7 Security Theory: Process, definitions, tools and techniques

Introduction

The widely respected Abraham Maslow's *Hierarchy of Needs* describes our basic requirement for safety and security as just above food, water, warmth, and rest. For the purposes of this chapter, safety is considered in the context of event security. In this context safety is an emotion that is affected by the trust a patron places on the signals, signs and feelings they detect when they review a place, an event, buy a ticket to an event, or attend an event. In essence, the relationship between a patron and a security provider is one of trust. Patrons attending events have an emotional investment in an event, based on both their expectation of the event itself and on their awareness of the risks of attending an event, formed via knowledge of security incidents at other venues around the world. The security profession, on the other hand, invests in the event process through planning, implementation, and application that needs to be robust and stable to fulfil patrons' trust and maximise their return on investment, and to prevent failure or any other incident that may significantly damage the event.

This chapter will explore what security does to make people feel safe and to prevent the loss of assets. It will use a systems theory approach to discuss the interrelation and interaction of the various dynamic aspects of the different parts of the security process.

What is security?

Security is the planning process that designs and creates the framework for supporting the trust placed by the public in those managing their safety at an event. It also protects the organisers of an event, and the assets invested in making that event a success. Successful security planning is considered a basic requirement for a successful event. This chapter details the application of methodology and processes to ensure an event both feels safe and is safe.

There are three key categories to consider when ensuring successful security. Decisions based on consultation and research need to be made in relation to:

- people,
- assets, and
- information.

The *people* category includes safety and security of patrons, employees, suppliers, and other stakeholders. *Assets* include infrastructure and intangibles like goodwill, brand names, and intellectual property. *Information* includes websites, databases, operational plans, and continuity and recovery plans. These elements combine to make people feel safe, to inhibit intentional malice, and to reduce petty crime and criminal behaviour.

These elements of security will be detailed in the sections of this chapter, as follows: what is security; security planning processes and methodology; emergency management; assessment of security threats; and planning inputs.

Methods to ensure security control can be broken down into the phases:

- **Preventative** — reducing the likelihood of risk, for example, Physical layering and separation using stand-off areas and barriers, closed-circuit TV (CCTV), entry searches; venue and service level lock downs and control.
- **Detective** — seeks vulnerabilities and gaps for correction, for example, audit reviews, penetration testing, information gathering, intelligence sharing with authorities; white level inspections

- **Corrective** — reducing the severity of the consequences after an incident, for example, medical first response, preparedness training and readiness with counterterrorism police and army. Rapid security deployment.

A common approach to security planning and management is to engage a security consultant or planner and then a contractor to deliver the services, so the key elements outlined above can be incorporated and independently assessed. This is likely to involve the event organisers setting security goals for the event and then auditing of delivery goals against a security plan by the consultant/contractor. As security planning needs a high level of independence, the advantage of engaging a consultant and/or contractor is that they provide outside eyes and views free from bias.

Systems

Given the dynamic nature of events and crowds, bringing security goals and actions together in a way that is holistic and integrated requires a systems approach. A system is an integrated collection of parts. Each part, although it is bounded, is interrelated to other parts. Systems theory seeks to understand this and to predict how developments and changes will affect the system as a whole.

General systems theory is about broadly applicable concepts and principles, as opposed to concepts and principles applicable to one domain of knowledge. It distinguishes dynamic or active systems from static or passive ones. Active systems are activity structures or components that interact in behaviours and processes. Passive systems are structures and components that are being processed.

Security implementation is an active system because changes made to increase security presence and security controls and response will change the other actors and agents in the event environment. This may be a positive change, for example, increasing the number of guards can make a crowd feel safer or happier. On the other hand, increasing the guards may increase the crowd hostility.

When developing security planning and methodology, a systems approach is the overarching theoretical framework on which the process relies.

Security planning processes and methodology

Consistent with the systems theory approach outlined above, a security team providing service at crowded places and events may be like a machine. Goals and objectives are defined, every job detail is specified, and all activities are planned, organised, and controlled. If there are weaknesses in this machine like structure, then adapting to changing circumstances will be difficult because it is designed to achieve predetermined goals.

A simplified model of security planning is shown in the flow chart in Figure 7.1, *Security planning process flowchart*.

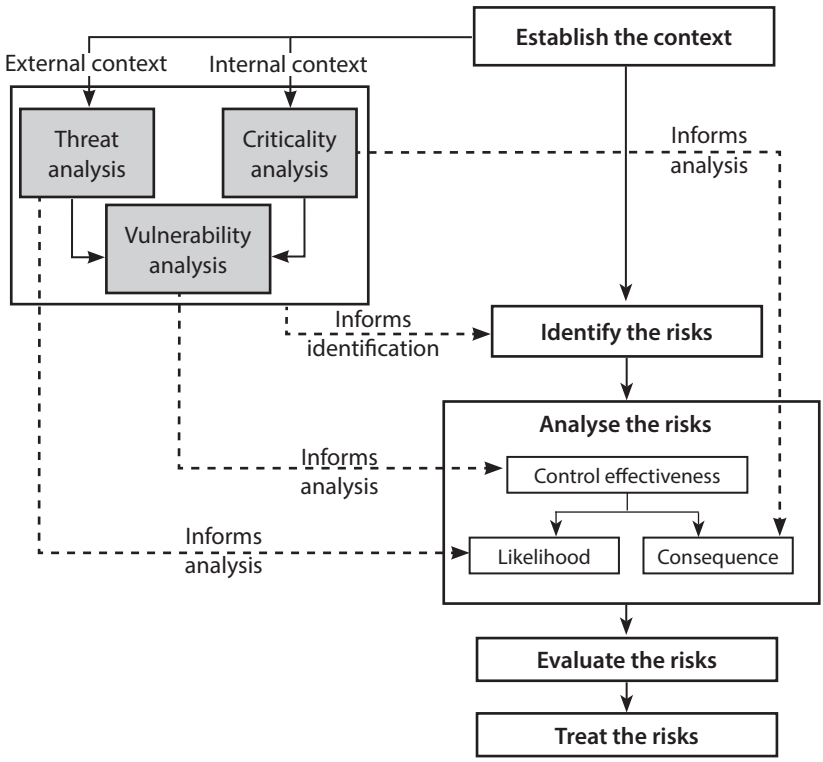

Figure 7.1: Security planning process flowchart. Source: Australia/NZ standard HB167:2006 Security risk management.

The first step is to establish the context of the security risk. Is it external or internal? From this it is possible to determine threats and vulnerabilities. Note the grey sections highlight where planning has to be robust enough to create resilience to overcome targeted and calculated attacks.