquire the resources and skill and technologies needed to do the work.

In short, while outsourcing to a cloud provider is generally not a strategy favored by IT (though the front office may be attracted to it from a myopic focus on temporary labor cost savings), they are potentially predisposed to embrace DRaaS – which provides a way to deliver on their data stewardship mission without a lot of effort.

- *What is really holding back prospective users from migrating to DRaaS faster?*

Public cloud service providers have had their share of outages and interruptions and unauthorized data disclosure events to give any IT planner pause. Memories of the business failure of Nirvanix and the subsequent challenges for its key customers will take a while to fade and have a chilling impact on the idea of storage as a service and cloud IT generally.

Competence must be demonstrated and reinforced to make DRaaS providers successful in surmounting logical and emotional objections. The good news is that most IT managers do not want the job of developing data protection and disaster recovery strategies. It is thankless work that only receives notice when something goes wrong. A

failed strategy is a career limiting event. Most IT folks I talk to want to believe that a DRaaS provider can remove the burden of DR/BCP from their shoulders in a reliable way. They just want to be convinced that the vendor knows what it is doing.

- *What messaging do those with legacy DR and SAN to SAN solutions need to hear to consider DRaaS solutions more seriously?*

  They want to hear that the vendor knows at least as much about data protection and DR as they do, so that relying on them to do the work is not a fool's errand. They want to hear that the vendor has facilitated others in their industry segment with services…and if possible that the service provider has delivered on its promises when a client had an interruption event.

  They want to hear that the vendor isn't "fly-by-night" – another start-up capitalizing on a shiny new term to make a few bucks until they sell their firm or shutter their operations. A lot of small DRaaS firms are dotting the landscape and there are more to come: how many of these will exist in a few years?

  Access to enterprise-class technologies for data protection and disaster recovery are important, but leading backup software vendors are going to bed with every DRaaS service provider that hands out a shingle. What is really important is how well XXXXXXXXX can communicate value around the software offering, an understanding of the DR planning process, of business continuity requirements, of information governance mandates, of business criticality and the simple fact that one-size-fits-most solutions never fit anyone's needs very well. Documented procedures and best practices helped make Sungard a success; the same is needed to propel a DRaaS provider to the top of the heap.

  Also, if a vertical market approach is selected, XXXXXXXXX needs to demonstrate that it understands the vertical – its sensibilities, economics, workflows and requirements. It helps to have a portfolio of clients in that vertical or a pedigree in hosting firms that are part of the vertical.

- *What features / benefits / messaging will mitigate the perceived risk of migrating to DRAaS?*

  Ideally, there should be service before the migration – assistance to the client to understand and document what data requires what kind of protection and recovery priority based on business and regulatory factors. This would instantly differentiate XXXXXXXXX from the many other firms who want to treat data assets as an pile of files or binary objects without reference to the application or business process that is being supported. This upfront service is critical to economizing on the strategy and ensuring its fit with actual recovery requirements.

The migration should be supported by an initial "seeding" that does not leverage the network. Network transport of a lot of data is slow and tedious. If data can initially be migrated via extra-network seeding (e.g. on high capacity removable media), XXXXXXXXX can argue that "with XXXXXXXXX, data protection begins immediately." Extra-network transport can also be leveraged to assuage customer concerns that their data can be returned to them or moved to an alternate service provider in the future if the company desires or if a Nirvanix-like exit were to occur.

In short, XXXXXXXXX must make the customer comfortable that its service offering is right-sized to customer needs, brings value the customer couldn't obtain elsewhere at a lower price, and that affordable and convenient exit is possible from the arrangement if XXXXXXXXX doesn't fulfill its promises – which is a big concern with today's clouds.

- *How do the enterprise and mid-market like to purchase DR? Point solutions or Swiss army knife provider?*

  This depends entirely on the company. If you provide a niche service, you may be perceived as difficult to integrate with other services used in a strategy. Medium-sized firms usually want and expect vendors to do it all, even if they won't be using the entire suite of services. Large firms with centralized management models may be less adverse to point solutions, but large firms with distributed management models are likely to prefer a vendor with a diversified portfolio or menu-based set of offerings.

  Ultimately, "customized" is more important than "diversified." Most buyers are less interested in what the scope of service offerings are than in how well the vendor can tailor those offerings to meet the unique requirements of the business and its data.

- *After you review* XXXXXXXXX*… Would prospects consider it to be differentiated? If so, how should we message it better? If not, how can we create a more differentiated product?*

  From the brief call already conducted, XXXXXXXXX strikes me as a service provider that could differentiate itself in the market rather successfully. You have some "anchor clients" and a savvy management team. Emphasis needs to be placed less on the specific software that you can offer (important, but not key to success), than on your understanding of business needs for data protection, the challenges that business DR planners confront today, and the capability you provide to custom-fit a cost-effective and business-savvy data protection strategy to the client.

