

# Integrating Technology, People and Procedures



Batsheva Genut Iluz, Vice President of Business Development at the Sdema Group, discussed effective security solutions at GDSF China.

SUBMITTED BY THE SDEMA GROUP

The security market continues to grow, marked by the emergence of new trends. One of the major trends has been from systems integrators, offering security seekers comprehensive solutions that integrate diverse technologies. Despite this emphasis, technology is not a stand-alone solution. This article will address a different kind of integration, maximizing the value of the technology used by optimizing its integration with people and procedures.

The interaction between the three components of homeland security — technology, people and procedures — determines the success of the security solutions employed to protect organizations' people, property, and assets. The key to integration of these three factors is engaging in a security planning process based on advanced threat assessment and risk analysis. Put shortly, before implementing a solution, users need to be able to identify with great precision their problems.

## AVIATION

In the wake of Sept. 11, pressure emerged in the aviation industry to develop technologies to safeguard air travel. The U.S. Department of Homeland Security spent US\$692 million in 2006 on developing explosives detection devices. There are indeed many new technologies. The question is, are they providing solutions to actual threats?

Most of the increased security at airports is aimed at keeping harmful people and materials off of planes — a direct response to Sept. 11. But anyone can enter an airport terminal with a weapon and open fire in a concentrated area, like a check-in counter.

It can be argued that surges in increased airport security follow attempted attacks, rather than anticipate future threats. Passengers take off shoes at airports around the world because of the failed shoe bomber Richard Ried.

Following the U.K. explosives plot, travelers throw away half-full water bottles at the security check areas.

Rather than direct the industry's energy to employing tactical solutions to yesterday's threats, the emphasis should be shifted to developing and implementing holistic security strategies. They should be based on an advanced model of threat assessment and analysis that anticipate threats.

The industry is indeed increasingly talking about threats, risks and vulnerabilities. But serious planning means considering each of these not as general concepts, but as specific events, clearly determined and defined.

## EVALUATING THREATS

The Sdema Group, an Israel-based homeland security solutions partnership, specializes in security

### RETHINKING SECURITY

Consider a corporate headquarters seeking to implement new protection measures against car bombs. The plan is to replace all existing windows with a stronger material. What if, by computer simulation, the company learned that altering the vehicle access location to the building by several meters could eliminate the possibility of a building collapse from car bombs? Altering the external entrance area to the building is significantly more cost-effective than replacing all exterior glass.



Consider that an airport, by computer simulation, could locate the precise points along take-off and landing routes that a MANPAD missile could hit an aircraft? A cost-effective solution could be as easy as altering the flight path.

planning and project management for governments and businesses worldwide. Sdema employs a methodology of operational planning developed by a founder, Shlomo Harnoy. This methodology is used to protect dignitaries and facilities in Israel, and serves as the foundation of all Sdema security plans.

The result of implementing this methodology is simple, but unfortunately absent in the security solutions that protect many organizations. Each security component put into place — from advanced technological systems to a camera; from a security screener to a manager and all procedures — confront a specific, relevant threat. This type of planning maximizes every security dollar.

This methodology of operational planning yields a map of specific threats — broken down into adversary modus operandi and potential attack scenarios. It also accounts for the scope of each threat and tests each attack scenario. Based on this map, circles of protection combining human elements, technology and procedures are crafted to protect against all threats.

To determine relevant threats, security planners must confront shifting threats in global terrorism and consider location-specific issues. The following parameters are key:

- Past experience
- Intelligence
- Estimation of adversary capabilities
- Estimation of weapons' capability and behavior
- Likelihood

After the relevant threats are defined, risk analysis tests each potential attack scenario, determining the scope of each threat. How many kilograms of explosives can an adversary conceal? From what range can an antitank missile successfully hit an aircraft? Through computer simulations and other means that pinpoint ranges of damage, security can be adjusted for the scope of each threat and the range of damage. This process maximizes protection and reduces client cost.

## EFFECTIVE SOLUTIONS

It is after defining the scope of each threat that protection options are crafted. At least two circles of protection are set against each potential attack scenario, assuming that one can or will fail. Where threats are most complex, three, four or even five circles of protection can be put in place.

This is where technology plays a significant role, but one no less significant than human resources and procedures. Consider a surveillance system for a control room, with more than 100 screens and two security agents manning that control room. Imagining that the two agents can do the impossible and monitor all of the screens, are they trained to recognize potential attack scenarios? And if they do identify scenarios, do they know what the next step is?

Several technology vendors recognize the significance of integration between the technical solutions that they develop, system users and the organizational security procedures, which act as the glue between technologies and the people who operate them.

Nice Systems, for one, is expanding the industry conversation from a dialogue about features to one about how features contribute to overall security “architecture.” They are forging this shift on two tracks — firstly, with products that pave the way for tight integration. Nice Systems' video surveillance applications support not only video content analytics enabling detection of predefined events (such as potential attack scenarios), but also unique applications that aid in real-time decision making during situation management. Features include to-do lists and pop-ups, which assist individuals in executing organizational procedures. Secondly, by partnering with the Sdema Group, Nice increases the relevance of its technologies, ensuring every dollar spent confronts a threat.

As the security industry continues to mature, an increasing number of security seekers are taking a figurative “step back” to examine the relevance and effectiveness of the systems that protect them. The market is replete with organizations that have implemented solutions, without considering in any consequential way the contours of their specific problem. The services of security planners like the Sdema Group take an organization to where it needs to be to confront the real and relevant threats facing it. **AS**

## GDSF JAPAN

GDSF will also take place in Tokyo, Japan!

- **Date:** Oct. 22, 2008
- **Theme:** IP and Intelligent Surveillance on the Go
- **Scale** 12 seminar sessions
- **Contact** Veronica Chen, [veronica@asmag.jp](mailto:veronica@asmag.jp)
- **Organizer** A&S Japan Co. Ltd.