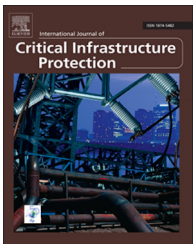
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Designing physical security for complex infrastructures

*Rick Nunes-Vaz**, *Steven Lord*

National Security Science and Technology Centre, Defence Science and Technology Organisation, PO Box 1500, Edinburgh 5111, SA, Australia

ARTICLE INFO

Article history:
Received 25 June 2013
Received in revised form
10 February 2014
Accepted 27 June 2014
Available online 2 July 2014

Keywords:
Critical infrastructure
Physical security
Security-in-depth
Design
Risk management

ABSTRACT

This paper uses security-in-depth principles to provide practical guidance for the design of physical security in complex infrastructures. Working from the central tenet of security-in-depth, that the strength of security comes from the coherence of the entire security system rather than just the technical excellence of sub-systems, a practical framework is constructed for assessing the risk reduction of an infrastructure security design proposal. In this way, alternative proposals may be evaluated for their effects on the overall security risk to a system, taking into account a broad threat and hazard space. The approach includes explicit consideration of organizational factors and management structures, ensuring that the design is consistent with enterprise objectives as well as internal and external policy and legal constraints.

1. Introduction

As the complexity and interconnectedness of physical infrastructures increase, the difficulties associated with designing effective physical security also rise, perhaps more steeply. Security [23] has always been a compromise between "locking the system down" to deny the opportunity of abuse and maintaining a viable and effective business [24]. However, designing effective, value-for-money security involves another set of trade-offs that are less well understood. These are the trade-offs between alternative security system designs based on their contributions to risk reduction. Translating strategic security objectives into wise or even agreed choices between investing in (figuratively) more cameras, more guards, higher walls or stronger doors is a challenging design problem.

We contrast this contribution from other works (e.g., [7,8,33]) that use risk to assign rankings of protection priority to multiple infrastructures in order to minimize the aggregate (expected) risk to all facilities. Our purpose here is to support the risk-based design of security for a single infrastructure assuming that, through other processes (e.g., [28]), the decision to enhance physical security against internal or external malicious attack has already been made and justified. As a result of the challenges to security design noted above and, in the absence of a useful (and simple) security risk evaluation framework, typical practice has tended to rely on three approaches that largely avoid tackling the problem directly. Each is acknowledged to be imperfect and, in some cases, has been shown to diminish the effectiveness of security [7,24].

The first approach, which we call "plugging the hole," involves retrofitting the system to manage vulnerabilities exposed by successive security incidents. This could be seen as characterizing the response of aviation security to the hijackings of the 1970s, the events of September 11, 2001, the

*Corresponding author.
E-mail address: Rick.Nunes-Vaz@dsto.defence.gov.au (R. Nunes-Vaz).

http://dx.doi.org/10.1016/j.ijcip.2014.06.003
1874-5482/

shoe-bomber in 2001, the underwear bomber in 2009, etc. The risk reduction benefit of particular security sub-systems must be assessed in relation to a plausible spectrum of potential security incidents, not just the incidents that have occurred.

The second approach, which might be termed "more is better", involves appending another "layer" to the security matrix [31]. Quite apart from the confusion in the literature about the meaning of the term "layer" (which we address below), security-in-depth analyses [20,23] have shown that it is better to have fewer layers if investment can make the layers stronger.

The third approach, which we call the "silver bullet" solution, involves investing in high performance technologies within sub-components of the security system. Security-in-depth principles [20] indicate that investment should be focused on the weakest function (e.g., detection or response) in a critical layer. If the response is weak, then investment in state-of-the-art scanning equipment to further enhance detection is not a wise investment [14].

