Homeland security

Secondary Echelon Site Security systems…

Security breaches – whether related to information technology, access control or misappropriation of assets – are increasingly difficult to protect against. Individuals or organisations who would seek to compromise site security are becoming ever more sophisticated in their tactics and knowledge of manipulating existing systems.

Integrated security systems that allow a single point of authorisation are a significant threat to site security and must be avoided. Concentric rings of security that are discrete, each with their own checks and balances, are ever more desirable.

Although iQBio as a company provides both physical and logical security products, we will for the purposes of this article focus on one solution – Secondary Echelon Site Security using the iGuard® IP appliance.

iQBio's Concentric Ring Theory describes security zones with varying degrees of sophistication, and each have their own methods of authentication and verification of individual identity and level of access.

Perimeter security

The outer and most secure ring

This level should involve only the most robust security systems, and have multiple checks and balances including human assets, video and audio recording, man traps, visual identification, mechanical (secure key), biometric or password authentication, and be resilient enough to withstand significant weather, moisture and physical abuse.

As the single most important ring to eliminate unauthorised entry into your facility, the perimeter system should not be connected to Second Echelon or Tertiary Security Systems, as a breach of or false acceptance by the perimeter system, if it is integrated, would allow an individual executing a breach full access to your facility, data and assets.

iQBio as a company focuses exclusively on Second Echelon and Tertiary Site Security systems. These systems are within the perimeter, but do not assume that those individuals that have passed perimeter security checks are automatically authorised.

This level of security will require its own statement of user identity, authentication methodologies and physical security barriers.

The iGuard security appliance (www.iguarddirect.com), manufactured by Lucky Technology and sold by authorised distributors globally, is the premier security device for Second Echelon Site Security. The iGuard appliance is not reliant upon a connected server, desktop or additional software for operation, and can be used in networked or stand-alone modes.

Among our many customers, The United States Air Force recently deployed 80 of the iGuard IP Appliances to protect information technology closets throughout a base in the US. Each of the 80 doors had its own iGuard unit attached to a door strike system, all connected by IP.

Authorised users, contractors and visitors are granted access based upon their assigned department, level of access and duty schedule utilising contact-less Mifare® smartcards, pin codes and fingerprint biometric verification (see www.iqbio.com/fingerprint.htm).

The deployment of the iGuard security system is uncomplicated and requires little more than a cat5 or better network drop and a local power source for the iGuard and door strike. Enrolling users, configuring and managing the iGuard is simple using a networked connected PC with any operating system and web

browser. The patented iGuard web server is a direct interface to the master iGuard on the system for all maintenance, enrolment and authorisation functions.

Transaction reporting is available via ODBC Database Direct Connection, .csv or .xls (MS Excel) download.

For more information on the iGuard security system or any of our other security products, look to us on the web at www.iqbio.com or www.iqbio.co.uk.

James Childers
Executive Director, Intelligent Biometrics, Ltd
CEO, Artemis Solutions Group USA

Artemis Solutions Group USA
PO Box 403
Freeland WA 98249
USA

Tel: +1 360 331 1071

jim@iqbio.net
www.iqbio.com