Selling Disaster Recovery-as-a-Service to the C-Suite

Executives don't need to turn to the Worst Case Scenario Survival Guide for potential threats because they typically don't need to worry about quicksand, volcanos, killer bees, or sharks. However, a quick look at today's headlines is enough to cause concern:

> Air travelers stranded for hours due to a "computer glitch."

> Data breach at a credit reporting firm releases personal information of millions of US customers.

> A popular social media site has a "data center outage" which affects thousands of businesses websites.

Increasingly, business continuity relies on the critical data resident in networked systems. When thinking of disasters that might affect businesses, we often conjure images of dramatic natural disasters. However, seemingly mundane acts such as a prolonged power outage or equipment failure can impact the continued operation of an organization.

While there may be a perception that these are no-to-low incidence events, according to a Ponemon Institute[i] report of data center outages, data centers experience total shutdowns an average of more than twice every two years, localized shutdowns nearly six times every two years, and limited outages more than 10 times per year.

> "Currently, organizations suffer application downtime 13 times a year, with the total cost of downtime and data loss reaching up to $10,163,114.00."
>
> — VEEAM DATA CENTER AVAILABILITY REPORT 2014[ii]

In TechTarget's annual IT Priorities Survey for 2015,[iii] Disaster Recovery/Business Continuity was the top priority for North American IT Professionals. However, while IT leaders consistently identify disaster recovery as a high or critical priority, projected spending as a percentage of overall IT budgets remains flat or down. With the demands placed on IT budgets, it may be a challenge to assign funding for a contingency that many believe is unlikely to occur.

What is Disaster Recovery-as-a-Service?

Traditional approaches to disaster recovery range from copying data on a flash drive and taking it home to duplicating the production data center. While the flash drive option is cheap, it is not a good solution. On the other hand, replicating a data center requires not just the initial capital investment but also ongoing personnel, management, real estate, maintenance, and upgrade costs. This is often cost prohibitive as well as inflexible. Fortunately, cloud-based resiliency services such as Disaster Recovery as a Service (DRaaS) offer IT managers more choices and flexibility, making disaster recovery available to all sizes of organizations.

DRaaS typically offers layers of protection ranging from simple backup to near-zero recovery time of data and workloads on all virtual and physical environments. Distinguishing factors in choosing the level of services and provider may be geographic coverage, range of services, ability to meet compliance requirements, flexibility of contract terms, depth of experience, and consultative and support services.

According to a survey conducted by the Aberdeen Group, respondents who utilize DRaaS report cost savings as the leading benefit of using cloud for disaster recovery. Faster recovery time from downtime incidents ranks a close second. In fact, DRaaS users recover three times faster than in-house infrastructure users.

There are a wide range of DRaaS offerings, so it is important to identify providers that have extensive experience not just with cloud hosting, but also with the imperatives of DR. Because disasters create a crisis environment they, increase the need for the immediate return to operation and the ability to test and view the solution. Therefore, DRaaS is not just an add-on to a cloud service provider's offerings but must be a focused discipline with appropriate infrastructure and staffing expertise.

> "iland has a sustainable approach with respect to product strategy and feature enhancements for customers. It has expertise on staff with respect to both DevOps and compliance. The result is material that is both concise and easily consumable."
>
> — GARTNER MAGIC QUADRANT, FOR DISASTER RECOVERY AS A SERVICE, JUNE 2017[vi]

> "According to a June 2015 Ponemon Institute report, there are "a large portion of companies remain vulnerable as a result of lack of executive interest in preparing for worst-case scenarios."

Disaster Recovery and the C-Suite

As we've seen above, IT executives are on board with the need for disaster recovery, yet often their budgets don't reflect this imperative. According to a June 2015 Ponemon Institute report,[iv] there are "a large portion of companies who remain vulnerable as a result of lack of executive interest in preparing for worst-case scenarios."

