AREA DEVELOPMENT
SITE AND FACILITY PLANNING
ONLINE

Security: The Big Picture

New technology is valuable, but facility planning and operations execs should remember - it's not all about the gadgets.

Cynthia Scanlon (April/May 06)

The security industry is more visible, more technical, more sophisticated, and more confusing than ever before. With a proliferation of companies, products, and services, it's hard to know how to evaluate an organization's needs or where to turn for help - and with good reason. According to the Security Industry Association, whose members are primarily physical security manufacturers, the total number of U.S. security companies was 29,590 in 1980. By 2000, that number had more than tripled to 92,270. The private security industry, including law enforcement, has quadrupled in the past 20 years to $147 billion. Even the U.S. federal government is a player, spending $4.3 billion on IT security in 2003, a number that is expected to grow to $5.9 billion by 2008, according to Sana Security.

So what role does security technology play in site selection and management today, and what do site selectors need to know? For starters, while facility security will almost always include good locks and roving security officers, the security facility industry has added advanced information technology with a futuristic flair, specifically through biometrics. The science of studying the physical characteristics of someone's finger or hand print, eye structure, or voice pattern, biometrics is usually implemented at higher levels of security, according to Tim Callan, group product marketing manager for VeriSign. For instance, VeriSign, which provides security against identity theft, phishing, and online fraud, uses biometrics to access some departments within its own organization. "We require a biometric screening to get into our Tier 3 level," says Callan. "Everyone [entering the area] has to go through a door, through a hand scan, and through another door. That is something our practices folks have determined is necessary for our level of security need."

But, according to Mark Peterson, director of iTD (intelligent technology design) resources for HID Corporation, "It takes special knowledge to operate a biometric. Fingerprints can be difficult to enroll and people can have physical characteristics that make use of some biometrics difficult." Callan agrees. "The trouble with biometrics," he says, "is they are expensive and difficult to implement, and they are not as reliable." Thus, many companies either forgo biometrics completely or use them in a multifactored authentication with two of the biggest trends in IT security today - digital certificates and smart cards.

"While technology that reads retinas or a thumbprint sounds cool, it requires physical hardware and people to read the outputs, so it can be expensive," says Jerald Murphy, vice president and service director for the Robert Frances Group. "A digital certificate is much more flexible, more reliable, and less expensive." A digital certificate is an attachment to an electronic message that verifies the sender is who he or she claims to be. The recipient is able to decode the digital certificate attached to an electronic message, verify the sender's authenticity, and send an encrypted reply. In other words, digital certificate technology verifies that both sender and receiver are who they say they are, and more and more companies are employing the technology. To illustrate the importance of this security technology, and the fear that companies feel toward cyberterrorism, consider this: the MSBlaster computer virus caused $2 billion in damage in just eight days, and the MyDoom computer virus caused $4 billion in damages.

Smart cards are also another line of security defense. Most of us are familiar with the smart card, the plastic card issued by a company to give us access to buildings and departments by swiping the card through a reader. What makes today's smart cards so powerful is the advanced technology in applications and flexibility. "We were limited by space in the old technology," says HID's Peterson. "Today, they actually exchange passwords back and forth, so the data is more secure in a smart card environment."

Now more solutions are available, such as access into a facility, access to copy machines, cashless vending, time and attendance counts, and production control to regulate machinery. "So now the card you use for access control, which is a security component, also becomes valuable in the operation of the organization," says Peterson. "It could be a source of revenue, making things more streamlined and easier to track." What's more, according to Peterson, the cost to implement smart cards throughout an organization has dropped. Companies using smart cards now have the same deployment, but with higher security and higher flexibility of formats, for virtually the same price.

This multifactored authentication, whether it is a combination of biometrics, digital certificates, smart cards, or other security measures, seems to be the best security practice. A multifactored authentication might include swiping a smart card, punching in a number on a pin pad, and then having a machine read a hand or thumbprint - "so I have to have something I carry, something I know, and something I am," says Peterson.

