

The Bioterrorism Act ... Implications for Business Continuity Planning

In the wake of 9/11 and in response to concerns about a terrorist attack involving bioterrorism (defined as the threat of terrorism involving biological agents), President George W. Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

The Bioterrorism Act, as it is known, is divided into five sections and deals with many different facets of the threat of bioterrorism. This article focuses on Section 3 of the Act: Protecting Safety and Security of Food and Drug Supply. (The complete act available at www.fda.gov/oc/bioterrorism/bioact.html.)

This section of the Bioterrorism Act, completed in December 2004, is comprised of new security guidelines for the entire food and beverage production industry, including agribusiness and animal feed supply. Philip Jan Rothstein, a business continuity expert, recently commented on the guidelines, "Like pharmaceuticals, healthcare and other industries which directly affect public health and safety, the food and beverage industry is governed by legal and regulatory requirements, as well as moral and ethical obligations. In the event of a public health crisis, access to business and operational records could become critical."

The following organizations are required to comply with the Bioterrorism Act record-keeping rule:

- Food manufacturers
- Importers
- Processors
- Packers
- Trucking firms/transporters
- Distributors
- Wholesalers
- Retailers

According to the U.S. Food and Drug Administration, approximately 707,700 facilities are covered under the record-keeping rule. "Of course, protection and preservation of essential business records should be considered a due diligence priority even when no crisis is looming," counsels Rothstein.

The new rules are designed to help the government track the source of contamination in the event of a terrorist event to target the nation's food supply. Since the FDA is the government agency in charge of safeguarding our food supply from inadvertent contamination, the agency has taken on a large role in efforts to prevent, prepare for, and respond to incidents of food sabotage.

Records Protection Requirement

One of the most important elements of the Bioterrorism Act is the new FDA record protection requirements outlined in Section 306: Establishment and Maintenance of Records for Foods. The record keeping rule propels covered organizations in the food supply chain to establish and maintain easily accessible paper or digital records that "identify the immediate previous source of all food received, as well as, the immediate subsequent recipient of all food released."

All businesses covered by this rule need to be in compliance within 12 months from December 9, 2004, and the Bioterrorism Act allows FDA to pursue civil action as well as criminal action to prosecute persons who fail to establish and maintain records, as required by the final rule.

In a press release issued by the FDA in December 2004, acting FDA commissioner Dr. Lester M. Crawford explained the reason for the record keeping rule: "The ability to trace back will enable us to get to the source of contamination. The records also enable FDA to trace forward to remove adulterated food that poses a significant health threat in the food supply." In other words, if terrorists tried to sabotage the food supply, the records provided by the covered organizations will enable officials to identify first *where* in the supply chain the contamination occurred and then, if necessary, immediately remove the product from stores, warehouses, or distribution centers before too many casualties occur. In addition, officials investigating a food contamination incident would most likely not even be able to determine whether the contamination was accidental or intentional until they (using the traceable records in the food supply chain) pinpointed the source of the outbreak.

What Records Need to Be Protected?

The FDA is generally concerned only with traceability, so at issue are any records that contain the information regarding the food's origin and its destination. The following types of records, common in food industry businesses, are excluded:

- Recipes for food (as defined in the rule)
- Financial data
- Pricing data
- Personnel data
- Research data
- Sales data (other than shipment data regarding sales)

Companies can maintain the required information in any format—paper or electronic. According to the record-keeping rule, the requirements apply in varying degrees to certain categories of businesses. For human food, records must be maintained in ranges from six months to two years, depending on the item's shelf life. The maximum record-retention requirement for transporters of all types of food is one year.

One of the key aspects of Section 306 is that records must be retained at the establishment where the activities covered in the records occurred or at a reasonably accessible location. This is to ensure that when FDA has a "reasonable belief that an article of food is adulterated and presents a threat of serious adverse health consequences or death to humans or animals, any records or other information to which FDA has access must be available for inspection and copying as soon as possible, not to exceed 24 hours from time of receipt of the official request."

What You Need to Do Now

The safeguarding of vital and irreplaceable paper and digitally stored documents is absolutely crucial for compliance.

Some potential approaches for Section 306 rule compliance include: onsite fireproof vault, onsite fireproof safes and/or file cabinets, and onsite data safes and media vaults that are specially designed to secure digitally stored information, i.e., disks and tapes.

Unfortunately, standard filing equipment is believed to offer fire protection by a large majority of consumers. This thinking, attractive in today's cost-conscious environment because it "seems" cheaper, is erroneous and potentially dangerous.

The stakes are high in this environment. Were terrorists to successfully attack the nation's food supply, the cost in human life and the economic damage could be astronomical. It is imperative for covered businesses to put forth the best effort possible to comply with the Bioterrorism Act.

Most risk management experts cannot agree more. According to Tom Weems, a consultant specializing in business continuity planning, "A few years ago, we defined vital records as those records critical to the operation of a business. That has changed. In today's world, there is an ever broadening set of records that businesses must protect for compliance purposes."

Weems continues, "For some businesses involved in the food chain, protecting certain records is no longer just good business practice it is a federal requirement. Fair or not, like it or not, the requirements are real and the means of protecting those records must be real as well."

Covered businesses are now required to store these vital records onsite, ensuring that they are accessible and secured against risk such as fire or flooding. Therefore, experts advise seeking records storage products that are tested by Underwriters' Laboratory (UL) (www.ul.com) or other nationally known independent testing labs—absolutely steer clear of equipment with manufacturers' or nonindependent ratings. UL, in particular, is the best, as no other testing and standards organization matches their reputation.

One trick to be wary of is a product that claims to be "built to" a certain UL class specification claim. This is marketing-driven word play, pure and simple, and can lead the customer to believe they are getting a UL rating when in reality it may be just the manufacturer's dubious claim. If UL has never actually test a product, how it will withstand a real fire is anyone's guess.

You won't have to sacrifice aesthetics for safety today, because the top vendors in the industry offer well-designed, attractive, media-rated safes, fire-resistant file cabinets, and fire safes for onsite records protection. You can readily find this equipment at your local office products dealer, in most office products catalogs, or increasingly, on the Internet. **CI**

Van Carlisle is President and CEO of Fire King (New Albany, IN), a security and loss prevention company. Carlisle studied criminal justice at the University of Louisville and served six years in the Air National Guard Security Police Force. He can be reached at (800) 457-2424 or via e-mail at vanc@fkisecuritygroup.com.