INGRAM MICRO ADVISOR

Protect your business (and that of your customers) as a disaster recovery provider

JAN
03

SHARE g+ in 🐦 f

Flood. Cyberattack. Disruptions can occur at any time. As a disaster recovery provider, you're likely prepared for that rainy (or worse) day. But what steps have you taken to keep you and your customers in business and out of court?

Practice what you preach

While offering disaster recovery as a service (DRaaS) may be a on your sales line card, do you have your own data center business-continuity plan in place? If so, you've gone a long way to mitigate your own businesses' risks and gain a competitive advantage. "Make sure your house is in order, especially with disaster recovery policies that make up the foundation of what you're providing to your customers," says Nick Vermiglio, Ingram Micro technology consultant. These business-continuity benefits apply to you and your customers, including:

- Keeping the doors open while continuing operations and service delivery
- Reducing the cost of disruptions
- Taking advantage of insurance premium discounts
- Building your customers' confidence and trust by being prepared and competent
- Meeting compliance, regulatory and legal requirements
- Mitigating reputation and financial exposure
- Preserving your brand value and company reputation

Get legal, get smart

If disaster strikes, your disaster recovery plan should help keep you and your customers in business and out of court. Consider the following pointers:

- **Get your customer's legal team involved:** TechTarget's article on the legal issues for business disaster recovery plans includes these 3 tips:
    - Advise your customer's legal staff of your disaster recovery planning
    - Invite their legal staff to be a part of the planning team
    - Encourage their input
- **Stay current:** Gartner's business-continuity report about the laws influencing business continuity and disaster recovery recommends staying current with federal and state laws and regulations that apply to your customer's specific business sector. Also, stay up to date with business continuity management (BCM) guidelines within International Organization for Standardization (ISO) 17799 to satisfy most federal- and state-mandated business-continuity plans. "Try to be as, if not more so, knowledgeable about your customer's industry than they are," says Vermiglio.
- **Partner for external auditing:** If requested, an external audit of your customer's disaster recovery plan goes a long way to validate that it meets all necessary requirements. For example, Deloitte offers a Risk and Financial Advisory Cyber Resilience service, which

reviews customer documentation and operations to make sure that your customer's plan complies with industry standards.

Consider certification

The training and testing processes for business-continuity certification programs demonstrate that your staff is fully trained and knowledgeable in the field of business continuity. Most are built around commonly accepted industry standards. Some of the more recognized business-continuity certifications include:

- **Certified Business Continuity Professional (CBCP)**: Disaster Recovery Institute International (DRI) offers education and accreditation in business continuity and related fields. The CBCP is one of the most recognized and popular designations in the business-continuity industry.
- **Certificate of the Business Continuity Institute (CBCI)**: Offered through the Business Continuity Institute, which is more widely used in Africa, Asia and Europe, this globally recognized credential tests knowledge of the Good Practice Guidelines (GPG)—comprehensive guide to business-continuity and resilience industry best practices.
- **EC-Council Disaster Recovery Professional (EDRP):** The EDRP certification demonstrates that its recipients have skills to develop enterprise-wide business continuity and disaster recovery plans.

Topics: Big Data, Data Center, Disaster Recovery

LEGAL DISCLAIMER

Opinions expressed on this publicly available site and any follow-on comments are the personal opinions of the author(s) and not of Ingram Micro Inc., its business units worldwide, employees, officers or directors. The content is informational only and is not an endorsement by Ingram Micro Inc., its business units worldwide, employees, officers or directors. The author(s) acknowledge and agree that this site is available to the public. Author(s) represent and warrant that neither confidential data nor information shall be posted on this site and if such is posted shall be the sole responsibility and liability of the author(s) and not Ingram Micro Inc, its business units worldwide, employees, officers or directors. The posting author(s) represents and warrants to all readers that it is solely responsible for the content of all information contributed, linked to, or otherwise upload on the site and agrees to hold Ingram Micro Inc, its business units worldwide and all employees, officers and directors harmless from and defend and indemnify Ingram Micro Inc., its officers, employees and directors from any and all claims related to the material so posted. The author grants Ingram Micro Inc. and its business units a royalty free, perpetual and worldwide license to publish any and all original works and content posted by the author(s) on the site.