  This is marketing 101: make the customer feel special. There is no one-size-fits-all solution, as your competitors are selling. To do an effective job, you need to focus on which data assets are critical and protect them with appropriate services, then apply less costly services that are appropriate to protect less mission-critical assets, and so forth.

Stop paying too much for data protection. Get what your data and your business needs, not what some vendor wants to sell you.

I also believe that I detected some considerable interest in tailoring services to a vertical market segment such as media and broadcast. This is a very good strategy, as it enables you to develop preeminence in a particular space with fewer competitors, providing a foundation from which you can branch out.

- *Are our product lines well aligned with market needs and expectations?*

  Your software offering features brands that are respectable in the industry. Your website fails to engage me. There is little or no confidence instilled by what I read on the site that you have a lengthy pedigree in DR or business continuity.

- *What DRaaS providers do you believe have a differentiated message?*

  The best market messaging is probably coming out of Unitrends. They have successfully retooled a software play into a service and have quite a long resume in data protection as a software vendor with consulting services. Their lack of a pedigree in managed hosting or cloud doesn't seem to have held them back.

  Other software vendors-turned-DRaaS vendors have been less successful. Zerto and actifio have products and pedigree, but their marketing messages fail to resonate. More and more backup software companies are getting into the market, but many seem to have adjusted their sights and they prefer to sell their wares to service providers rather than opening their own data centers.

  VMware recently launched a service that will appeal to their minions but that offers little support outside the VMware camp. Give than most companies will have a mix of hypervisors and mission-critical transactional workload that is not virtualized at all, VMware's service provides at best a niche solution.

  Stalwart hot site providers like Sungard and IBM have mostly failed to attract much attention as they transitioned to DRaaS delivery models for their services. Others who have come out of the facility space know what they are doing technically, but appear to have largely failed to resonate with consumers who do not have decades of experience in IT. Verizon, iLand, CenturyLink, nScaled and a few others populate Forrester Wave views, but I am not hearing about them or seeing them widely adopted in the industry.

- *Are there industry verticals that are underserved that* XXXXXXXXX *should target?*

  Yes. Based on many conversations with Hollywood production and distribution companies, there is a very underserved need for data protection both during the production process and over the long haul once the project is "in the can."

Financial services companies are also looking for business-savvy providers to help them protect their data in accordance with the legal and regulatory mandate in their industry. Deduplication is suspect as an out of compliance technology from an SEC perspective so all data needs to be uncompressed and not deduplicated. The cost to store primary and replicated data is accelerating. Service providers with a special knowledge of financial industry requirements would be highly prized.

Healthcare is another vertical worth exploring, but the focus should be on medical imaging. Medical imaging is the big bread winner for most hospitals and the administrators tend to have their own budgets, their own storage infrastructure, and very little staff to manage it. Their data is growing exponentially, as is the cost to store and protect it in accordance with HIPAA.

- *Is there a common catalytic event that initiates companies to look for a DR replacement, especially to look at DRaaS?*

  Budget cuts tend to drive change, as do actual disaster events in which less than satisfactory outcomes were realized from existing DR strategies. Good DR consultants watch the newspapers for recent disasters to identify potential clients.

- *Who within a company typically heads up the search for a new DR solution? Take us through typical buyer journeys.*

  As indicated above, the model varies. In medium size companies, the responsibility for DR is typically vested in the IT manager, who assigns it to the staffer who was the slowest to dive into his or her cubicle. The staffer does the legwork of attending a seminar or conference, talking to prospective vendors, getting demos, and making recommendations. A one stop shop vendor is usually preferred. The IT manager then conducts his own reviews and recommends to senior management for funding. Assuming that approval is received, implementation is scheduled as a project.

  In a larger enterprise, one with a centralized management model, the DR responsibility may be part of the CIO's job – or in some cases, a committee comprising IT and GRC (Governance Risk and Compliance). They set goals and objectives to frame the investigatory process, hire consultants to evaluate requirements, then issue an RFI or RFP to potentially suitable providers. Demos follow and haggling over services and costs. The decision is ultimately made and the implementation project rolls out.

  In an enterprise with a distributed model, decisions may well be made "seat of the pants" usually following an adverse audit or a recent flirtation with a disaster event. Typically, a non-technical manager decides to protect data from further calamity and directs IT-savvy staff to look for alternatives. Google and, to some extent, analyst recommendations drive the candidate list. Demos follow and a decision is made. These decisions usually take the least amount of time.

- *What is the role of other team members in influencing the decision?*

  Management is usually inclined to support the decision of the technical team unless cost is a large factor. Technical teams are interested in the specific support provided by the vendor for their applications and their infrastructure. Personal affinity is also a big factor, which accounts for the many steak dinners and sporting events to which technical reviewers are often invited by competing vendors. In the final analysis, the technical staffer will usually go with the solution that instills the most confidence.