Enlisting the support of top executives can influence budgeting for this critical decision as long as it is presented in a way that addresses their concerns and issues. Due to the varied charters of top executives, there may be multiple approaches required and a variety of potential impacts. Step into the shoes of the decision maker to determine how to best make the case for disaster recovery.

"C-Suite" typically refers to the top executives at an organization, so named because many of their titles begin with a "C," as in Chief Executive Officer. Let's examine a few of the key positions and their primary charters, challenges, and considerations so we can build the case for disaster recovery.

CEO/COO - Chief Executive Officer and/or Chief Operations Officer

Depending on the size and scope of an organization, there may be both a CEO and a COO. Although they have delegated detailed budget decisions to their subordinates, anything that risks the ongoing conduct of the business is their purview. Components of a DRaaS offering that would appeal most to CEO/COOs are the time to business resumption (e.g. near-zero RTO), the ability to pay-as-you-go without a large capital investment, the ability to prioritize data and workloads for

restoration and the flexibility to test to ensure proper operation in case a disaster is declared. They will look to trusted independent sources and similar customers for proof that a DRaaS solution is reliable, proven and cost-effective.

Chief Information Officer

CIOs have a tough balancing act: they must balance costs with the need to limit exposure. They may have to meet compliance requirements imposed by regulation or standards bodies. They also often have a personal stake in the recovery after adverse events. The CIO of a large global retailer was forced to resign in 2014 after the theft of 40 million customer credit card numbers and details on 70 million customers. CIOs need to satisfy the needs of different stakeholders and business imperatives with DR – and this is a huge challenge. The iland 6 Disaster Recovery Doppelgangers quiz and e-book can help CIOs approach their disaster recovery challenges across their organization.

From the CIO's standpoint, the ability to see and manage the recovery process is essential. CIOs also value access to scalable, on demand resources; especially when coupled with flexible terms. The ability to maintain security and compliance are imperative. Additionally, the ability to test on-demand to ensure the DRaaS solution continues to perform even through ongoing configuration changes to the day-to-day operational environment is important to most CIOs.

Chief Financial Officer

As their primary responsibility is financial, they must be approached from a fiscal angle. They look for an unbiased, independent perspective. Often perceived as being risk averse, they will invest in sound decisions, especially when they see a value proposition backed by financials and metrics. Flexible pricing options that can be tailored to a granular level based on services required per resource and the ability to 'Pay-as-you-go' and avoid high upfront capital investment will be very important to the CFO. The geographic constraints on their data (maintaining presence in a particular jurisdiction) may also be a factor for the CFO. They too will look to trusted independent sources and similar customer situations for references.

> The average cost of a data breach is $3.79 million (23% increase since 2013)

> The average cost per lost or stolen record is $154 (12% increase since 2013)

— INFOWORLD, MAY 2015[v]

CMO Chief Marketing Officer

While traditionally associated with branding, advertising, and public relations, more often the CMO has key objectives tied to customer loyalty as well. An obvious concern of CMOs is how the negative press around disasters affects brand image and customer loyalty. This is not just the headlines and news coverage. A quick look at the Twitter feed during a recent United Airlines technical outage provides insight into just how profoundly the news of the outage influenced the likelihood of customers choosing United the next time they flew. On average, it is cheaper to retain a customer than to acquire a new one. However, retaining or re-acquiring a customer after an IT disaster can be almost impossible: it's not just the downtime, but the loss of trust. The CMO will not be interested in the details of the services chosen but can be a strong supporter on the need for DR to protect brand image as well as maintain excellent customer support.

Roadblocks to Fulfilling your DR Plan Making the Case to the C-Suite

This grid can help you decide which aspects of DRaaS are most helpful in presenting the need for DR to the executive team. We've identified key aspects of DR and mapped them to the priorities of each executive team member. Identify which ones you require for your situation now and in the future.

