

# THE JOURNAL OF BIOLAW & BUSINESS®

[www.biolawbusiness.com](http://www.biolawbusiness.com)

Reprint Series  
The Journal of BioLaw & Business  
Volume 6, Number 1 2003

## Surviving A Catastrophe: Are You Prepared?

**Philip W. Fiscus, CPCU**  
Chubb Group of Insurance Companies





# Surviving A Catastrophe: Are You Prepared?

Philip W. Fiscus

## ABSTRACT

*As biotech executives move to the front lines with patriotic and commercial fervor, many of their own firms remain vulnerable to terrorist threats and other catastrophes. From a business standpoint, a key lesson of September 11 was that companies that survive a catastrophe with a minimum amount of damage are inevitably those that plan ahead. However obvious the message, many biotechnology companies do not take the time to develop comprehensive plans that would reduce the likelihood and impact of a disaster; enable them to respond quickly and effectively to an emergency to ensure the safety of employees and to contain losses; and establish contingencies to stay in business during a disaster and resume normal business operations as quickly as possible. This article discusses specific protective measures that biotechnology companies should consider.*

## INTRODUCTION

Soon after the terrorist attacks of September 11, 2001, U.S. law enforcement officials discovered operating manuals for crop dusting equipment in terrorist hideouts, arousing fears that Al Qaeda was planning to disperse biological or chemical agents from planes normally used for agriculture.<sup>1</sup> With bioterrorism high on the national radar, attention turned to the critical role of the biotechnology industry in the nation's defense against biological and chemical weapons.

As biotech executives move to the front lines with patriotic and commercial fervor, many of their own firms remain vulnerable to terrorist threats and other catastrophes. From a business standpoint, a key lesson of September 11 was that companies that survive a catastrophe with a minimum amount of damage are inevitably those that plan ahead. However obvious the message, many biotechnology companies do not take the time to develop comprehensive plans that would reduce the likelihood and impact of a disaster; enable them to respond quickly and effectively to an emergency to ensure the safety of employees and to contain losses; and establish contingencies to stay in business during a disaster and resume normal business operations as quickly as possible.

Of course, biotechnology companies are not the only ones to leave themselves exposed. A worldwide information security survey by Ernst & Young found that only 53 percent of organizations had a business continuity plan, and many of those were not well developed or tested.<sup>2</sup> Nevertheless, with

their laser-like focus on research and development-and too little funding-biotechs may be less likely than other firms to dedicate the resources required to develop and maintain a comprehensive plan.

## THE RISKS

In many respects, the risks that biotechnology firms face are not very different from those of other companies. Fires, floods, hurricanes and equipment failures can affect any type of business. In some ways, though, biotechnology firms face greater risks. For one thing, they are disproportionately located on the East and West coasts, where they are vulnerable to hurricanes and earthquakes.<sup>3</sup> In California, where more than 25 percent of U.S. biotechnology firms reside, an energy crisis last summer ruined many experiments and damaged costly equipment at the many organizations that did not have sufficient backup power.<sup>4</sup>

Even before September 11, terrorism of a different sort posed a real threat to firms engaged in controversial genetic research or studies involving laboratory animals. Organizations like the National Association for Biomedical Research, whose members have been victimized by animal rights activists, estimate that the Animal Liberation Front has caused more than \$45 million in medical research and fur industry losses in the last 10 years.<sup>5</sup> In April 1999, the animal-rights group ransacked laboratories at the University of Minnesota, causing \$1 million to \$2 million in damage and setting back at least one research project by two years.<sup>6</sup> More



*Philip W. Fiscus, CPCU, is senior vice president of Chubb & Son, Whitehouse Station, N.J., where he serves as the worldwide product manager for Chubb's life sciences business segment.*

*Cite as: Philip W. Fiscus Surviving A Catastrophe: Are You Prepared? J. BIOLAW & BUS., Vol. 6, No. 1, 2002.*

recently, another extremist group, Earth Liberation Front, took credit for an arson fire at the construction site of the university's new Microbial and Plant Genomics building.<sup>7</sup>

What has been discussed far less frequently is the real possibility that individuals or groups who want to use chemicals or biological materials as a weapon may target biotechnology companies. The anthrax that was sent through the mail may have been stolen from a military or university laboratory. The government is just beginning to tackle the real possibility of terrorists contaminating the U.S. food supply. With their dependence on electronic information systems, biotechnology firms are also vulnerable to cyber attacks. Computer viruses and hackers cost businesses \$1.5 trillion worldwide, according to estimates by PricewaterhouseCoopers.<sup>8</sup>

The consequences of a disaster—whether caused by nature, an equipment failure or the deliberate act of a hacker or terrorist—can be devastating to a biotechnology firm. Almost any property loss in a laboratory or manufacturing facility can spark a series of disruptive and financially lethal chain reactions. The combination of property loss and business interruption can have an especially dire impact on the liquidity picture of small startup research enterprises. Revenue problems for these companies are not caused by decreased sales; their cash flow woes may result from a sudden and substantial loss of benchmark payments or grants from investors. These payments are tied to R&D deadlines that cannot be met because of disaster-related property damage. Newer and more fiscally fragile enterprises are less apt to survive such a loss of funding.