- *What kind of intangible, emotional elements influence the decision making process for DR? What emotional space can* XXXXXXXXX *own?*

  Increasingly, IT folk are suspicious of hypervisor vendors. Things are not going as planned in terms of application performance post-virtualization or the reliability of HA clusters and VM movement. They want validation of these concerns from a DRaaS vendor, who wants to help them to protect their jobs and reputations "while the hypervisor vendors work out the bugs" by delivering a reliable data protection and disaster recovery service.

  The IT person also wants to be respected, to feel as though his needs are special and trump the standard service requirements of other companies. Customization to the needs of his shop is key to selling service.

  Emphasize that the IT person still has control, that dashboards and other management tools are available for his use in inspecting and reviewing services at any time. This is supposed to make his life easier, not give him more trouble or another pile of technology to need to master.

  Senior management wants the endorsement of IT and a good cost model. Period.

- *TCO - what is important, what should be included?*

  This is a challenging question, since not everyone looks at TCO the same way. Certainly, providing a ball park of the costs for redundant facilities, hardware, software for data protection, clustering with failover/failback, etc. is a good idea. But it will never be able to take into account the discounts and other incentives that OEMs can deliver to customers. So acquisition costs are rarely modeled accurately. The real sale of any cloud service is based on expected OPEX cost savings: knowledgeable cloud folk will do a better job at a lower cost to the client of protecting data and keeping the protection service up to date with business needs than already overburdened staff who are doing DR as an additional task. The problem is that such OPEX advantages are difficult to quantify.

I try to speak minimally about TCO except when an alternative bid has been delivered and I want to critique the other guy's numbers.

The real issue is what the data's value is and how much revenue the company stand to lose for every hour that their data is unavailable. Is an investment of x dollars per month worth it to prevent an outage cost of over $1M per hour?

- *ROI - what is the acceptable time 6 mos, 9 mos, 1yr?*

  ROI is irrelevant, or perhaps, better stated, ROI is immediate. Once data is protected, it will not be lost. If ROI is a comparison of the cost of a do it yourself approach versus XXXXXXXXX, with savings going to offset the annualized cost for the DRaaS service, the actual difference in cost will determine the return received. Most firms, however, have no idea what their homegrown DR strategy is costing them.

- *Why should potential customers purchase from* XXXXXXXXX *rather than competitors?*

  I cannot answer why they should buy XXXXXXXXX. I would buy XXXXXXXXX if…

  - They could demonstrate practical capabilities that I need: good software, good facilities, good network connectivity, smart and efficient staff, responsive support
  - They were affordable given my budget
  - They seemed to know something about data protection and DR and could support me with additional services like business impact analyses and hosting for some of my VMs in an emergency
  - Emphasized the privacy and security of my data at every turn (the key hit against clouds is the data vulnerability
  - They had impressive clients in their list or at least some reference accounts that would say nice things about them
  - They had press accounts attesting to their success in saving a client's data
  - They could show me a document detailing their best practices and methodology for doing data protection and disaster recovery: this would show me that they know what they are talking about

    - They offered useful references on their website describing what things cost, what techniques companies are preferring, what legal or regulatory mandates are coming, etc. This data can help me sell my management

- How important are the following individually and collectively to our prospects?
    - Buying from a vendor with a singular focus on DR – VERY
    - Buying a purpose-built solution – VERY
    - Low RTO and low RPO – MUST MEET CUSTOMER NEEDS
    - Ability to test in mirrored sandbox environment before pushing to production -- TERMS LIKE MIRRORED SANDBOX ARE SILLY, MUST BE ABLE TO TEST SIMULATED BEFORE ACTUALLY FAILING OVER
    - DR vendor that can also provide point-in-time recovery and managed backups – IF I NEED THAT I WOULD SO SPECIFY
    - North-American based Tier 1 Support Engineers – VERY
    - Easy to deploy solution – VERY
    - OPEX versus CAPEX model – SEE ABOVE, MOSTLY IRRELEVANT
    - Security: Penetration testing in a complete mirrored environment to mitigate risk to production systems during pen testing – SECURITY IS KEY, REGARDLESS OF THE TESTING METHODS USED TO VALIDATE

CONCLUSION

The above responses provide our insights into the DRaaS business and what is required to make a firm such as XXXXXXXXX competitive in the DRaaS marketplace. Additional information is required to focus these responses more explicitly on XXXXXXXXX go-to-market strategy.

The final component of the XXXXXXXXX email comprised a series of “fill in the blanks” statements. Generally speaking, these cannot be completed until after the responses above are reviewed and discussed to identify how XXXXXXXXX elects to frame its service. Ideally, filling in the document would be an interactive process.

We hope this helps.