Health Information Technology/ BioDefense Needs to Fight Bio-Terrorism

Tanushree Govil
Stanford University, USA

Jivesh Govil
Cisco Systems, USA

INTRODUCTION

Recent advances in biological research and biotechnology have allowed development of bio-lethal weapons intending to create deliberately detrimental consequences such as fear and mortality amongst modern organizations, governments, and society. Public awareness of growing threats of bioterrorism in the world is rapidly gaining momentum. As these concerns have been elevated and form the agenda for many international government meetings, IT has a strong opportunity to empower professionals such as clinicians, public health officials to prepare to respond rapidly and effectively to combat any form of bioterrorism.

This article aims to primarily focus on bringing technology profession to build effective strategies and analyzing solutions to detect, manage, and communicate any bioterrorism event. Further, the article explores opportunity areas and challenges in the realm of bio-surveillance across a range of information systems over the life-cycle of an event. Although various organizations and governments have made significant efforts, there is no comprehensive set of recommendations that exist yet to build such IT and Health infrastructure to combat bioterrorism. Accordingly, the article discusses fundamental criteria and strategy to build next generation IT/Decision Support System to deal with bioterrorism related technological, warfare challenges. Finally, the article provides recommendations on maturation of bio-surveillance system's capabilities since, presently, there is no uniform prevention mechanisms, global preparedness, response and recovery plans by different nations.

The evaluations and recommendations presented in this article aspire to build technology relevance for managing dire consequential national bioterrorism events. This review aims to spur a new field in IT that focus on building IT platform to establish mechanisms for identifying and prioritizing uses of IT to better support nation's ability to prepare for and respond to public health emergencies.

BACKGROUND

Several United Stated General Accounting Office (2002, 2003) publications define bioterrorism as an attack that occurs regardless whether a disease agent has been released or a hoax has been performed. The role of fear is central to a bioterrorism event: if the sole intention was to cause death, there are much easier ways to cause a mass casualty situation. It is the fear of the unknown, the invisible, and the undetectable that makes the fear of bioterrorism so potent. Since it is difficult to prove with certainty that unknown agents or toxins are not present within a specific building or area, this uncertainty adds to the cycle of fear. Lastly, the self-centric nature of humans causes most individuals to assume that they, personally, may have been exposed to the unseen agent or toxin and should expect to be presenting symptoms at any moment, often causing them to exhibit irrational behaviors.

Through emails, blogs, and wikis, triggering the spread of erroneous information. Government officials at the local, state, and Federal levels would be forced not only to quickly calm public concerns, but also to rapidly sort out truth from fiction to discern whether or not any real disease agent(s) had been released and if so, which ones. According to Bray et al. (2006), if technology is to help with bioterrorism response, it needs to not only address mitigation of civilian illnesses and deaths, but also help to manage individual

DOI: 10.4018/978-1-4666-5888-2.ch330

and societal fears springing from the real or threatened occurrence of such an event. Timely integration of data at the local, state, and Federal levels can serve as a foundation for bio-threat assessment. This foundation in turn, serves to develop a better context for action thresholds related to emergency response, public health decisions, and communications.

MAJOR CHALLENGES IN ACHIEVING A BIOSURVEILLANCE SYSYEM

US Department of Health and Human Services, Centers for Disease Control and Prevention (2010) has cited some reasons.

Firstly, responsibility for public health is shared across levels of government, professional practices, and scientific disciplines. Because of this distributed responsibility, the timely sharing of multi-sector, all-hazards information is both essential and incredibly challenging. In summary, policy or governance directive on bio surveillance is missing in most countries.

Second, efforts to build a network of complementary biosurveillance systems advance, it will be necessary to balance and prioritize new initiatives and existing programs esp. given the macroeconomic conditions. New biosurveillance initiatives will require new funding from various sources.

Third, because public health threats are often multifaceted, there is a need to integrate `various types and forms of information. This complex task includes identification of potential diseases, natural disasters, or hazardous exposures and surveillance data collection from a wide range of sources which requires flexible approaches to biosurveillance system design and operating procedures. Another key requirement will be to develop methodologies, tools, and models to systematically harvest and contextualize all sources of biosurveillance data. This broader integration necessitates interagency discussions to define the trigger points for policy decisions on countermeasure and response options, and planning exercises to incorporate all sources of biosurveillance information in those decisions.

CURRENT BIOSURVEILLANCE LANDSCAPE

1. A single comprehensive biosurveillance system is probably not possible, and many systems will be needed.

Because the type of data that are important for detecting and managing outbreaks is not the same for all causative agents. In efforts to build effective biosurveillance technologies, Toner et al. (2011) have examined various findings that describe current status in biosurveillance systems.

2. Rapid laboratory reporting or clinical case reporting are the most important means by which health departments detect outbreaks.

In general, laboratories often provide the earliest indication of potential outbreaks, as health departments often receive laboratory reports of notifiable diseases or conditions weeks before they are reported by clinicians.

3. Established public health departments have systems to answer a number of the key outbreak questions, but this takes time.

Even with better and faster information systems, only a few of these questions can be answered in real time. Even the most basic question—"How many people are already sick?"—is difficult to answer in real time. There is issue of establishing case definitions and dealing with them across jurisdictions. Even counting cases is unreliable in real time because of the difficulty in identifying mild or asymptomatic cases. Office visits are greatly underreported, and home-treated cases are nearly invisible to existing surveillance systems. Therefore, early case counts often both underestimate and overestimate the number and severity of cases, hence is misleading.

Answering question about how the epidemic will unfold, requires an outbreak investigation, which takes time and may require approaches such as the completion of serologic studies. Computer modeling can be used to predict the course of the outbreak, but it takes time, and its accuracy depends on the strength of a number of assumptions about the disease.