The Legal Issues of Business Continuity Planning

By Neil H. Kaufman
SVP & National BCP Practice Leader
Risk Solutions International LLC

Despite the widespread reporting of disasters and their effects, many companies, corporate directors, and officers remain apathetic toward implementing a business continuity/disaster recovery plan. Many companies are generally unwilling to commit the finances and resources to implement a plan unless forced to do so. However, implementing a business continuity/disaster recovery plan is a strategic, moral, and legal obligation to one's company. If the billions of dollars spent on technology annually to maintain a competitive edge is an indication of how reliant our society is on technology, then failing to implement a disaster recovery plan is an indication of corporate negligence. Standards of care and due diligence are required of all corporations, public or private. Not having a disaster recovery plan violates that fiduciary standard of care.

The legal issues involved in corporate contingency planning are some of the most misunderstood and confusing aspects of the entire process of creating a disaster recovery plan. Disaster recovery planners are not expected to be lawyers. However, they are encumbered with the responsibility of understanding the minutiae and vagueness of existing regulatory guidelines and the legal consequences of their company's failure to implement an effective disaster recovery plan. Although no specific laws state categorically that companies must have a disaster recovery plan, there is a body of legal precedents which can be used to hold companies and individuals responsible to those affected by a company's inability to cope and/or recover from a disaster. The entire basis of law relating to the development of disaster recovery plans is based on civil statutes and an interpretation of applicability to disaster recovery planning.

One of the precedents which can be used against companies which fail to plan for a disaster is drawn from the case of FJS Electronics v. Fidelity Bank. In this 1981 case, FJS Electronics sued Fidelity Bank over a failure to stop payment on a check. Although the failure to stop payment of the check was more procedural in nature, the court ruled that Fidelity Bank assumed the risk that the system would fail to stop a check. FJS was able to prove that safeguards should have been in place and therefore was awarded damages.

This case shows that the use of a computer system in business does not change an organization's duty of reasonable care in its daily operations. The court ruled that the bank's failure to install a more flexible, error-tolerant system inevitably led to problems. As a result, information technology professionals will be held to a standard of reasonable care and can breach that duty by not diligently pursuing the development of a disaster recovery plan.

To help you become aware of the areas where disaster recovery planning and the law intersect, we have categorized applicable statutes. While each category is presented, this list is intended to be neither exhaustive nor fully comprehensive.

1. **Contingency Planning Statutes** - Apply to the development of plans to ensure the recoverability of critical systems. Example: Federal Financial Institutions Examination Council ("FFIEC"). The FFIEC guidelines replace previously issued Banking Circulars BC-177, BC-226, etc.

2. **Liability Statutes** - Establish levels of liability under the "Prudent Man Laws" for directors and officers of a corporation. Example: Foreign Corrupt Practices Act ("FCPA").

3. **Life / Safety Statutes** - Set out specific ordinances for ensuring the protection of employees in the workplace. Examples: National Fire Protection Association ("NFPA"), Occupational Safety & Health Administration ("OSHA").

4. **Risk Reduction Statutes** - Stipulate areas of risk management required to reduce and/or mitigate the effects of a disaster. Examples: Office of the Comptroller ("OCC") Circular 235 and Thrift Bulletin 30. Security Statutes cover areas of computer fraud, abuse and misappropriation of computerized assets. Example: Federal Computer Security Act.

5. **Vital Records Management Statutes** - Specifications for the retention and disposition of corporate electronic and hardcopy records. Example: IRS Records Retention requirements.

STATUTORY EXAMPLES

When the time comes to defend your company against a civil or criminal lawsuit resulting from damages caused by your company's failure to meet a standard of care, you'll need more than an "Act of God" defense. When no direct law or statute exists for a specific industry, the courts will look to other industries for guidelines and legal precedents. The following three statutes represent the areas in which a court will most likely seek a legal precedent:

1. Foreign Corrupt Practices Act ("FCPA") - The FCPA of 1977 was originally designed to eliminate bribery and to make illegal the destruction of corporate documents to cover up a crime. To accomplish this, the FCPA requires corporations to "... make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets..." The section of this Act which keeps it at the forefront of disaster recovery liability is the "Standard of Care" wording, whereby management can be judged on their mismanagement of corporate assets. The FCPA is unique in that it holds corporate managers personally liable for protecting corporate assets. Failure to comply with the FCPA exposes individuals and companies to the following:

- Personal fines up to $10,000;
- Corporate fines up to $1,000,000; and
- Prison terms up to five years.

