

SECURITY DIRECTOR NEWS

THE BUSINESS NEWSPAPER FOR SECURITY DIRECTORS

www.securitydirectornews.com

marketwatch:enterprise FEBRUARY 2006 • SECURITY DIRECTOR NEWS

19

Standardization a key term with enterprise-wide systems

More organizations are looking for a level of commonality in technologies they install at multiple office locations

By JOANNE FRIEDRICH

As more and more companies seek a level of commonality in security systems, such as an enterprise-wide access control system, they are also employing new levels of standardization.

Companies have always needed to establish at least baseline policies as part of good governance, noted Jim Brooks, senior vice president at Control Risks. Within those minimum standards for physical protection, access control and the like, companies can then establish local variances that take into account specific threat conditions for each site, he explained.

Brooks said security policies and procedures should be based on local needs and regulations, which require programs "to be descriptive in each category but prescriptive at a local level."

TRENDS IN MOTION

In terms of the technology itself, Brooks said the continuing trend toward integration and networking has led the way toward standardization of an enterprise's security system.

That's easier to accomplish, noted Chris Grniet, vice president at Kroll Schiff & Associates, when a company owns its locations. Tenant situations, he said, may be harder to standardize because they need to consider both their own systems and those already employed by the building owner.

John Imhoff, director-office of firm security for Ernst & Young, said his company is a tenant in all of the buildings it occupies and has experienced varying degrees of security in different locations.

As Ernst & Young moves toward enterprise architecture for access control, Imhoff said it begins by seeking good, secure locations then employing a card-based access control plan that interfaces with the vast majority of existing building systems.

What that does, said Imhoff, is provide a convenience factor for employees, which also means more of them will want to use the security system, rather than seek ways around it.

Imhoff said he is about halfway through implementing the enterprise-wide access control system, which operates on the company's IT infrastructure and is linked to the human resources database. The card system will also provide the company with data on real estate usage, so it can get more accurate figures on which locations are being used by whom and how often.

SYSTEM IMPLEMENTATION

Rolling out a system, as Imhoff is doing, is typical of most companies' approach to enterprise access control, noted Jay Vaitkus, product and market manager for Stanley Security Solutions. "Corporations have employees everywhere. It's difficult to do it all at once," he said.

Vaitkus said there exists a couple of enterprise level software platforms on which companies can base their access control systems. After that, he said, their next big decision is the credential. "They not only ask about the card technology but how to future-proof the system," he said.

In an ideal world, noted Greg Pearson, chief operating officer at The Steele Foundation, companies will employ a single platform for security, making it easier to install and maintain. This is true whether the company operates just within North America, he said, or has a global enterprise.



Chris Grniet

Being able to monitor international locations remotely and use a single access card for travel to company sites anywhere in the world provides both cost and time benefits, noted Pearson.

"Globalization is forcing corporations to think beyond North America," said Pearson. "More companies are moving to enterprise systems. It's too difficult to manage risk without it."

GLOBAL OUTLOOK

Getting started on a global platform means determining a company's needs and goals. John Sullivan, director-worldwide security and corporate flight operations for Texas Instruments, said he began to establish an enterprise-wide access control system by benchmarking what three or four other companies were doing and then developing specifications for TI's system.

The planning process began six or seven years ago, said Sullivan, with implementation now at 95 percent.

As is common in the case of introducing an enterprise-wide program, Sullivan said he had to make his business case to the chief executive officer. The system, he said, offered TI economies of scale as well as standardization for access to sites

in 36 countries.

Karl Perman, manager-corporate security and emergency preparedness for Southern California Edison, said his technical systems division within the security department also formulated a strategy for security within the company and then "marketed and sold that to our superiors."

ACROSS THE ENTERPRISE

The standardized approach taken by Southern California Edison includes creating a list of equipment and making decisions based on ASIS and EEI standards, as well as peer review and consultation.

In addition to standardizing equipment, there is the need to set common policies and procedures.

"At the corporate level, we have a security manual that the whole company is managed on," noted Perman. The information is updated electronically and in writing. In addition to applying the policy internally, Perman said vendors must also sign on to Southern California Edison's security policies and procedures.

Sullivan said he has been "deliberately basic and generic" on policies and procedures, requiring everyone to have a badge and be background checked. Then, he said, each location as needed can ratchet up their requirements but not go below the basic security policy.

Grniet of Kroll Schiff agreed that policies and procedures should take into consideration local conditions.

For example, he said, a company may

have a policy that each individual have a visual ID for the corporation. But in the case of a tenant situation, there may be an exception that allows those employees to carry two forms of ID so they can access the building's system as well.

Exceptions may also be needed when using CCTV or even access control, said Grniet. In a small office, he said, the company may prefer to use a burglar alarm system rather than access control. "It depends on the risk, the size of the operation and what are its situations geographically," he said.

WHO'S ON BOARD?

Personnel is also an issue when looking at standardization for enterprise solutions. "Depending on the industry, I'm an advocate of leveraging people whose primary role isn't security," said Brooks. Whatever the scenario, it's important to have training, said Brooks, both informal through regional working groups that can discuss common issues and share best practices, and formal training via webcasts, conference calls or on-site audits.

Fortunately, said Pearson, enterprise systems are now easier to manage remotely, so the need for manpower decreases. "A lot of times," he said, "we find real estate, human resources, plant managers or facilities may have responsibility for monitoring security, and they do so remotely through their laptops."

Still, said Pearson, best practices would dictate that the company have someone charged with security at each location.

Imhoff said within his organization, each office has a location manager "who wears the security hat." These people are responsible for handling local alarms, which are also brought to the attention of a national manager. **SDN**



Jim Brooks