Directors and officers are also at risk. Should a disaster interrupt the smooth and profitable running of an organization, shareholders and their attorneys may try to prove that business leaders were negligent in their management and hold them responsible for their loss in stock value. Or, customers may hold a business responsible for their loss of revenues if the biotechnology company is unable to provide them with the product or service they need to continue their own operations. Even if the pursuit of a claim against a company's directors and officers does not succeed, the cost of defending it can cost millions of dollars.

If biotechnology firms do not act to adequately protect themselves from potential disasters, regulators may take steps to ensure they do. Since September 11, states with large concentrations of biotechnology firms have been discussing how such facilities may pose a threat to the public welfare, and they are trying to assess how well-protected they are. If the industry does not act on its own accord, it may face additional regulation.

## THE NEED FOR A PLAN

No one wants to contemplate the horrible possibilities, but the events of September 11 are forcing companies to think outside the box of traditional threat assessments as they consider a wide range of new and rapidly evolving exposures.

Biotechnology companies should be more proactive and plan against sudden business interruptions or disasters. A loss control audit is a good first step in minimizing your exposure to disaster. Such an audit might include property conservation and security hazard assessments and the development of loss control checklists to identify deficiencies and establish controls. When conducted by experienced loss-prevention experts, an audit provides a clear picture of the strengths and weaknesses in safety and security. An audit would identify proactive actions, based on current loss control measures, that could be put in place to lower the cost and minimize the overall energy or effort that would be needed to execute a business contingency plan.

To prepare for a disaster, a biotechnology firm must identify worst-case scenarios; conduct a business impact analysis that addresses all critical business functions; and formulate effective emergency preparedness and business recovery strategies. Because their work is so sensitive and is conducted in a highly regulated environment, biotechs should make sure they have good resources to assess security needs, to mitigate physical threats and to establish alternative business arrangements.

As companies attempt to develop plans to protect business assets, a critical component is the methodology used to identify and control vulnerabilities. Biotechs should locate corporate risks on four continuums: people, processes, technology and information. Using this approach will help organizations put together a strong framework to aid in the continuity or resumption of operations after any type of business interruption or disaster. A comprehensive plan addresses these major areas:

**1) Disaster preparedness.** This involves straightforward activities that reduce the likelihood and impact of a disaster. Once a company assesses its vulnerabilities, it can take steps to make sure it is protected. This may include backup power generators, fire protection systems, information backup, protection of vital records and security systems.

**2) Emergency response.** Companies should have a formal emergency response plan and a team to execute the plan. They must have proper plans for ensuring the safety of employees and, in the case of the release of a hazardous material, the safety of the community. Employees must be trained in what to do when a disaster strikes.

**3) Business continuation and restoration.** This involves defining priorities, arrangements and procedures that will keep a company viable during and after a disaster and returning operations to normal. As part of this process, companies must analyze the impact of "downtime," identify operational vulnerabilities and prioritize the allocation of critical resources so the business can continue while it recovers. Business continuation addresses alternate locations in the event of a prolonged facility

shutdown and arrangements with suppliers if specialized materials or equipment must be replaced. It also takes into the account the possible necessity of building a new facility.

The task of developing disaster preparedness and recovery plans can seem overwhelming, but once accomplished, they become a road map for a biotech's future and way to ensure that the company is adequately protected, physically and financially, against the potentially devastating effects of a disaster.

## PROTECTIVE MEASURES

Preparing for a disaster starts with taking a hard look at how well a company and its assets are protected. Animal rights groups have exposed the security vulnerabilities in many biotechnology organizations. The fundamentals of good security seem obvious, but too often they are overlooked. Security fundamentals include establishing a boundary around the facility; procedures for controlling access, including who can come in and when; security guards and/or electronic surveillance systems; and tests to ensure that those controls are always working.

Biotechs should be as concerned about who walks in the front door as they are about a possible break in. Consider the ease with which terrorists received training at legitimate flight schools. It is not far-fetched to consider any number of guises under which they could gain access as easily to a biotechnology firm.

