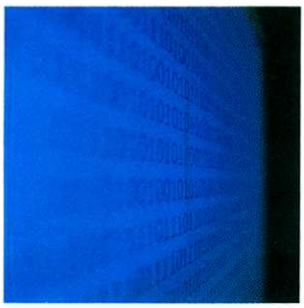

"Now, because of the IT influence, we see global platforms linked through IT systems."
— Yvonne Hao, Honeywell Security

If there is an "it" topic among security industry participants these days, it would have to be IT. The convergence of traditional security systems with the IT network has given rise to a host of issues from how this will work and who has control to what the impact will be on integrators' business and manufacturers' products.

Of course, the debate over how best to work with the IT department isn't limited to the security sector. A recent survey from Deloitte Consulting LLP and IDG Research Services showed only 10 percent of companies say their enterprises have been "extremely successful" at aligning IT and business efforts. Yet, 96 percent of them predicted a "significant" or "moderate" positive impact if IT spending were planned and measured against corporate priorities.

The ineffective communications between the business side and the IT side represented a significant or moderate challenge for 65 percent of respondents.

So if security personnel are having a difficult time finding common ground with the IT department, as the Deloitte/IDG research shows, they aren't alone.

"It's a strange evolutionary process," says Frank LaPlante, vice president-marketing for NetBotz. Calling IT and physical security "two separate islands," LaPlante says the move toward digital, IP-based systems has driven the migration of security onto the existing IT infrastructure.

While the needs of corporations differ based on the organization's size and nature of its operations, there is little doubt that the economies of consolidating the security functions onto an enterprise network has been a major driver of that migration.

For global technology firm Cisco Systems, putting the security system on the network was the company's "only logical decision" in order for comprehensive security management at Cisco locations around the globe, said Bill Jacobs, Cisco's manager-security, technology and systems. "Our goal was to have one centralized security database of information, linked and synchronized to the human resources database so that security administration was minimized and information was current," he said.

Smaller player Deere & Co., which has run its access control system for 55 different locations on the corporate network since 1997, also sees the economies of scale and cost-savings in using one infrastructure for many different systems. To operate without a server at each location would require a minimum of five people on site, according to Wes Eller, manager-security systems division, Deere & Company.

The real buzz, according to Carey Boethel, vice president, electronic security systems division-NetVersant Solutions, is total "operational convergence between physical and cyber security controls." For example, if a person doesn't use their access control card to enter the building, and they use their password to try to log onto their computer, the system sends up a red flag because the person logging on may not be the appropriate user.

Taken a step further, true convergence is the melding of security functions within an organization, using the tools of security in other applications. For example, video surveillance systems used by Club Car, a division of Ingersoll-Rand that manufactures golf, utility and transportation vehicles, are also being used so that potential buyers of Club Car's used vehicles can view vehicles at remote sites.

"We are just looking at technology within organizations and how it can help businesses. It's convergence for efficiency."
— Jim Scott

"We are just looking at technology within organizations and how it can help businesses," said Jim Scott, president of IR Security and Safety Solutions. "It's convergence for efficiency."

But marrying two applications or departments for efficiency doesn't always breed cooperation, particularly given the sensitive nature of security information.

"The co-dependence is starting to be there and its making

links between transactions on the physical side and the IT side," Boethel said. "Now you have two disparate groups seeing the value of working together, although it's not there yet. There are a lot of territory battles."

TURF JOUSTING

A large part of the debate has been over who owns, or runs, the network. At Cisco, a compromise of sorts occurred when the company migrated its access control functions onto the corporate network. Early on, Jacobs said, he had ownership and management responsibilities of all the servers, but the company "transferred the responsibility of management of the hardware (infrastructure) and the operating system/virus protection to IT. I own the application and the relationship with the manufacturer of updates and future business enhancements."

To hear some say it, the most common result of this tug of war is IT personnel often taking the lead as the two sides begin to work together, said Eli Gorovici, chief executive officer of DVTel. "It's on the network, so the IT people take charge," he explains.

Yet Gorovici says businesses need to bring security into the organization, such as into a multi-source intelligent management system, he says, rather than viewing it as a separate function.

"We must remember that the operation of physical security protection systems demands very high reliability, security and trust relative to commercial-grade IT systems."
— Arpad Toth

Arpad Toth, senior technologist with IT integrator GTSI, agreed. But Toth, who is also chairman of InteGuard Physical Security Alliance, a group of physical and IT companies that have teamed up to provide physical security solutions, also cautioned about the high-maintenance nature of the two disparate disciplines.

