

The Security Industry Needs a Code of Ethics

by Michael A Pepper MSc CPP PSP

(First published in *New Zealand Security* - June/July 2009)

The Private Security Personnel and Private Investigators Bill is now before Parliament. At long last the security industry can hope to have governing legislation that is up to date, relevant and has some teeth. The draft Bill as it stands has some serious shortcomings, and the Government has chosen to make changes via the Select Committee process rather than withdraw the Bill and start from scratch. Submissions close on 12 June 2009 so there's not a lot of time left to get your points across.

The Bill mentions the necessities such as licensing arrangements, enforcement, training, offences and penalties. It also discusses rules of conduct including possible codes of ethics. The word "possible" worries me not a little, since provision was made in the 1974 Act but never implemented. I have written a number of articles over the last few years about professionalism in the industry from the point of view of the need for adequate training, qualifications and above all, a code of ethics. Codes of ethics do exist. The NZSA has a Code of Professional and Ethical Conduct to which all members must subscribe. ASIS International has a Code of Ethics that applies to its members. Additionally, those who hold the CPP[®], PSP[®] and PCI[®] certifications are bound by much more stringent Codes of Professional Responsibility. The NZSA and ASIS Codes are published on the respective websites. The Bill does not state that membership of a professional association is a pre-requisite for obtaining a licence. This is a requirement in some of the States and Territories in Australia. Perhaps New Zealand should adopt something similar.

I was recently questioned by an industry colleague as to whether it was fair that a client should specify membership of NZSA in tender documentation. Additionally the client only wished to receive applications from companies that were audited against the NZSA Codes of Practice. My response was simple. Obviously the client wanted an assurance that tenders would only be forthcoming from those companies that subscribed to a code of ethics and met at least a minimum standard in terms of how they operated. As far as I am concerned the client was completely correct; fairness was not an issue. Whether or not a company chooses to hold NZSA membership (or indeed membership of any other body) is currently a voluntary matter. If a company does not subscribe to the code of ethics of a recognised association, does it simply develop its own? If it does have its own code of ethics, does the company then sanction itself in event of a breach? I rather doubt it. Membership of ASIS International is only open to individual security professionals; not to companies. Just because the director of a company or some of its employees are ASIS members does not imply that the company adheres to the ASIS Code of Ethics. A company is, after all, an entity in its own right. One way to overcome this dilemma is for the legislation to incorporate a code of ethics. An alternative is to insist that companies are members of a relevant organisation that has a publicly available and enforceable code.

For several years, many in the security industry have bemoaned the fact that the cowboys were getting everyone else a bad name. The Bill goes some way to

addressing this in terms of increased penalties and better enforcement. In any event, things seem to be improving due to greater public awareness; however the industry is not out of the woods yet. Even when the legislation becomes effective, a lot of work will be needed to help industry clients recover from what both unlicensed and, yes it is unfortunately true, some licensed providers have done to them.

It is in the nature of things that the industry's clients want better security but paying for it is sometimes quite another matter. Inevitably, many will opt for the cheap and nasty 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. The bottom line here is that sometimes 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 four CCTV images below. 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 a lack of ethical conduct. It also demonstrates the lack of a System Operational Requirement, something I shall be discussing at the forthcoming NZ Security Conference on 26 June 2009.

Regrettably it does not stop there. The security industry is in a constant state of flux and acquisitions are a common feature of the landscape. When one company takes over another, all the installation records should follow thus ensuring compliance with the NZSA Code of Practice requirement of complete Client and Equipment Records. Not only do these records frequently disappear, so do the original contracts. The

acquiring company usually continues with the old arrangement sometimes leaving the client confused as to who the service provider actually is. What is worse, the client's equipment is not inspected or tested at the time of takeover. I frequently find in such cases that security systems have been poorly maintained in the past. What then of the responsibility of the acquiring company? It is easy to say, "Oh, that was before our time". It shouldn't be forgotten that one purpose of the acquisition was to increase the client base for the benefit of the acquiring company. Ethically, the acquiring company should accept the bad as well as the good and assume some responsibility for the mess the client is sometimes left in.

I have recently completed security audits on behalf of clients who have experienced the aftermath of such acquisitions. For the majority, the experience has been perfectly painless. For the not so lucky, they are looking at considerable expense to restore their security systems to a reliable state. The biggest problem has been the lack of a robust maintenance programme; followed rapidly by poor advice and continued bad practice. An example of the latter behaviours is when a client recently upgraded its alarm system not long after the takeover of the previous installer by a larger company. There was insufficient space on the alarm expander panel to accommodate a new sensor. The technician kindly offered to connect two sensors together. Of course the client accepted the offer when faced with the additional expense of a new panel, but was left in ignorance of the potential consequences. The disturbing feature of this is that the technician's company has been successfully audited against the NZSA Code of Practice for Intruder Alarm Systems. This demonstrates that not only do companies need to subscribe to a code of ethics, but they need to ensure compliance from their employees.

I could go on ad nauseam, but I think I have made my point. I do of course accept that many security companies try their utmost to demonstrate and maintain high professional standards. Nevertheless the cowboys are still among us. The industry as a whole needs an enforceable code of ethics. Unless it is specified in the new legislation that licensing is subject to membership of a recognised professional body, subscription to a code of ethics will remain voluntary. The only other way to ensure that it applies to all is to have it included in Regulations that support the new legislation. Maybe this time we'll get it.