Beyond the security fundamentals, biotechnology firms must be concerned about other possibilities that would leave their facilities vulnerable to infiltration. Imagine that after an earthquake, explosion or toxic spill local officials order an evacuation. Biotechnology firms need another level of security to compensate for the absence of security guards. This may include shutdown and lockdown procedures to prevent anyone from breaking in and stealing sensitive materials, releasing laboratory animals or contaminating or otherwise sabotaging products in clinical trials or on the market.

Safeguarding lab animals is particularly important since they can be both expensive and difficult to replace once research is under way. Sensitive laboratory experiments should be discussed only with those employees and others who need to know about them. Publicity can draw unwanted attention from extremist groups and thieves.

Biotechnology firms must also know who is working for them. It's an unfortunate reality, but up to 75 percent of thefts suffered by a business are committed by trusted insiders. At a minimum, biotechnology companies need to do background checks on individuals during hiring. In some cases, ongoing

random screenings may be appropriate, especially if a company is dealing with hazardous materials where small quantities can harm a significant number of people or have a severe impact on the environment. Biotechnology firms must be on the alert for suspicious events and signs and symptoms of disgruntled employees.

In a biotechnology firm, protecting records, costly equipment and sensitive materials is vitally important. To help prevent the theft of proprietary R&D information and expensive equipment and supplies, companies need to establish clear security policies and measures. Access to critical information should be provided only on a need to know basis.

Duplication procedures for lab books, electronic data, samples/cell lines and cultures should be established and followed carefully. All critical records should be backed up weekly and kept in fireproof file cabinets and protected from water damage. Depending on how much data is generated, lab records should be backed up at least weekly, too.

Duplicate documents, as well as cell lines and cultures, should be stored off site. If disaster strikes, staff scientists or technicians can swiftly recreate research without significant interruption of their work.

**“To prepare for a disaster, a biotechnology firm must identify worst-case scenarios; conduct a business impact analysis that addresses all critical business functions; and formulate effective emergency preparedness and business recovery strategies.”**

The arson at the University of Minnesota construction site demonstrates how terrorism compounds ordinary risks of fire. How a biotechnology firm stores and handles flammable and combustible liquids can have a dramatic impact on fire safety and employee safety. Biotechs almost must protect

against potential contamination problems presented by chemical reagents.

The California energy crisis presented an extreme example of the types of problems biotechs can face as a result of power outages. Without alarms or a backup supply of electricity or refrigeration, weeks of research can literally melt away. For example, a series of power failures at one facility rendered frozen cells in solution useless. Even more devastating than the \$250,000 property loss was the fact that it took the firm several months to reproduce the cells.

Now more than ever, biotechnology firms also need to be aware of the potential for a computer intrusion and consider installing computer security systems to detect and respond to a cyber attack.

## AFTER A DISASTER

A well-conceived plan that contemplates all potential disasters and all appropriate responses can make the difference between never recovering from a major loss and continuing daily operations with minimal disruption. It also can reduce a firm's financial vulnerability and keep its insurance costs in check.

Geared for a quick response, the plan should address everything from communicating with the media to emergency procedures for handling lab animals and hazardous materials. It should detail how to secure a facility against further damage as well as suggest procedures to implement to help rebuild the company's physical operating environment. The plan should also include a response team composed of staff from various areas of the company and should assign specific responsibilities to each team member in the event of an emergency or disaster.

Naturally, the immediate concern in the event of a terrorist attack or other disaster is the welfare of employees and their families. Only then when they know that they and their families are safe will most employees be able to think about getting the business back in action.

Depending on the severity of the disaster, a facility may be closed for a day, a week or even a month. Making arrangements for temporary facilities is one of the most challenging—and most important—parts of the planning process.

After conducting a business impact analysis, a biotechnology firm may decide to establish a fully equipped secondary lab that is always available in case the primary location is inaccessible. For many companies, however, that level of protection may prove too costly. As an alternative, a company might maintain an updated list of potential sites where it can relocate temporarily and prearrange with suppliers for both equipment and biologic materials. This is especially important for key equipment like automated cloning machines, gas chromatographs, mass spectrometers and refrigeration equipment.

Biotechnology firms should also establish plans with suppliers of lab animals. Common animals may be kept in stock, but a company that requires specially bred rats, for examples, may need to work out in advance how long it would take a supplier to provide them. If a company's exposure is significant, it may be worth the cost to ensure the supplier maintains an inventory of the hard-to-obtain animals.

In addition to their own risks, biotechnology firms need to understand their vendors' abilities to deal with a disaster and to meet client needs under those circumstances.

The more discussions that a biotechnology firm has internally and with its suppliers, the better able it will be to evaluate the possible threats and ways to address them. Companies cannot know how they will deal with a disaster until a team, working with full support of top management, sits down and lays out the scenarios, including the time required to return productivity to the level that existed before a disaster.

