Creating a Culture of Security & Risk Awareness: A new best practice approach

Dr. Jonathan Di Rollo

Critical Infrastructure/Motivation

The motivations of attackers are numerous, diverse and hidden. Money, jealousy and religious beliefs are some of the most common motivations for attacks on critical infrastructure around the world. These motivations change in number and priority or frequency of occurrence but they are all hidden inside the psyche of the attacker. What changes an ordinary individual in to an attacker can range from financial problems to religious conversion or simply losing your job. Other people are just borne criminals.

What is important in better protecting critical infrastructure is assessing the size of possible losses, financial and emotional, and the probability of a successful attack. The size of losses can range from small amounts of money to millions of dollars but the emotional damage caused can affect people's lives, well-being, jobs and careers for generations. Assessing the risk of threats to critical infrastructure should therefore involve not just the organisation but the individual.

The size of gain to an attacker may be financial such as in the case of a cyber heist or it may be emotional such as the 911 attack on the United States. In order to better protect critical infrastructure the size of potential loss from an attack must be assessed. Assessing the size of loss can then be used as an indicator to assess the weak points of a company or national infrastructure and may yield new insights in to previously unidentified critical infrastructure. It may also identify infrastructure that is no longer critical.

The probability of a successful attack depends on many factors, in systems and in people. How well protected is the critical infrastructure? How better protected can the infrastructure be? These are key questions to ask when assessing the probability of mitigating an attack. Having in place a fully operational system that is staffed by trained, vigilant staff is a first step in reducing the probability of a successful attack. Identifying and assessing threats are the next steps. Reaching out to intelligence and assets outside of an organisation and communicating are further strategies for reducing the probability of a successful attack.

The motivations of attackers cause them to attack critical infrastructure around the world but motivations cannot be seen only their consequences through behaviour. Motivations of attackers emerge after an attack, once the damage has been done. However, how motivated an attacker will be can be used to indicate which parts of an organisation are most at risk of attack and how to better protect these critical infrastructures from attack. In a changing world the incidence and frequency of cyber attacks has increased dramatically in the last few years. This can be explained by the high probability of success of a cyber attack and the large financial gains from a successful attack.