The security industry can be like a house built on sand without professional standards in place

*Picture the scene:* You’re suffering from a persistent pain and so decide to take a trip to your doctor to get it checked out. You step into the consulting room but, before you can speak, he looks you up and down, haw and hums, and then writes out a prescription. Would you be happy that drugs prescribed in this manner will cure your ailment when your doctor has not even bothered to establish what the problem is? Would you accept this as any sort of professional approach? Of course you wouldn’t, and yet every day, in every corner of the Security Industry, this is exactly what is happening, informs Stephen D Green, Physical Security Sector Champion for the Security Institute Research Directorate Knowledge Centre.

Security Managers, faced with an immediate security problem and Directors screaming for action, over-rely on experience, leap to conclusions as to what the solution should be, reach for the catalog and start ordering. This is why, for example, all too often I will come across vehicle control points in site perimeters equipped with K12 crash-rated roadblockers, when 10 yards to each side of the entrance is a chain-link fence that my kids could punch through. The Security Managers, like the doctor above, have failed to analyze and diagnose the problem, leaving it to...
chance that the action taken will fit the need. But when the measures put in place fail, it is the Security Managers competence that is drawn into question.

All security system designs should be risk-based. Such an approach encourages analysis of evaluation of risks such that priorities may be established.

Is such criticism fair? After all, Security Managers are only human, and humans use unconscious heuristics, or shortcuts, to achieve their goals. We all have personal biases and comfort-zones ("...it's what we've always done"...), we all benchmark or crib off others ("...it's what Bill down the road does..."
"…and we all satisfice (…"it’s good enough and it’s available now’…). And it’s not as if there is a wealth of reliable, independent information out there on which to base procurement decisions; in 2007 Professor Adrian Beck of Leicester University, describing the “data desert” at the heart of the Security Industry, stated that “…if CCTV or EAS were a drug, we would be absolutely appalled at the way it has been introduced and widely used without any rigorous testing of its likely impact on the patient". I also wonder if the prevalence of second-careerist, ex-armed forces or police officers in the industry has a bearing; General Colin Powell famously once stated that “…if you have between 40 and 70% of the information required to make a decision, go with your gut”. So what can the poor beleaguered Security Manager do to improve this situation? The answer is simple; all security system designs should be risk-based. Such an approach encourages analysis of causality and evaluation of risks such that priorities may be established, leading to problem-oriented solutions which, most importantly, are justifiable before a Company Board being asked to provide funding.

An initial and comprehensive risk analysis assessment should be executed prior to purchasing products for the system.

Risk was defined in the seminal 1992 Royal Society report as “..the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge”.

There are many variants of quantified risk assessment process around the world, including the relatively-new ISO31000 standard, which developed out of the AS/NZS 4360 standard. Alternatively a good method, widely used within the petrochemical industries, is the American
Petroleum Institute Security Vulnerability process. All of these various methods share a number of common features:

**Risk Identification** – Identifying and characterizing all critical assets and the specific threats facing them

**Risk Analysis** – Identifying from the list of all possible risks those which are credible given the existing vulnerabilities, the counter-measures already in place and the capabilities of the adversary

**Risk Evaluation** – Assigning a numerical, ordinal value against each risk to allow ranking and prioritisation of effort

The level of understanding required to achieve this can only come from careful and continuous stakeholder engagement to ensure a good cross section of views and opinions; it cannot come from one person, or indeed one discipline, in isolation. The perception of risk is influenced by too many factors to describe here, but suffice to say that it is subjective, personal and experiential in nature. This is why some people read a book or walk the dog at weekends while others throw themselves out of perfectly good aeroplanes or climb up the side of mountains.
Even risk-based technical countermeasures are only of use when deployed in support of a set of good, well-thought out security policies, procedures and practices on which staff have been trained and exercised.
Risk management is inherently a group activity, and should be iterative to reflect the changing nature of threat environments. The outcome of the risk assessment process should be a document, known variously as a security treatment plan or a Concept of Operations, which outlines the way the proposed new counter-measures are intended to work. From this it should be possible to define a detailed Operational Requirement for every device, listing its intended functionality and any technical performance criteria it needs to comply to. Later, following implementation, it is these two documents that will close the circle by verifying the installation delivers that which was intended at the outset.

Of course, it must be acknowledged that getting the technical element right is only part of the solution. Security is a sociotechnical system; it is made up of technical and human elements. Even risk-based technical counter-measures are only of use when deployed in support of a set of good, well-thought out security policies, procedures and practices on which staff have been trained and exercised. Remove any of these elements and the project can only fail. Therefore, paraphrasing Mathew 7:26, the Security Industry can often be “...likened unto a foolish man, which built his house upon the sand”. If the industry wishes to present itself as professional, it needs to adopt professional standards of evidence-based and methodical design rather than the haphazard guesswork which remains all too prevalent today.


Author Profile
Stephen D Green