"We must remember that the operation of physical security protection systems demands very high reliability, security and trust relative to commercial-grade IT systems," Toth said. "Integration of hardware and software resources will happen mostly at the backend of the IT and security systems, for example, matrix switcher, data storage, trunk and feeder lines, servers, switchers, routers."

BANDWIDTH AS A BARRIER

Different parts of the infrastructure will provide different barriers to marrying the two discplines, but one of the major issues between security and IT include bandwidth, said Peter Strom, chief operating officer, March Networks. Security is now transmitting over a mission-critical network; and security of the network itself, which is exposed to more viruses and attacks as more information goes up onto it, he said.

That high bandwidth usage by physical security systems, such as for surveillance, will initially limit their place on the network, according to Glenn Hirsh, enterprise architect, with GTSI. "I believe you will see simple integration of systems such as magnetic badges or common access cards into network systems for tighter security and, as organizations become more aware of the possibility of integrating physical and network security, the scope will then grow."

FOLLOW THE LEADER

Many in the industry say they believe security needs to be an active, vital participant as the two departments come together. And maybe even take the lead role.

Rudy Prokupets, chief technology officer and vice president-research and development at Lenel Systems International, agrees there is no separation between physical and logical security any longer. "People live in both spaces," he says, "you have convergence and can use it (the network) for whatever you need."

But the question remains: who in an organization is leading the charge for this consolidated approach?

"Security helps IT people do it (run the network) securely," said Reg Foulkes, chief technical officer, CSC's Global Security Solutions, which is becoming more important as companies need to comply with the information security measures laid down in Sarbanes-Oxley Act and other regulations. But other rules, such as privacy laws, in one country may be in direct conflict with information access laws in another, such as Canada's privacy law versus the U.S. Patriot Act.

"It impacts how we engineer and do convergence on the IT network," Foulkes explains.

Perhaps the most important facet in the fight over control over a network infrastructure is where corporate management grants the purchasing power, a decision that affects not only the end user but also the vendor community of integrators and product suppliers looking to tailor their offering to today's new customer base.

The end user used to be the security department, "but now we're seeing more influence from the IT director," said Yvonne Hao, vice president-global marketing for Honeywell Security, which also affects on what level decisions are made. "Now, because of the IT influence, we see global platforms linked through IT systems," she said.

The best customers, said IR's Jim Scott, have been a team that is grounded in the security department but also has input from finance, IT and human resources.

Alan Lipton, chief technology officer and director-research and development at ObjectVideo, agrees the IT decision-makers are gaining ground when it comes to purchasing power within the security space. "It's a different class of buyer," Lipton says, going from security's traditional one-stop shopping view to IT people "who want different components and plug-and-play—the best of all worlds."

But to properly tailor a new offering, vendors need

Continued on page 15

CONVERGENCE

Continued from page 6

to explore where the customer is coming from. According to Jim Coleman, president, Operational Security Systems, the two sides differ on their approach: Security places the higher premium on value, while "IT lives in a world where reliability is important," Coleman said.

They also differ on what they bring to the table. IT has insight into database management, WAN and LAN, "but they don't have stunning insights into security. If you allow them (IT) to dominate decisions, they may not be good decisions from a security standpoint," he said.

On the integrator side, Coleman said he sees that role as a bridge between the security director, who may or may not have an understanding of networking, and the IT department. As integrators, "when you jump into that (IT) domain, you have to know networks and all the buzzwords," he said.

Ray Shilling of Canon USA's NVS Group, video division, said just as security integrators are learning networking skills, "IT firms are also entering the marketplace by hiring security industry experts to expand into new business areas."

Hammering out funding for consolidated corporate security functions can be a significant barrier to implementing such a unified approach, said John Kronick, managing director of the North American Security Practice for GE IT Solutions.

"One of the biggest deterrents to rolling out security over the enterprise network is the hidden cost of the security solution," Kronick said, and who foots the bill hasn't been clearly articulated.

But other technical barriers still remain, said Stephen Pineau, president and chief executive officer, Viscount Communications.

With access control, "the biggest barrier to true convergence between IT and physical security is the Weigand standard that requires controllers," Pineau said. "The future will be in addressable and network readers." ❖