Business Continuity and Disaster Recovery Checklist

Threats to your business operations come in many forms, from hurricanes and fires to cyberattacks on your company's network. Conducting a risk assessment and putting a business continuity plan in place now might mean the difference between hours out of operation and days out of operation. Disaster recovery — a company's ability to save and restore its data — is a critical part of business continuity planning. This checklist can help your company assess its readiness.

☐ Take steps now to prevent and plan for a disaster

- ☐ Assign an employee with sufficient seniority and skill to "own" business continuity and disaster preparation and recovery
- ☐ Conduct a risk analysis, to identify the most likely risks and the impact of each on critical operations
- ☐ Conduct a security analysis, to determine the company's resiliency for each risk as to critical operations
- ☐ Build and implement a business continuity / disaster recovery plan, and update and train employees on it periodically
- ☐ Appoint and train a business continuity team to lead response efforts
- ☐ Select external business continuity / disaster response partners, including information technology consultants and attorneys, and inform them of their role
- ☐ Discuss disaster preparation with key suppliers and customers
- ☐ Assess network security
- ☐ Assess data backup and recovery systems
- ☐ Assess alternate communications methods for email or phone outages and compromises
- ☐ Assess cash management needs during a disaster, including with the company's bank
- ☐ Assess insurance coverage, particularly for business interruption
- ☐ Identify alternative operational locations
- ☐ Maintain contact lists of key customers and vendors, and copies of key agreements with each
- ☐ Maintain an inventory of all equipment
- ☐ Identify options for accommodation (hotels, etc.) and provisions (food & drink, etc.) during disaster operations

☐ During a disaster, implement the plan

- ☐ Notify and assemble the business continuity team
- ☐ Implement the business continuity / disaster recovery plan
- ☐ Make appropriate warning, evacuation, or other initial communication to employees
- ☐ Commence physical mitigation, focusing on employee and public safety
- ☐ Commence technical mitigation, focusing on critical systems
- ☐ Implement alternate communications methods
- ☐ Activate redundant or alternate information systems (“failover”)
- ☐ Notify external partners for assistance with containment and remediation (including counsel for attorney-client privilege considerations)
- ☐ Communicate regularly with employees, suppliers, customers, and vendors
- ☐ Notify insurance brokers and carriers
- ☐ Notify law enforcement as appropriate
- ☐ Preserve records of the disaster and mitigation efforts

☐ After a disaster, improve the plan

- ☐ Continue communication efforts, both internal and external
- ☐ Document damages to systems, physical plant, and revenue
- ☐ Bring the day-to-day information systems back online, integrating with your disaster recovery systems (“failback”)
- ☐ Consider any regulatory reporting obligations
- ☐ Assess liabilities and remedies under contracts with suppliers, customers, and vendors
- ☐ Assess insurance coverage
- ☐ Evaluate effectiveness of prevention, mitigation, and backup tools
- ☐ Hold a “lessons learned” meeting of disaster recovery team
- ☐ Revise business continuity / disaster recovery plan as appropriate

For more information, contact:

Joseph W. “Joe” Swanson
Direct: 813.229.4335
JSwanson@carltonfields.com

Steven J. Brodie
Direct: 305.539.7302
SBrodie@carltonfields.com

John E. “Jack” Clabby
Direct: 813.229.4229
JClabby@carltonfields.com

David M. Leonard
Direct: 404.815.3380
DLeonard@carltonfields.com