All of which brings us to convergence. With multiple security access points and multiple technologies in play, electronic and physical security operators are finding their environments merging. "People who have IT networks are asking, `Why can't we just incorporate all of our security into the same company-wide network?'" says Jennifer Hart Ackermann, director of marketing for the Security Industry Association. "But it takes some doing because they are disparate systems."

As might be expected, convergence has created logistical and security issues for security personnel, facility managers, relocation specialists, and IT executives. "When telephone networks and data networks are separate, and either one is compromised, rarely would it cause the compromise of the other," says Murphy. "But when we converge things and they go across the same network, and that network gets compromised, everything is exposed."

Convergence is now requiring a balance between the security personnel who want to shut down access and other company executives who want to provide seamless access to business processes. "Companies want to open more interfaces to give [employees and customers] places to interact, conduct business, and potentially make money - which is, of course, a security manager's nightmare," says Murphy. He suggests that companies ask, What is the business benefit to opening this point of exposure compared to the risk? And how much is it going to cost to mitigate that risk? "Frankly, a lot of companies have said the risk is too great," he says.

Cost is also playing a role in today's converging security environment. "If everything can be on one network, and one is half of two, it ought to be cheaper to put things on one network as opposed to two," says Murphy. "But if you already have two, it costs you money to make two into one. Just because I can technically do something doesn't mean it makes business sense to do so."

Energy is another factor to be considered by those who are siting or relocating businesses, particularly where security is concerned. "People have assumed that utility is ubiquitously available," says Murphy. "While the performance of the [computer] chip has increased, its power consumption has increased at that same geometric rate. So 10 years ago the power requirement was low enough that people didn't have to think about it. Each chip took a watt; each rack of computers took 10 watts. Now you have individual chips that are consuming 170 watts per chip." He adds that the power requirements for a data center have gone up by an order of magnitude in three years - 100,000 watts today becomes a megawatt in three years, then becomes 10 megawatts in another three years.

For siting specialists, this can pose particular concern. According to Murphy, companies today may locate their main headquarters in one state, but locate or relocate their data or other IT center in another. "What companies are realizing is their backup center may need to be outside the geographic footprint of a natural disaster," he says. "So companies have gone from putting those 60 miles away to putting them 400 miles away." The problem with this is the varying power

100 miles away." The problem with this is the varying power infrastructures across the country. "It's one thing to tell the utility in New Jersey that you need 20 megawatts of power," says Murphy. "But now I'm going to go to Nashville and say I need 20 megawatts of power, and their utility grid is not necessarily designed to handle huge power requirements by big company data centers. Companies have to make more conservative estimates of what the power consumption is going to be, and that has to be an integral part when making the site selection because more and more companies are going to start to hit this as a problem."

Understandably, keeping all of these physical and electronic security measures running smoothly, and in conjunction with one another, may now require employing a "security guru" or chief security officer, who, according to Murphy, is looking across different IT disciplines and focusing on an overarching security policy. "The security officer usually establishes the policies and procedures and then passes them to IT, which then puts the appropriate technology on the servers, checking for compliance," he says. Peterson adds, "If you're moving a company to a new facility in Colorado, and [the people in charge] have to get that facility ready to do business and start generating revenue, who has the time to check security? They are not security professionals, they don't know how to evaluate new products, and they don't know the salient issues of new products and technologies because they don't live in that world."

Another complication is the perceived conflict over who may own security in a company, according to Peterson. "Just because we have convergence doesn't mean IT has taken over physical security," he says. "IT's role has not changed and security's role has not changed. They just need to work together now, when they never had to in the past. And a good security consultant can bridge any gaps in defining roles." Most agree that a good security consultant should have a background in data and communications infrastructure. "IT people aren't necessarily good security people and there are security people out there that don't have the right IT background," says Peterson. "You have to have the balance of a security professional and an IT technical professional."

The combination of physical security with IT security, state-of-the-art technology, and highly skilled personnel is now more important than ever. Cybertheft and terrorism are on the rise and not going away anytime soon. "There is a well-connected cybercriminal community that shares information very readily with each other," says VeriSign's Callan. "Security has to keep getting better because the bad guys are going to keep getting better. They find a new threat, and then we block that threat, and then they find a new threat, and then we have to block that threat. It's a continuing, constant battle."