Chapter 78
Protection of Critical Homeland Assets:
Using a Proactive, Adaptive Security Management Driven Process

William J. Bailey
Edith Cowan University, Australia

ABSTRACT

The protection of critical infrastructure assets is vital to every government, organisation, business and person. If the asset forms part of the vital critical infrastructure, the loss could be catastrophic and far reaching with considerable knock-on effects. To avoid such negative outcomes requires a wide range of in-built resilient security structures, plans and operating procedures. A more adaptive, proactive, comprehensive security management process needs to be embraced to: prevent, detect, deter, respond and defeat potential damaging events and incidents. Core to security planning is a full understanding of the potential consequences of worst case scenarios. Adopting a process driven model is a proactive approach and grounded upon current operational procedures used by major international companies in hostile and dangerous environments. By utilizing a clearly defined comprehensive risk management tool, a more systematic Security, Threat, Risk and Vulnerability Assessment (STRVA), process can be developed. This process uses a multi-layered intelligence gathering capabilities.

INTRODUCTION

Threats to society and the supporting infrastructure have increased exponentially. The need to ensure the protection of critical infrastructure has taken on a new dynamic as the capabilities of potential adversaries has become more sophisticated. Although the primary threat remains terrorist or criminally based, those posed from natural phenomena and catastrophic events should not be forgotten either. A more adaptive, proactive, applied approach is required to identify the source and the likelihood these potential threats actually pose. The starting point is to define what exactly needs to be protected and why.

DOI: 10.4018/978-1-5225-5481-3.ch078

An executive order made by President Clinton, EO-13010 in 1996, led to a report entitled Critical Foundations: Protecting America's Infrastructures, often called the "Marsh Report" (Marsh, 1997), provides a definition as "a network of independent, mostly privately-owned, and man-made systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services"(Lewis, 2014, p. 7). A supporting definition from the office of Infrastructure Protection identifies critical infrastructure as a:

systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any Federal, State, regional, territorial, or local jurisdiction..(Office of Infrastrcuture Protection, 2012, p. 12)

An Australian Government definition is:

those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation…(Australian Government, 2010)

Based upon these definitions, it is clear there are multiple cross-overs that need to be considered, requiring a multi-layered approach involving more than one facility, organisation, regional or national authority. Because of the complexity of systems and structures, it is necessary to have a much more integrated and comprehensive methodology to identify where weaknesses might occur, or be targeted. The potential consequences caused by a major incident need to be consistently understood and dealt with forthwith. By adopting the proposed integrated assessment process, a more proactive approach can be used to increase readiness, improve the robustness of the systems and put effective mitigation measures in place.

This chapter has been adapted from (Bailey & Doleman, 2013) and brings together a series of methods, which are currently being used by many security professionals' operationally in hostile and dangerous operations in the field. Therefore, the approach presented here is to advance this all-inclusive method as part of the process that should be used when dealing with complex multi-dimensional organisations that need to harmonise their security operations to make them more robust against attack.

Working in hostile environments requires a more comprehensive approach than most security mangers have hitherto experienced. Hence, by incorporating the hostile-based-methodology into the process, adds a broader dimension to assessing the security measures required to protect critical infrastructure. However, when so many disparate organisations are also involved, a more structured, cohesive approach is required. The goal is to improve protection by producing a more all-encompassing risk and threat identification audit process. The template presented here should provide a useful guide to putting this into place by identifying which areas need to addressed and how the process can function successfully.

Vulnerability and potential consequences are key components to the assessment process. Additional inputs such as computer generated modelling techniques, red teaming and penetration tests can assist where available. In addition a comprehensive intelligence gathering structure should underpin the whole procedure; capable of producing a formidable output that is organic and evolving, but highly useable by the security manager.