2. In the financial services industry, the **Federal Financial Institutions Examinations Council ("FFIEC")** - The Comptroller of the currency has issued various circulars dating back to 1983 (e.g., Banking Circular BC-177) regarding the need for financial institutions to implement disaster recovery plans. However, in 1989, a joint-agency Circular was issued on behalf of the following agencies:

- Board of Governors of the Federal Reserve System ("FRB");
- Federal Deposit Insurance Corporation ("FDIC");
- National Credit Union Administration ("NCUA");
- Office of the Comptroller of the Currency ("OCC"); and
- Office of Thrift Supervision ("OTS").

The Circular states that "The loss or extended interruption of business operations, including central computing processing, end-user computing, local area networking, and nationwide telecommunications poses substantial risk of financial loss and could lead to failure of an institution. As a result, contingency planning now requires an institution-wide emphasis..." The FFIEC guidelines relating to contingency planning are actually contained within 10 technology related Supervisory Policy Statements. These policies are revised every two years and can be acquired through any of the five agencies listed above.

3. The Consumer Credit Protection Act ("CCPA") - On November 10, 1992, the 95th Congress, 2nd Session, amended section 2001 of the Consumer Credit Protection Act (15 U.S.C. 1601 et seq.) "TITLE IX - Electronic Funds Transfers." The purpose of this amendment was to remove any ambiguity the previous statute had in identifying the rights and liabilities of consumers, financial institutions, and intermediaries in Electronic Funds Transfers. This Act covers a wide variety of industries, specifically those involved in electronic transactions originating from point-of-sale transfers, automated teller machines, direct deposits or withdrawals of funds, and fund transfers initiated by telephone. The Act further states that any company which facilitates electronic payment requests which ultimately result in a debit or credit to a consumer account must comply with the provisions of the Act. Failure to comply with the provisions of this Act exposes a company and its employees to the following liabilities:

- Any actual damage sustained by the consumer;
- Amounts of not less than $100 or greater than $1,000 for each act;
- Amounts of $500,000 or greater in class action suits; and
- All costs of the court action and reasonable attorneys' fees.

Companies covered under this Act are subject to all liabilities and all resulting damages proximately caused by the failure to make an Electronic Funds Transfer. The Act states that a company may not be liable under the Act if that company shows by a "preponderance of evidence" that its actions or failure to act were caused by "... an Act of God or

other circumstances beyond its control, that it expressed reasonable care to prevent such an occurrence, and that it expressed such diligence as the circumstances required ..." Each of these statutes are based on the precept of Standard of Care. Standard of Care is described by the legal publication entitled Corpus Juris Secundum, Volume 19, Section 491 as "... directors and officers owe a duty to the corporation to be vigilant and to exercise ordinary or reasonable care and diligence and the utmost good faith and fidelity to conserve the corporate property; and, if a loss or depletion of assets results from their willful or negligent failure to perform their duties, or to a willful or fraudulent abuse of their trust, they are liable, provided such losses were the natural and necessary consequences of omission on their part ..."

CONTRACTUAL SERVICE LEVEL AGREEMENTS

Any service, whether in-house, contracted or outsourced, can be accused of being insensitive to the requirements of its customers (or users) and of providing inadequate service, absent specific duties assigned to its business partners. One difficult aspect of disaster planning that you will have to tackle and that will determine many elements that you should include in your plan is the "service level agreement" (SLA) that you negotiate with your vendors and customers. SLAs are essentially the contractual promise you make to your customers, and that *your* vendors make to *you*, about how long business processes will remain available, regardless if there is an emergency. SLAs are made up of, among others:

- Order, inventory and delivery quantities
- Shipment and receipt dates
- Customer support
- Service hours
- Roles and responsibilities

SLAs are often predominantly influenced by customer perspectives and prejudices, making them very difficult to deal with on a technical level, yet highly influential as to whether your company will remain in business - from a disaster impact perspective. These service level agreements are well understood in the technology realm (recovery time guarantees from outsourced data center vendors, e.g.). In the manufacturing, distribution, retail and consumer packaged goods industries, the issue of supply chain disruptions are taking on the legal spotlight. Natural disasters, vendor/distribution failures, dock strikes and border/importing issues highlight reasonable and foreseeable risks to mitigate. Supply chain partners, vendors and their clients have set a higher standard for operational resiliency at their business partners' organizations and have mandated that senior management be involved strategically and tactically in the event of disruptions. They recognize that their biggest risk – their vendors' ability to withstand emergencies – is largely out of their control. Incidents of supply chain tampering are growing as sourcing continues to move into less developed countries and longstanding quota protocols are eliminated. The new threats to consider include:

