Chapter XIII
Pandemic Influenza, Worker Absenteeism and Impacts on Critical Infrastructures: Freight Transportation as an Illustration

Dean A. Jones
Sandia National Laboratories, USA

Linda K. Nozick
Cornell University, USA

Mark A. Turnquist
Cornell University, USA

William J. Sawaya
Texas A&M University, USA

ABSTRACT

A pandemic influenza outbreak could cause serious disruption to operations of several critical infrastructures as a result of worker absenteeism. This chapter focuses on freight transportation services, particularly rail and port operations, as an illustration of analyzing performance of critical infrastructures under reduced labor availability. It develops models to assess the likely impacts of varying levels of worker absenteeism on the capacity of these critical systems. Using current data on performance of specific rail and port facilities, we reach some conclusions about the likelihood of severe operational disruption under varying assumptions about the absentee rate. Other infrastructures that are more dependent on information technology and less labor-intensive than transportation might respond to large-scale worker absenteeism in different ways, but the general character of this analysis can be adapted for application in other infrastructures.
INTRODUCTION

Influenza viruses have presented a threat to the health of animal and human populations for centuries. Pandemics occur when a new strain of influenza virus emerges, and develops the ability to infect and be passed between humans. Because humans have little immunity to the new virus, a worldwide epidemic, or pandemic, can ensue.

In 1997, the H5N1 influenza virus emerged in chickens in Hong Kong. The virus has shown the ability to infect multiple species, including migratory birds, pigs, cats and humans (World Health Organization, 2008). While it is impossible to predict whether the H5N1 virus will lead to a pandemic, history suggests that a new influenza virus will emerge at some point and spread quickly through an unprotected human population. The impact of a pandemic is likely to be pervasive, removing essential personnel from the workplace for extended periods. This has significant ramifications for the economy, national security, and the basic functioning of society.

An area of particular concern is the potential effects of worker absenteeism on the functioning of critical infrastructures in our society. In 1997, the report of the U.S. President’s Commission on Critical Infrastructure Protection identified eight critical infrastructures, including telecommunications, electric power, oil and natural gas, banking and finance, transportation, water supply, government services and emergency services (President’s Commission on Critical Infrastructure Protection, 1997). In subsequent years, this list of critical infrastructures has been expanded and now includes a set of 17 critical infrastructures / key resources (CI/KR) identified in the National Infrastructure Protection Plan (U.S. Department of Homeland Security, 2006).

An important part of government planning for the possibility of a pandemic influenza episode is to understand the potential impacts on the functioning of critical infrastructures. This portion of the government’s role in creating a pandemic influenza response plan is part of the homeland security mission. The National Infrastructure Protection Plan lays out an integrated view of physical, cyber and human resources, with a series of iterative activities designed to enhance protection of CI/KR, as illustrated in Figure 1. The volume of which this chapter is a part is focused on cyber security, but a broad view of cyber security should include consideration of the interactions among human and cyber resources, in particular the possible effects of large-scale worker absenteeism resulting from a pandemic event.

The work described here is not focused directly on the cyber infrastructure. It focuses instead on another critical infrastructure — freight transportation. Provision of transportation services is much more labor-intensive than provision of cyber services and one might reasonably question the applicability of this analysis to cyber security concerns. We believe there are two good reasons for inclusion of the work in this volume on cyber security, apart from what we hope are interesting implications for worker absenteeism in the freight transportation sector. First, the analysis illustrates a mechanism for focusing attention on parts of a “flow through” system that may create critical bottlenecks if insufficient resources (in this case, labor) are available. The units of flow through the freight transportation network are containers and railcars, rather than information packets, but the core concepts are transferrable between transportation networks and information networks. Second, the primary focus is on delays and congestion associated with the bottlenecks. This concept of service degradation is also transferrable to information networks. Thus, rather than providing results that are directly reflective of cyber network concerns, this analysis should be viewed as an illustration of an approach that has implications for analysis of cyber systems.

Within the transportation infrastructure, we’ve chosen to focus on freight services because the demand for freight movements is unlikely to fall very much during a pandemic episode — the basic