



## **Security Industry Trends**

*The Impact of Information Technology on New Security Strategies*

The most important trend in security today is convergence. Convergence includes the merging of physical and computer security departments, as well as increasing involvement of IT vendors, departments and personnel in the manufacture, purchase and operation of security equipment. Next-generation equipment and software combine the monitoring and management of physical and computer security.

Similarly, another goal of convergence is to have employees use only one employee ID to access the premises and equipment. Approximately 39% of businesses worldwide are considering integration of access control and security systems for their premises, according to Access Control Technologies and Market Forecast World Over (2007), Sept. 2005, published by RNCOS. Another important element of convergence is the use of open IT standards to develop comprehensive security systems.

The end results of these actions are standardized technology platforms that enable enterprises to eliminate redundant systems, technologies and data. This enables security/IT personnel to solve problems once and take common approaches to threats, be they physical or logical. Convergence also results in the creation of clear responsibilities for handling security threats and promotes close cooperation amongst all IT and physical security professionals working together.

While convergence helps to streamline security systems, processes and procedures, the tasks at hand for ensuring security continue to grow in complexity and expense. Fortunately, IT staffs that have been watching over non-physical IT/IP-based assets for many years can manage new IT/IP-based security systems. As convergence unfolds, security and IT staff can team together to perform activities such as identity management, investigations, and infrastructure. The enterprise enjoys the cost savings this provides.

In addition to meeting their own security needs, converged systems enable companies to meet security requirements being shaped by the world's political climate and legislation such as HIPAA, GLBA and Sarbanes-Oxley. Top executives and boards of directors are under great pressure to maintain a secure workplace and ensure that their companies are meeting legislative demands.



### **Evolution of the Securest**

Until convergence has become completely IT-centric, security will be held in balance between the IT department, the security department and the facilities department. Legacy security systems, which are traditionally homed to a field panel and power supply, are connected by miles of proprietary wiring to physical access points (PAPs) such as doors. These set-ups are being replaced by IP-based Identity Management Software systems which connect to IP-based cameras, gateways and intercoms at the PAPs.

Driving the security evolution in the U.S. is a presidential directive handed down in 2004. The goals of the Federal Information Processing Standards Publication 201 (FIPS 201) and the accompanying Personal Identity Verification (PIV) card directive are to standardize the procedure for vetting and issuing ID cards for all government employees and contractors and providing them with standardized smart card credentials for computer and building access. In addition to standardizing the ID cards and their issue, the use of PIV cards will collapse a myriad of separate systems into a single system in a 10-year time period. This enormous undertaking requires assistance from security providers that have solid knowledge of smart cards, network security and identity management.

While the success of legacy security systems of the past hinged primarily on a supplier's ability to provide excellent wiring skills and capability, success with next-generation systems requires an IT knowledge set. Today, access hardware is a commodity and software is the key to success. Seeing the value and growth that the booming security market affords them, traditional IT software suppliers are moving into the market.

### **Trends in Selling**

Because it touches so many areas of an enterprise -- Operations, Legal, Finance, HR, Security, IT, Facilities-- selling security is a complex sell for integrators. Successful integrators bring to the table solid IT and network knowledge, complex C-level sales skills and experience. First and foremost, the integrator's sales team must convince the potential customer that they, and their company, really "know" networks and integration. And they must be able to provide the references and certifications to back up that claim.



Customers are looking for the integrator to provide them with the all-around and detailed knowledge they do not have in-house to achieve convergence. The integrator must demonstrate knowledge of security technology such as camera placement and door hardware, and have a thorough understanding of the hardware and software products he or she is presenting in the sales pitch.

The sales team also must understand the IT products with which the security system will work, such as databases, ID management systems, reporting engines, etc. Also essential is excellent pre- and post-sale support and the ability to develop a working relationship with both IT and security personnel that helps facilitate the effective and uniform management of single or multiple locations.

### **Going Forward**

Security systems revenue is forecast to grow at a rate of 10.8% per year through 2008. This growth and investment trend is fueled by a continuing pressure on cost reduction and ROI.

There is growing demand for integrators and suppliers that understand IT and security issues with equal clarity that also can provide worldwide installation and service capability. Finally, successful integrators are able to sell best of breed solutions and treat the members of the IT and security departments they work with, with equal respect and help them implement systems and procedures that make their facilities and companies more secure.

### **Fun Facts**

The Department of Homeland Security has budgeted US \$115 billion for the next five years for security for aviation, ports, ground transport, bio-terrorism and law-enforcement.

- *Department of Homeland Security*

Sales of network cameras and video servers are soaring and are expected jump from \$800 million in 2007 to \$1.2 billion by 2010

- *Frost & Sullivan, JP Freeman, IMS Research and IDC*

Market sales for hardware and software security systems will surge to US \$3.8 billion this year.

- *Access Control Technologies and Market Forecast World Over (2007), Sept. 2005, published by RNCOS*

*Note: Information contained in this article is derived from the Phare Consulting Presentation given at the TAC GSC06 conference.*