Chapter XLIV
A Model for Emergency Response Systems

Murray E. Jennex
San Diego State University, USA

ABSTRACT

Cyber war and cyber terrorism is real and is being waged. Cyber terrorists and cyber warriors are attacking systems and succeeding in their attacks. This requires management to prepare for the worst case, the loss and destruction of critical data and systems. This chapter helps management prepare for this worst case by discussing how to design and build emergency response systems. These systems are used to respond to worst case attacks. Additionally, these systems are useful for responding to other disasters that can cause the loss of systems and data. This chapter presents research into emergency response systems and concludes with a model of what an emergency response system should consist of.

INTRODUCTION

It is clear from the 9/11 terrorist attacks, the anthrax events, the Slammer worm attack on the Internet, the London subway bombings, the 2004 Tsunami, and now Hurricane Katrina, that terrorist and cyber terrorist attacks and/or disasters (henceforth referred to generically as emergencies) are increasingly involving the necessity to coordinate activities and responses by a much broader host of organizations involving the private sector, nonprofits, and volunteer organizations. While some of these organizations are always involved in emergency response; the total span of organizations depends very much on the type of emergency, its location, and scale of impact. As a result one can not completely predict where and who are the people and units that will be gathering and supplying information as well as who will be responding and contributing resources. The most likely way this will be done effectively is by utilizing a centrally organized but fully distributed command and control center that can add functional nodes and linkages as needed and is triggered by the occurring events (Turoff, Chumer, Van

de Walle, & Yao, 2004). Additionally, while we have intrusion detection systems, IDS, for monitoring for cyber attacks, we need to become aware that these attacks also need emergency response systems that guide responders in the correct response and recovery actions and which facilitate communications between the various responding groups and managers.

The goal of this chapter is to provide a reference for managers needing to prepare, should their defenses fail and their organization is severely damaged. The chapter is primarily focused on providing a model for creating an emergency or crisis response system (henceforth referred to generically as Emergency Response System, ERS). An emergency response system is good for any emergency, be it cyber attack or natural. The chapter presents research conducted on emergency response systems and presents a model that reflects current thought for them.

EMERGENCY RESPONSE SYSTEM RESEARCH

Emergency response systems are used by organizations to assist in responding to an emergency situation. These systems support communications, data gathering and analysis, and decision-making. Emergency response systems are rarely used but when needed, must function well and without fail. Designing and building these systems requires designers to anticipate what will be needed, what resources will be available, and how conditions will differ from normal. A standard model for an ERS is from Bellardo, Karwan and Wallace (1984) and identifies the components as including a database, data analysis capability, normative models, and an interface. This model is only somewhat useful as it fails to address issues such as how the ERS fits into the overall emergency response plan, ERS infrastructure, multiple organization spanning, knowledge from past emergencies, and integrating multiple systems. Additionally, many organizations do not address the need for an ERS until an emergency happens, and then, only for a few months until something more pressing comes up (Jennex, 2003). The result is that many organizations have an ERS that may not be adequate.

Emergencies are high stress situations that require organizations to respond in a manner that is different from their normal operating procedures (Turoff, 2002). Patton and Flin (1999) discuss these stresses on emergency managers and how to reduce them. Emergency stressors, in addition to fatigue, include dealing with a complex, unpredictable and dynamic response, time pressure, and communications, dealing with the media, and operating within an integrated emergency management context. To reduce these stresses, emergency response plans should be based on operational demands, tested regularly, and have resources allocated. These plans should not be based on implicit and untested assumptions that reflect routine operational requirements and conditions as plans based on assumed capabilities are less effective than anticipated and will increase ad hoc demands on managers. Working in teams is required during emergencies and having a well trained, experienced team will reduce the impact of team dynamic stressors. Additionally, emergencies may require interagency coordination and dealing with interagency conflict and terminology increases stress. These stresses can be reduced if these agencies are integrated in their response and participants train together so that they are familiar with each other and comfortable with the integrated emergency response plan. Finally, communication systems are necessary for getting the right information to the right people, but they will not reduce stress unless participants are trained and practiced in their use. In addition to the stresses identified by Patton and Flin (1999), Bellardo et al. (1984) identify the stress of decision-making during emergency response and recommend the creation of an ERS to assist decision makers. The components of the ERS, as suggested by Bellardo et al. (1984), were previously mentioned but several researchers have looked at decision stress and address methods for decreasing this stress. Turoff (2002) expands the discussion on stressors by discussing the philosophy of the United States Office of Emergency Preparedness (OEP) (Note: The OEP was disbanded in 1973 in the same executive order that also eliminated the