Components of Disaster Recovery (Not all providers may offer all aspects.)	Important to our situation	CEO/COO	CFO	CIO	CMO/CSO
Access to scalable, on demand, infrastructure			X	X	
Pay-as-you-go with less upfront capital investment		X	X	X	
Flexible contract and payment options		X	X	X	
Maintaining security and compliance throughout and after failover		X	X	X	X
Ability to failover test on demand, as often as needed				X	
Supports range of virtual machines (VMware, Microsoft Hyper-V, Citrix Xen, etc.) as well as physical environments				X	
Backup of data to a secondary cloud site: 'cloud-to-cloud replication'			X	X	
Near-zero Recovery Time Objective (RTO)		X	X	X	X
Customer service and consultation				X	
Visibility and control: Ability to see and manage DR resources on demand via a portal				X	
Operation in desired geography & global data center coverage			X	X	
Solution vetted by independent sources and other customers		X	X	X	

X = primary consideration for this management position.

Build your case based on the key elements of your firm's DR requirements. Focus on the aspects that the target executive needs the most and that will be highly impacted by unplanned outages. These will be the biggest factors that can positively influence the C-suite towards prioritizing DRaaS come budget time.

> "iland had solid customer survey satisfaction scores, and existing customers applauded support, the portal and the underpinning Zerto-based solution"
>
> — GARTNER MAGIC QUADRANT, FOR DISASTER RECOVERY AS A SERVICE, JUNE 2017[vi]

iland Disaster Recovery-as-a-Service (DRaaS)

iland is a global cloud service provider of secure and compliant hosting for infrastructure (IaaS), disaster recovery (DRaaS), and backup as a service (BaaS). With over a decade of disaster recovery expertise, we can go far beyond simple backup to ensure all your key workloads are protected. We've partnered with Zerto and integrated their replication technologies into our Secure Cloud Console to provide cloud-based DRaaS that replicates data at the hypervisor-level. The combined iland and Zerto solution delivers exceptional recovery times and recovery points – both measured in mere minutes. And, you'll be able to test your DRaaS system on a self-service basis from the iland console, whenever you like, ensuring your confidence in the solution. Don't just take our word for it – iland was named a Leader for DRaaS by Gartner and Forrester in their 2017 reports.

> "Its self-service console integrates the underpinning replication solutions and makes it easy for customers to perform all operations on a single console."
>
> — THE FORRESTER WAVE: DISASTER RECOVERY AS-A-SERVICE PROVIDERS, Q2 2017[vii]

About Zerto

In today's connected world, businesses need to be available to their customers, 24/7/365. Zerto's software platform provides enterprise IT resilience for the cloud, enabling customers to withstand disruptions, incorporate new technology easily, and quickly adapt to accommodate evolving IT priorities. Zerto's award-winning Cloud Continuity Platform, protecting thousands of enterprises worldwide, is a simple and reliable business continuity and disaster recovery software solution built to protect applications on virtualised IT environments, be it public, private or hybrid cloud. Learn more at www.zerto.com.

i) Ponemon Institute 2013 Cost of Data Breach Study
http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

iii) Veeam Data Center Availability Report 2014 The Challenge of the Always-On Business
http://www.veeam.com/wp-availability-report-2014.html

iii) TechTarget's 2015 IT Priorities Survey April 2015, http://searchcio.techtarget.com/essentialguide/IT-Priorities-Survey-Pros-2015-tech-plans-projects-and-concerns

iv) Ponemon Institute 2015 Cost of Data Breach Study: Global Analysis
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF

