Journal of Bioterrorism and Biodefense

Editorial Open Access

Editorial-Announcement

Editorial

Biosecurity has multiple meanings and is defined differently according to various disciplines. The original definition of biosecurity started out as a set of preventive measures designed to reduce the risk of transmission of infectious diseases in crops and livestock, quarantined pests, invasive alien species, and living modified organisms. The National Academies of Science define biosecurity as "security against the inadvertent, inappropriate, or intentional malicious or malevolent use of potentially dangerous biological agents or biotechnology, including the development, production, stockpiling, or use of biological weapons as well as outbreaks of newly emergent and epidemic disease". It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems. Biological attacks can result in destruction of crops, temporarily discomforting a small community, killing large numbers of people, or other outcomes. The way that a biological weapon is used depends on several factors. These include: the agent itself; its preparation; its durability in the environment; and route of infection. Some agents can be disbursed as an aerosol, which can be inhaled or can infect a susceptible spot on the skin, like a cut or wound. Attackers can also contaminate food or water with some agents.