Once the hard work of developing a plan is done, it cannot be considered complete unless it is tested and re-evaluated every year. After the 1993 bombing of the World Trade Center, many companies developed disaster recovery plans. Unfortunately, they didn't test them sufficiently to know that they wouldn't work under the direst circumstances.

## FINANCIAL PROTECTION

Although disaster recovery planning may help contain losses and put a company back on its feet, it does not diminish the need for a well-rounded insurance program. Examining the effectiveness of a biotechnology firm's insurance portfolio in light of its current, as well as its emerging, vulnerabilities is a critical part of the planning process. A thorough evaluation can reveal, for example, that insurance might be needed to pay for the extra expenses of reproducing research and to pay for continuing business expenses, such as salaries, when research and development (R&D) income is lost or delayed. An evaluation would also consider other insurance issues, such as a biotechnology company's requirements for property, key person, commercial general liability, product and clinical trial liability, product contamination and other types of insurance coverages.

Biotechnology firms should also consider an insurance company's financial strength and its reputation for paying claims fairly and promptly. While every company is required to have workers compensation insurance, after the event of September 11 many companies discovered that not all workers compensation coverage is the same. The terrorist attacks demonstrated that some insurance companies were able to weather the financial hit better than others; in addition the quality of service in responding to workers compensation claims of such a sensitive nature often varied greatly.

## SEEKING ADVICE

Proactive biotechnology executives can seek advice from insurance professionals who specialize in insurance and risk management solutions for life science companies to ensure that they have a well-rounded insurance program. Such specialists can help companies reduce the potential for financial ruin by helping them develop a loss prevention program and disaster recovery plan combined with an insurance plan that accurately reflects that vulnerabilities their companies face.

### ENDNOTES

- 1 Massimo Calabresi and Sally Donnelly. Cropduster Manual Discovered. Time.com. [Online] Sept. 22, 2001.
- 2 Ernst & Young. Global Information Security Survey 2002. [Online]
- 3 Ernst & Young. Biotechnology Industry Report: Focus on Fundamentals, 2001.
- 4 Douglas Steinberg. California Steamers. The Scientist, 15[13]:8, June 25, 2001.
- 5 House Resources Committee, Subcommittee on Forests and Forest Health, Statement on Ecoterrorism by James F. Jarboe, Domestic Terrorism Section Chief, Counterterrorism Division, Federal Bureau of Investigation, 107th Cong., Feb. 12, 2002.
- 6 Frankie L. Trull. Animal Rights and Violence. Speech delivered to the FBI in Chicago. [Online] Nov. 4, 1999.
- 7 University of Minnesota News Service. U' Decries Arson After Underground Organization Claims Credit. [Online] Jan. 30, 2002.
- 8 PricewaterhouseCoopers. PwC Security Benchmarking Service 2000 Now Available to Help Organizations Learn How Their Security Measures Stack Up Against Their Peers. Press Release [Online] July 12, 2000.

# IS YOUR INSURANCE AS SOPHISTICATED AS YOUR BUSINESS?

With nearly 20 years of experience in the biotech, medical device and other life science industries, Chubb has become the property/casualty insurer of choice for over 40% of the world's leading technology-focused organizations. Here's why. Our technology specialists can help you build a portfolio of property insurance products and loss prevention services to protect production, R&D facilities, lab animals and equipment, as well as various sources of funding and income. We also offer liability insurance for products and clinical trial risks to help protect your company's lifeblood – your future financial success. And, our global network of 132 offices in 33 countries ensures that we do business wherever you do business.

From cultures to catastrophes, Chubb offers a dynamic approach to your insurance needs. Talk to your independent agent or broker to learn how Chubb can help you.

*Chubb's property/casualty program is endorsed by the Biotechnology Industry Organization and the BioIndustry Association.*

**COVERAGE BEYOND YOUR EXPECTATIONS**

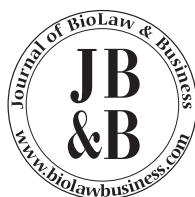


Chubb refers to the insurers of the Chubb Group of Insurance Companies. Actual coverage is subject to the language of the policies as issued. Chubb, Box 1615, Warren, NJ 07061-1615.

*For More Information*

Ronni Zimmerman  
Chubb Commercial Insurance  
Marketing/Communications  
(908) 572-4783  
rczimmerman@chubb.com

[www.chubb.com](http://www.chubb.com)



The Journal of BioLaw & Business®

Voice: 888.732.6732

Telefax: 973.627.5872

E-mail: [orders\\_biolaw@fulcoinc.com](mailto:orders_biolaw@fulcoinc.com)

Web: [www.biolawbusiness.com](http://www.biolawbusiness.com)