Why are these workarounds used? Principally, it is because of the inherent complexity of the problem. We consider the challenges in terms of three types of complexity. The first type of complexity involves the breadth, diversity and adaptivity of the threats and hazards that the system may face in the future, and the fact that the effectiveness of each control depends on the particular threat and its context. The second type comes from the fact that controls have varying degrees of interdependence (e.g., CCTV, monitoring staff, movement sensors and guards are strongly interdependent), which means that assessing the risk reduction or benefit-cost of possible additional controls can be difficult. The third type of complexity arises from the need for all stakeholders, from the risk owner through the various levels of management, possibly down to the system operators, to be involved and contribute to security design deliberations [9,29]. Broad involvement and ownership is necessary because the design process must strike a balance between considerations of technical performance, usability and strategic security value.

Accepting these challenges to effective security design, this paper describes a set of structured templates that are intended to guide and facilitate security design discussions. Using the principles of security-in-depth, the process is intended to take input from and develop ownership within the broad group of stakeholders, while ensuring that the decisions remain transparent and traceable. The aim is to create a practical toolset for security practitioners involved in security system design or redesign. Using this approach, each incremental enhancement of the security solution will be justifiable on the basis of (i) its relative (value-for-money) contribution to security risk reduction and (ii) its ability to manage the risks that are identified by risk owners and stakeholders as their primary concerns.

The design process is illustrated through the development of example solutions to manage a hypothetical terrorism attack on an infrastructure site or facility. The paper shows how security solutions are progressively built by considering pathways to harmful events and how packages of controls (in "layers" defined below) are developed to change the probabilities of the events. The paper then develops other control packages to reduce the potential consequences of the events. Each stage in the design process is supported with generic, transferrable templates that are intended to help deliver a cost-effective, coherent and complete security solution.

In addition to the objective of facilitating a more effective security system design, this paper considers the less tangible aspects of security [17] that, nevertheless, underpin its effective operation. These aspects, which include system maintenance, staff training, policy development, etc., are termed enablers, and their absence or inadequacy can be just as detrimental to the delivery of effective security as the failure of security controls.

This paper is structured as follows. Section 2 provides a brief review of security-in-depth principles. Section 3 uses a hypothetical infrastructure security problem as a vehicle to generate a series of templates intended for use in security design or enhancement discussions in any complex context. Section 4 discusses security system enablers and where they fit into the overall framework. Section 5 reviews the strengths and limitations of the approach. Section 6 presents the conclusions.

2. Security-in-depth framework

Because the security-in-depth framework lies at the core of the approach, it is important to provide a brief overview of its primary tenets. Nunes-Vaz et al. [20] have proposed a hierarchy of terms to describe security-in-depth or layered security. Referring to Fig. 1, a security control, or a physical, procedural technical or other device contributes to the performance of one or more security functions, such as detection, response or decontamination. Security functions are commonly performed by several interconnected controls. A simple threat detection function might involve a guard watching for people who jump over, and therefore bypass, swipe-authorization entry gates.

Although a function such as detection might be performed perfectly, no risk reduction is achieved unless actions to manage the detected threats (e.g., entry denial) also occur. Note that risk is assumed to be a function of the consequences of a harmful event and the likelihood of the consequences eventuating. Risk is reduced by reducing the likelihood and/or consequence. For this reason the term "security layer" is reserved to represent the integrated arrangement of controls that could either stop a harmful event, or preclude its consequences (see Fig. 1). In this way, only security layers explicitly manage security risk. A poorly integrated set of security controls may fail to create layers and, therefore, fail to manage security risk.

It is argued in [20] that physical security systems should be described in terms of four layers: deter, prevent, protect and contain. These are shown together in the common "bow-tie" diagram [29] in Fig. 2. The deter and prevent layers serve to reduce the likelihood of a potentially harmful event. Deter is largely passive and relies on the attacker's perception of security, which is primarily influenced by his/her knowledge of, or assumptions about, actual security strength (as well as the severity of sanctions). Prevent is an active combination of security functions that usually include detect, alert, respond and impede. In general, each layer acts serially, that is, either an attacker is deterred and prevention plays no part (other than