

Legal Requirements for Disaster Recovery Planning: Common Facts and Misconceptions



By [Leo Wrobel](#)

Date: Aug 3, 2007

[Return to the article](#)

Legal responsibility for disaster recovery is no longer limited to the executive corner office. Today, new federal laws and regulations make it everyone's concern. Get the straight story from Eddie M. Poe, author and attorney, and Leo A. Wrobel, noted author and industry expert. Learn about the liabilities of not complying with these regulations; then share this information with management to add a new sense of urgency to your disaster recovery planning efforts!

As noted in my previous article, ["How Sarbanes-Oxley Affects Your Disaster Recovery Planning"](#), there are many misconceptions about the legal requirements for disaster recovery planning. As with the previous article, I went straight to the source to inquire exactly what we should be concerned about.

Naturally my lawyer friend, Eddie M. Pope, began by stating that this is not legal advice, per se, and if you have detailed questions, you should consult a lawyer. Gee, I wonder why he said that.

All kidding aside, this article is intended as a brief overview for the layperson of what is legal fact, what is fiction, and what lives in the gray area in between the two.

As best I can tell as a non-lawyer, there are certainly many honest-to-goodness laws that mandate having a plan. Having said that, it is also my experience as a businessman that people tend to embellish. Sometimes they interpret "the law" in a way that is favorable to them instead of as it truly is.

Case in point: The aforementioned Eddie Pope, who is incidentally a co-author on my new book, was researching a chapter he wrote on legal requirements for a plan.

NOTE

The book is entitled "Business Resumption Planning, Second Edition" © 2007 Taylor Publishing, New York. It is the most awesome book on disaster recovery planning since *Noah and the Great Flood*. There, Eddie, now you can see lawyers aren't the only ones who can plug things... Look for publication this summer!

Eddie found several citations on the Web that said defense contractors must have a disaster recovery plan. That seems to make sense on the surface. I have published a lot over the last couple years about how disaster recovery activity 30 years ago in the military is now "fashionable" with what is going on today commercially.

Set in that context, the idea that the DOJ *must* have a plan has to be true, right? In fact, however, when my co-author tried to find a bona fide law, rule, or regulation that actually *stated* this fact, there was nothing to be found.

Is the notion of any law that mandates a disaster recovery plan the disaster recovery communities' equivalent of an urban myth or a story that is passed along from planner to planner, without anyone ever tracking back to see if it's true? If your management thinks it is true, this could seriously jeopardize your credibility and set back your planning efforts severely. Therefore let's get our facts straight on the legal requirements if possible.

An often-cited reason for disaster recovery planning is the Sarbanes Oxley Act of 2002, otherwise known as SOX 2002.

NOTE

Since I discussed this in my previous article, ["How Sarbanes-Oxley Affects Your Disaster Recovery Planning"](#), you should be able to go back and read it to separate fact from myth.

Besides Sarbanes-Oxley, the law keeps changing. Even if you are a lawyer, there is no way to easily or accurately keep up with all the changes. Even if you try, legal semantics and terminology come into play. (Hey, I am up to some antics!)

There is a myriad of terms in law and industry that *might* apply to different cases. For example, this series of articles discusses "disaster recovery planning." This is also commonly known as "business resumption planning." Other frequently used terms can include "crisis management," "emergency response planning," "contingency planning," and others.

If a law or a regulation includes a term of art akin to any of these, or even one it even mentioned above, it could *still* apply to your business. Is this confusing enough for you yet? Read on

So Who, Legally, MUST Plan?

With the caveats above, let's cover a few of the common laws where there is a duty to have a disaster recovery plan. I will try to include the basis for that requirement, where there is an implied mandate to do so, and what the difference is between the two

Banks and Financial Institutions MUST Have a Plan

The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, Title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established the Examination Council (the Council)

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS); and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council.

In March of 2003, the Council released its Business Continuity Planning handbook designed to provide guidance and examination procedures for examiners in evaluating financial institution and service provider risk-management processes.

Stockbrokers MUST Have a Plan

The National Association of Securities Dealers (NASD) has adopted rules that require all its members to have business continuity plans. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices and more than 658,770 registered securities representatives.

As of June 14, 2004, the rules apply to all NASD member firms. The requirements, which are specified in Rule 3510, begin with the following

3510. Business Continuity Plans. (a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to NASD staff.

NOTE

The rules apply to every company that deals in securities, such as brokers, dealers and their representatives, it does NOT apply to the listed companies themselves.

Electric Utilities WILL Need a Plan

The disaster recovery function relating to the electric utility grid is presently undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only *coordinate* volunteer efforts between utilities. This has changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C. §240). That new law authorizes the FERC to create an Electric Reliability Organization (ERO).

The ERO will have the capability to adopt and enforce reliability standards for "the users, owners, and operators of the bulk power system" in the United States. At this time, FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards.

It is very safe to assume that the ERO will adopt standards for service restoration and disaster recovery, particularly after such widespread disasters as Hurricane Katrina.

Telecommunications Utilities SHOULD Have Plans, but MIGHT NOT

Telecommunications utilities are governed on the federal level by the Federal Communications Commission (FCC) for interstate services and by state Public Utility Commissions (PUCs) for service within the state.

The FCC has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure [sic] optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks and the internet." The NRIC members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations, and government-related organizations.

There is no explicit provision that we could find that says telecommunications carriers *must* have a Disaster Recovery Plan. As I have stated frequently in this series of articles on disaster recovery, however, telecommunications facilities are tempting targets for terrorism. I have not changed my mind in that regard and urge caution.

You might also want to consider what the liability of a telephone company is if it has a disaster that causes loss to your organization. In three words: It's not much. The following is the statement used in most telephone company tariffs with regard to its liability:

The Telephone Company's liability, if any, for its gross negligence or willful misconduct is not limited by this tariff. With respect to any other claim or suit, by a customer or any others, for damages arising out of mistakes, omissions, interruptions, delays or errors, or defects in transmission occurring in the course of furnishing services hereunder, the Telephone Company's liability, if any, shall not exceed an amount equivalent to the proportionate charge to the customer for the period of service during which such mistake, omission, interruption, delay, error or defect in transmission or service occurs and continues. (Source, General Exchange Tariff for major carrier)

All Health Care Providers WILL Need a Disaster Recovery Plan

HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring "Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards."

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The final Security Rule was published by HHS on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect

against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect network, computers and other electronic devices.

Companies with More than 10 Employees

The United States Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. For example, 29 USC 654 specifically requires:

(a) Each employer

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act.

(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.

Other Considerations or Expensive Research Topics for Lawyers (Sorry, Eddie!)

- The Foreign Corrupt Practices Act of 1977
- Internal Revenue Service (IRS) Law for Protecting Taxpayer Information
- Food and Drug Administration (FDA) Mandated Requirement
- Homeland Security and Terrorist Prevention
- Pandemic (Bird Flu) Prevention
- ISO 9000 Certification
- Requirements for Radio and TV Broadcasters
- Contract Obligations to Customers
- Document Protection and Retention Laws
- Personal Identity Theft...and MORE

Suffice it to say you will need to check with your legal department for specific requirements in your business and industry!

I would like to thank my good friend, Eddie M. Pope, for his insightful contributions to this article, our upcoming book and my ever-growing pool of lawyer jokes. If you want more information on the legal aspects of recovery planning, Eddie can be contacted at my company or via email at <mailto:mempope@tellawcomlabs.com>. (Eddie cannot, of course, give you legal advice, but he can point you in the right direction)

I hope this article helps you better understand the complex realities of the legal reasons why we plan and wish you the best of luck