- Pandemic Flu Quarantines that can shut down FOB ports
- Increased regulatory attention from Homeland Security and U.S. Customs
- Geographic concentration of facilities in high risk countries of origin
- Business partner service level agreements that require business continuity plans and include a "right to audit" those plans
- Diversion, trans-shipping, counterfeiting, "grey" goods and supply chain "shrinkage" significantly impact globally-stretched supply chains
- Requirements by leading retailers for third party certification of the resilience of your operations as a supplier
- Single and sole source supplier dependency

DETERMINING LIABILITY

Courts determine liability by weighing the probability of the loss occurring against the magnitude of harm, balanced against the cost of protection. This baseline compels companies to implement a reasonable approach to disaster recovery in which the cost of implementation is in direct correlation to the expected loss. In other words, if a company stands to lose millions of dollars as a result of an interruption to its computerized processing, the courts would take a dim view of a recovery plan which lacked the capability to restore the computer systems in a timely manner.

Another precedent-setting case referred to as the Hooper Doctrine can be cited when courts are looking to determine a company's liability. This doctrine establishes that even though many companies do not have a disaster recovery plan, there

are "precautions so imperative that even their universal disregard does not excuse their omission." Simply put, a company cannot use, as a defense, the fact that there are no specific requirements to have a disaster recovery plan and that many other companies do not have one.

Liability is not just related to corporations, but to individuals who develop disaster recovery plans as well. In 1989, in Diversified Graphics v. Ernst & Whinney, the United States Eighth Circuit Court of Appeals handed down a decision finding a computer specialist guilty of professional negligence. In this case, professional negligence was defined as a failure to act reasonably in light of special knowledge, skills and abilities. If the directors and officers of a corporation can be held accountable for not having a disaster recovery plan, then this case provides the precedent for individuals who are certified disaster recovery planners to be held personally accountable for their company's disaster recovery plan.

INSURANCE AS A DEFENSE

Directors and Officers ("D&O") of companies have a fiduciary responsibility to ensure that any and all reasonable efforts are made to protect their companies. D&O insurance only protects officers if they used good judgment and their decisions resulted in harm to their company and/or employees. D&O insurance does not cover a company officer who fails to exercise good judgment, e.g., not implementing a disaster recovery plan.

Errors and Omissions ("E&O") insurance covers consequential damages which result from errors, omissions, and/or negligent acts committed in the course of business. In a 1984 precedent-setting case heard in the District Court of Ohio, the court ruled, "Negligence is a failure to exercise the degree of care that a reasonably prudent person would exercise under the same circumstance." With regard to a trade, practice or profession, "the degree of care and skill required is that skill and knowledge normally possessed by members of that profession in good standing in similar communities."

Property Coverage will not cover companies from loss of shelf space for your product. It will also not cover losses from interruptions like a dock strike or pandemic disease outbreak that negatively impacts your critical business processes.

Liability insurance will not prevent court actions, but it will pay toward the litigation and any penalties incurred as a result. Disaster recovery practitioners possess a unique expertise and subsequently could be held accountable for their actions and advice in the development of a disaster recovery plan. A word of caution here is that if you pass yourself off as an expert; expect to be held accountable as an expert.

SUMMARY

Courts will assess liability by determining the probability of loss, multiplied by the magnitude of the harm, balanced against the cost of prevention. Ostensibly, should your company end up in litigation, the burden of proof would be on your company to prove that all reasonable measures had been taken to mitigate the harm caused by the disaster. There are clearly enough legal precedents for the courts to draw on in determining if a "Standard of Care" was taken or if "Due Diligence" was exercised in mitigating the effects of the disaster on your company's critical business operations.

Every business is governed by laws which dictate how they must conduct themselves in the normal course of business. By researching these laws and statutes, you will eventually find where penalties for non-performance are stipulated. These penalties become your demarcation point for "reverse engineering" your business operations, and thus exposing the points of failure which could affect your company's ability to perform under the statutes that specifically govern your business.