Chapter 19
Proactive Security Protection of Critical Infrastructure: A Process Driven Methodology

Bill Bailey
Edith Cowan University, Australia

Robert Doleman
Edith Cowan University, Australia

ABSTRACT

The belief that a static alarm system will safeguard critical infrastructure without additional support mechanisms is misplaced. This complacency is no longer satisfactory with the increase in worldwide threat levels and the potential social consequences. What is required is a more proactive, comprehensive security management process that adds to the ability to prevent, detect, deter, respond, and defeat potential harmful events and incidents. The model proposed here is proactive and grounded upon current operational procedures used by major companies in hostile and dangerous environments. By utilising a clearly defined comprehensive risk management tool, a more systematic security, threat, risk, and vulnerability assessment (STRVA), process can be developed. This process needs to identify deliberate targeting of assets through multiple intelligence gathering capabilities, plus defeat testing to probe existing security defences. The consequence approach to a potential breakthrough is at the essence of this methodology.

INTRODUCTION

Over the last few years the level of threat has increased substantially throughout the world. The need to ensure the protection of critical infrastructure has taken on a new dynamic as the capabilities of adversaries have become more sophisticated. The threats are not just terrorist or criminally based, but also from natural phenomena and catastrophic events. New methods and approaches are required that can assist in dealing with this increased anxiety from these threats. However, first is necessary to define what exactly needs to be protected and why.

Critical infrastructure as laid out by "The "Marsh Report" (1997- US) and the subsequent executive order EO-13010 (1998)...a network of independent, mostly privately-owned, and-made

DOI: 10.4018/978-1-4666-8473-7.ch019

systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services" (Lewis, 2006, p. 3). A piece of infrastructure is considered critical when it is vital to national security and to the country. But as Lewis points out, the Marsh Report did not define critical. However, this has evolved since 1998 and most countries have a structured definition that allows them to encompass what they consider to be part of their critical infrastructure. This approach will often include parts controlled by the government and by private industry. This is where the heart of the problem often lays as the resources required to protect are not unified and are asymmetrical in approach (Lewis, 2006, p. 3).

A more widely accepted definition is:

Critical infrastructures involve multi-dimensional, highly complex collections of technologies, processes, and people, and as such, are vulnerable to potentially catastrophic failures on many levels. Moreover, cross-infrastructure dependencies can give rise to cascading and escalating failures across multiple infrastructures (Tolone et al., 2004, p. 214).

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 or regional authority. Because of the complexity of systems and structures involved, it is necessary to have a much more integrated and comprehensive methodology to identify where weaknesses might occur or be targeted. The potential consequences that such a dislocation could cause needs to be firmly understood and dealt with accordingly. By adopting the proposed integrated assessment process, a more proactive approach can be used to increase readiness, improve the systems and put mitigation measures in place.

This chapter brings together a series of methods, which are currently being used by many security professionals' operationally in hostile and dangerous operations in the field, but have not been documented, into a single methodology. 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. Working directly in hostile environments requires a more comprehensive approach than most security mangers have hitherto experienced. Hence, by incorporating the hostile-based-methodology to the process, it adds a broader dimension to assessing the protective measures required for critical infrastructure. However, when so many disparate organisations are also involved, a more unified approach is required. The template presented here should provide a useful guide to putting this into place by identifying what areas need to addressed and how the process can operate successfully.

The goal of this chapter is to demonstrate how organisations can improve their overall protection by increasing the information that is required to produce a more comprehensive risk and threat identification audit. The audits should also include vulnerability and consequence assessments, together with additional inputs such as computer generated modelling techniques, red teaming and penetration tests. A comprehensive intelligence gathering structure should underpin the whole process capable of producing a formidable output that is organic and evolving, but highly useable.

This comprehensive model is based upon a recognised approach by security professionals operating in volatile and hostile situations where oil and gas recovery is taking place such as: Algeria, Sudan, Nigeria, Angola, Iraq and Equatorial Guinea. Experience has shown it is possible to manage potentially dangerous situations if the right approach has been taken to mitigate the risks. The Risk Assessment process being discussed consists of seven sequential sub-elements:

1. Threat,
2. Criticality,