Interview with Mike Bluestone 15 July 2003

Most security setups operate on a 10-minute delay. The castle-and-moat system. The physical barriers should be sufficient to delay intruders for 10 minutes after the first alarm goes off.

This means good quality perimeter fencing and lighting. Ideally, a double electric fence (not to electrocute intruders, but to sound an alarm when breached) with either dogs or a patrol vehicle between the two fences.

A hydraulic ramp at the access points.

Metal turnstile.

Access control: There are several kinds of biometric access control: a palm reader, fingerprint recognition, iris recognition, and retinal scan (but this last has caused a cancer scare in the US).

An infra-red beam between two posts, or two walls, will give a warning signal when someone passes through it.

There are three kinds of CCTV camera: Overt, usually with PTZ (Pan, Tilt and Zoom) which may be controlled by an operator many miles away; discreet, i.e. the dome type (you can't see where it's pointing); and covert, with the lens poking through a pinhole.

In high-security establishments, there will security cameras directly pointed at, for example, the door of the safe where the dangerous materials are kept. In addition, there must be two people there to open it, each using a different code (but you could learn someone else's code).

Warning and alarm systems can be integrated with other aspects of security; for example, when the alarm is sounded, shutters may descend automatically, or lights come on, or video recording activated.

Animals infected with dangerous viruses could be electronically tagged.

Most sites are controlled by outsourced security. MB gained entry to a supposedly secure bank site by posing as a welfare officer in the security company. With faked uniform, badge, pass, letter from head office bearing bogus phone number, and rented blue van bearing laminated "Securicor" type sign, he said he had come to ask the security guards about their welfare and pension benefits, and how satisfied they were. They admitted him to the visitors' area, but when he asked for the toilet he was allowed into the secure area, where he wandered around at will.

Fire officers wander everywhere at will, as to health and safety people. An outsourced IT engineer might gain access to the security computer, and would need only two minutes to alter the settings.

Poor screening and vetting of guards is endemic. A guard is supposed to have a ten-year employment history, with no gaps, but it's easy to cover up gaps, or steal someone's identity. (There is a British Standard for all this.)

The loiterer scenario: He gains admission to a low-security zone in the day, hides, then comes out at night. A scientist is called in to deal with a bogus emergency in the lab. The loiterer emerges from hiding and tailgates the scientist through the airlock.

Biometric readers have tamper switches, but regular swipe card readers do not. Employees don't like biometrics.

If an organisation wishes to do bag searches, this must be in the contract of employment.

Security guards' clocking system: uses a Deister Gun, a digital security clocking device, which is pressed into a socket on the wall, which then informs the computer of the date, time, location, and identity of the guard. Guards now normally patrol in pairs.

The guards have assignment instructions, which tell them what their duties are, and an incident log.

Intruder and panic alarms would normally be linked (via the central monitoring station) to the police; but could be linked simply to your own control room. Also, local police might make random visits, and come in for a chat, especially at a time of high alert. There might even be a permanent copper on the site. MB would put a high-profile vehicle with police-style markings on perimeter patrol, plus an unmarked vehicle with staff in civilian dress (ideally a man and a woman) for covert observation.

Fire drills and evacuation drills are when the site is most vulnerable.

When a laptop is stolen, so is the information on it.