JDiBrief – Security

Scenario based risk assessment for critical infrastructures: TOPIC OVERVIEW (2 of 5)

Author: Dr Tanya Le Sage, UCL Department of Security & Crime Science

Since the turn of the millennium democratic countries have seen increased attempts by violent extremists to commit terrorist attacks. The primary targets of these attacks are often symbolic buildings (i.e. key government departments or historic landmarks) or critical infrastructure (such as transport networks or energy-grids). When successful, these attacks have a major impact on society, causing death, serious injury, damage and disruption on an unprecedented scale. To mitigate these threats to national security a variety of strategies and tactics are adopted by politicians, private sector organisations and security companies. Within the risk management environment, risk assessment is often a prerequisite step for the prevention of terrorist attacks. It is is a critical aspect of security and crime control, and forms the core of many risk management frameworks.

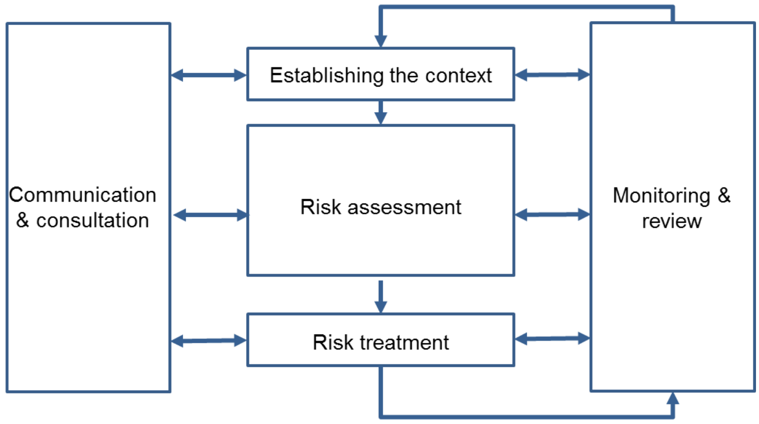

Figure 1 – a representaion of the ISO 31000 risk management framework

Probabilistic risk assessment is a practical approach for assessing the capabilities of security systems.

Security systems can take many forms – for example, CCTV networks, air ventilation systems or biometric technologies – and are designed to protect assets from being altered in an undesirable manner.

Terrorism risk assessment is usually performed by security professionals, and involves estimation of the probability and consequences of hypothetical attacks against a target. Such estimates are derived through a mix of experience and historical evidence. Risk assessments will also commonly look to anticipate future and emergent threats to security. The results of the risk assessment help formulate and implement a suitable security strategy.

In response to the heightened risks, the past decade has seen the security technology industry grow substantially. Many security products and measures are now available for the purposes of protecting critical infrastructure. Security managers have to decide between different measures (i.e. technologies or policies), often using cost-benefit analysis to substantiate their decision. Such costs and benefits are sometimes directly in conflict though (i.e. a ‘perfect’ system may be prohibitively expensive) and decisions are made with a view to finding the optimal balance between the two.

At present, one of the key issues with computer based risk models is that they often lack the ability to integrate new security measures. This means that the assessment of the effectiveness of the inclusion of new technologies is inaccurate, or at best, time consuming. The approach outlined in the subsequent page of this JDiBrief permits the impact of new technologies to be evaluated, and further allows the impact of a malfunctioning security system to be assessed.

ISSN 2050-4853