

## Could your security systems be leaving you vulnerable?

by Michael A Pepper MSc CPP PSP

(First published in *Security Today* - July/August 2009)

Many clients take security systems for granted. They believe they have a need for a system, whether CCTV, intruder detection or access control, and proceed to talk to commission-driven sales people masquerading as security consultants. The sales people convince the client that their particular product is the panacea for all ills. The system is duly installed and the client assured that all is working OK and of course the invoice is paid. A maintenance contract is not even a consideration as the client needs to minimise ongoing operating costs.

At some point not too far down the track, the client discovers that the system is not performing quite as expected. Worse still, the client may be blissfully unaware that the system has developed serious problems and may even have ceased to function as it should. It is then that the arguments are likely to start. The upshot is that the client is left with an unwanted vulnerability.

What has been missed in the procurement process is a System Operational Requirement. Had one been developed, the client's expectations of the system would have been satisfied and the installer would have had a clearer understanding of the client's needs. The Operational Requirement process is not new. It was originally developed by the UK Home Office Police Scientific Development Branch (PSDB) to provide police and government departments with a specific methodology for the deployment of CCTV. Previously, many such deployments were on the basis of "it seemed like a good idea at the time". The original definition of an Operational Requirement is:

*"A statement of needs based on a thorough and systematic assessment of the problems to be solved and the hoped for outcomes"*

*PSDB Operational Requirements Manual 17/94, 1994*

The Operational Requirements Manual has had a number of revisions since 1994, and the latest iteration was published in April this year by the Home Office Scientific Development Branch (HOSDB). It is an excellent reference for anyone thinking of installing any type of security system, not just CCTV. I have successfully used variations of the Operational Requirement process for other systems including access control, perimeter intruder detection and even a lone worker alert system. The outcome is a non-technical document that serves to justify the need for the system as well as provide for installation, commissioning, operation and maintenance.

I recently read an article by a colleague, Andy Hays, who is operations manager for UK company CCTV In Focus. He noted that well maintained security systems are essential, but sadly many are not. He went on to say:

*"Clients are often sold technology which is not needed to achieve their operational requirements for CCTV. Sales people, who may have limited technical knowledge of the equipment and no real understanding of the customer's true requirements state that the system will do everything that is asked of it. This inevitably creates problems*

*for the installer engineer when the client questions why the system does not perform as promised. This just highlights that fact that without an operational requirement what the client is sold is not always what they expect.*

*The end user, whether it be local government or a small corner local shop, has been often missold and misinformed about CCTV. CCTV is too often specified and installed on the basis of how it looks to a human eye instead of to a set of technical standards. This has resulted in millions of pounds of public and private money being spent on equipment that is either not needed or is not effective.”*

*Andy Hays in Info-4-Security, 26 May 2009*

Whilst Andy was talking about the vulnerability of a large utility site and specifically about CCTV, I could readily reflect that his comments could be directed to many other security systems, and not just those in the UK either. Clients in New Zealand often suffer the same fate.

The industry’s clients naturally want better security but paying for it is sometimes quite another matter. Inevitably, many will opt for the cheap and cheerful option whilst others will simply accept the sales pitch and install the latest bit of kit with all sorts of bells and whistles that are not actually needed. Of course, the extra bells and whistles are still being paid for by the client. Frequently there is little difference in performance of the system if it is poor equipment installed reasonably well or good equipment installed badly. To illustrate this, have a look at the following four CCTV images that were obtained during recent security audits. The top two images are from a cheap monochrome camera and an unbranded digital video recorder. They show the daytime and night time views. The lower two images are from a colour camera and digital video recorder, both of a widely used and reputable brand.



In each case the clients have been left with equipment that does not meet the need, which was to observe and record after-hours activity. This clearly demonstrates the lack of a System Operational Requirement. It is also clear that the cameras were set up during daylight hours with absolutely no thought as to what was going to happen after the sun went down. In both cases, the only records available were the DVR instruction manuals (both were photocopies). There were no as-built drawings, no equipment lists, no completed maintenance schedules and no information as to what each camera was supposed to see. Unfortunately, other security systems I have encountered recently have caused me not a little consternation.

During another recent audit, the client complained about the high number of false alarms from the security alarm system. A quick inspection revealed why this might well be the case. Several cables and sensors had been joined using crimp or terminal-block connections and were generally in a very untidy state. Pairs of sensors were connected to the same alarm zone in some cases. Labelling of cables inside the cabinets was frequently illegible or non-existent. In one case a faulty cabinet tamper switch was simply disconnected. Lack of maintenance was a major failing. When the installer was contacted about the extent of the false alarms by the client, the solution was to upgrade the control panel and replace several sensors. The cost to the client was several thousand dollars. Did the false alarm problem go away? Not on your life. The focus of the installer was to sell more product rather than resolve the underlying infrastructure issue. Yet again, even after the “upgrade”, there were no as-built drawings, no equipment lists and no completed maintenance schedules. A zone list was available, however it was hopelessly inaccurate.

There is no doubt that the relevant NZSA Codes of Practice would have assisted these clients, however they were unaware of their existence. Development of System Operational Requirements would have helped as well, but once again the clients were unaware. Security is not, after all, their core business. The Operational Requirement process is relatively straightforward but it involves a high level of interaction with stakeholders. This can be time-consuming, especially where the client is a large organisation. In such cases the organisation’s security manager would most likely assume responsibility for development of the Operational Requirement. Small organisations are unlikely to have an in-house security manager and might rely on an external consultant to provide such a service. An astute supplier or installer could apply the Operational Requirement process even though it focuses on the problem rather than a specific technical solution or product; however the cynic in me feels that this may be too much for some to bear.

Before procuring any security system, there is a need to be very clear about the problem that is to be addressed. Having procured, installed and commissioned your system you need to know whether it has actually dealt with the problem. If the Operational Requirement process has been properly followed, the system you have purchased is highly likely to be appropriate and will function as desired. Even if all has gone well, forgetting about the need for ongoing maintenance can turn your state of the art system into a heap of junk well before the end of life of the equipment. The Operational Requirement process flags the all-important management and maintenance issues in advance. In particular, it provides a high degree of assurance that your new security system has not solved one vulnerability and created another.