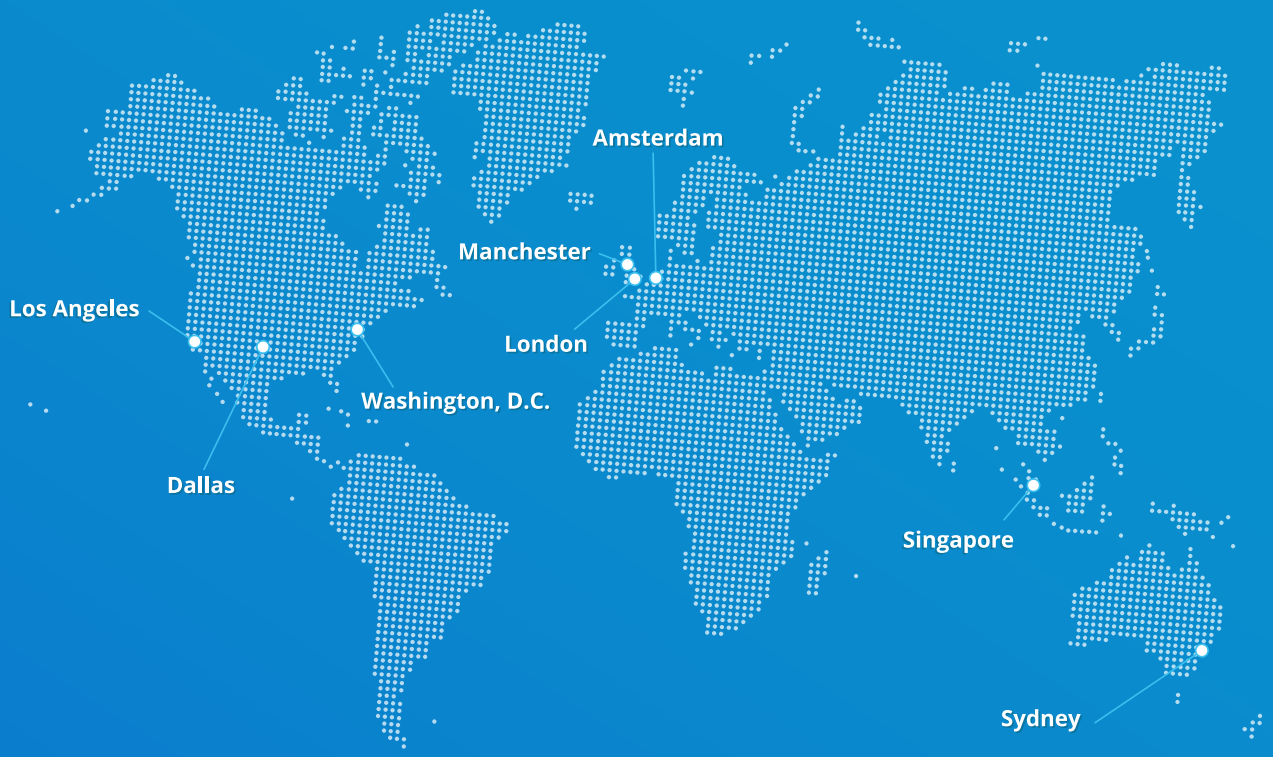
v) InfoWorld May 28, 2015 http://www.infoworld.com/article/2927397/security/the-cost-of-a-data-breach-jumped-23-percent-in-two-years.html

vi) Gartner Magic Quadrant for Disaster Recovery as a Service, June 2017 https://info.iland.com/gartner-draas-mq

vii) "The Forrester Wave™: Disaster-Recovery-As-A-Service Providers, Q2 2017,"
Forrester Research, Inc., https://info.iland.com/draas-forrester-wave-17

Contact

United States	+1 713 868 2267
United Kingdom	+(44) (0) 20 7096 0149
Netherlands	+(31) (0) 10 808 0440
Singapore	+(65) 3158 8438
Australia	+(61) (0) 2 9056 7004



About iland

iland is a global cloud service provider of secure and compliant hosting for infrastructure (IaaS), disaster recovery (DRaaS), and backup as a service (BaaS). They are recognized by industry analysts as a leader in disaster recovery. The award-winning iland Secure Cloud Console℠ natively combines deep layered security, predictive analytics, and compliance to deliver unmatched visibility and ease of management for all of iland's cloud services. Headquartered in Houston, Texas and London, UK, iland delivers cloud services from its data centers throughout the Americas, Europe, Australia and Asia. Learn more at iland.com.

iland®