Integration:
The Future of
Commercial Office
Building Security

Providing security in commercial offices involves

more than the best choice of products and features.

Learn how security systems such as access control,

intrusion detection, and digital video surveillance

can be integrated into a building automation system

to protect people, property, and data.

t.a.c
by Schneider Electric

Table of Contents

I. Executive Summary

Owners of commercial office buildings today face security issues that concern owners and occupants alike. Whether a property is owner-occupied or tenant-occupied, providing the best security to ensure the safety of people and protection of intellectual and physical property is essential.

Employee theft, property crime and information security are major concerns today. Companies invest millions of dollars in security technology with the intention of increasing security, protecting people, and solving security issues. This technology includes burglar alarms, fire protection systems, video surveillance, access control systems, and intrusion detection devices. Technology, in the hands of competent and capable security officers, can reduce property liability, cut material losses, and keep people safe. But keeping security staff trained on separate, stand-alone systems can be challenging, and must be addressed as part of broader security objectives.

The key systems of security are intrusion detection, access control, and video surveillance. If each of these systems is purchased separately, administration and training can burden a company or property owner. Intrusion alarms occur on one system, access badges are administered in a stand-alone database, and intelligent digital video technology runs on dedicated computer equipment. Each system requires service, maintenance, administration, and training.

By integrating these separate security systems under a flexible building automation system (BAS), building owners realize a lower upfront investment for a considerably more powerful security solution. Installation and training occur on a single system. Operational costs like administration and maintenance are also reduced. Component devices are used in multiple ways to trigger lighting, video capture, pan-tilt-zoom, higher video resolution or frame rate, door locks, and other aspects of building control. A single system enables greater flexibility to add security components that can be easily integrated into the overall system, keeping the cost of capital expenditures low, and requiring little additional training.

An independent study by Strategic ICT Consulting of a 145,000 square foot office building shows a system installation cost saving of 24% for an integrated BAS versus separate systems. And after installation, operations and life-cycle savings continue. Project analysis by Teng & Associates shows that training is reduced 33%, IT administration is reduced 82%, and the cost for changes, upgrades, and additions to an integrated system are reduced by 32%. These operational figures are based on experience and measurement, and clearly demonstrate the value of an integrated BAS.

Finally, this paper will show several examples where TAC has effectively applied building automation products and related services to provide effective integrated security for its customers.

II. Security Concerns Today

Employee theft, property crime and information security are the major security concerns of large U. S. companies, according to a survey reported by the American Society of Industrial Security (ASIS). Burglary and vandalism ranked high as additional concerns (see Figure 1). For owners of commercial office properties, these findings translate to two priorities: keeping occupants safe and protecting buildings and contents.

The importance of security can also be measured by the amount of money major companies have committed to it. The ASIS survey determined that respondents on average spent more than $1 million on security in 2004. Companies are spending this money on a variety of technology and equipment to increase safety and protect property. Computer and network security equipment lead the list, representing nearly 40 percent of all security purchases. An estimated one out of four surveyed companies also said they had purchased burglar alarms, fire protection systems, digital video recorder (DVR) surveillance and video cameras. Security lighting, access control, sensors and detectors, and badging/ID card printers were commonly purchased items as well.

But are these investments the best way to increase security? These separate systems each address a different security need, and require training and familiarity to be most effective. A system that integrates the functions of many security devices into a single system significantly reduces capital expenditures and lowers facility operating costs because component devices are used in multiple ways and security officers can be trained on one system rather than many. Through integration, the whole security system becomes greater than the sum of its separate parts.
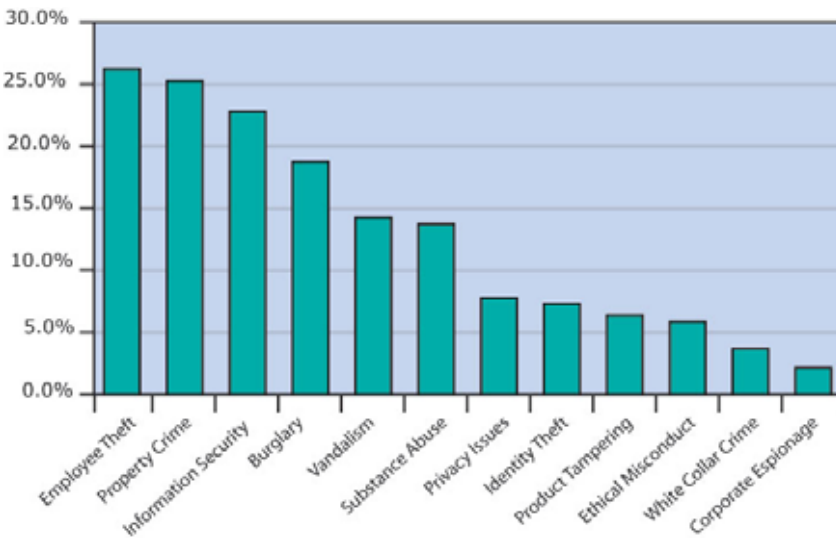

FIGURE 1
ASIS Survey of Top Security Concerns at Commercial Offices

INTEGRATION: THE FUTURE OF COMMERCIAL OFFICE BUILDING SECURITY

PROTECTING COMPANY PROPERTY AND INFORMATION

Protecting data on computers and networks is a growing and expensive issue. In another ASIS survey of both Fortune 1,000 corporations and small and mid-sized companies belonging to the U.S. Chamber of Commerce, 40 percent of respondents reported incidents of known or suspected losses of proprietary information. The study suggests these losses amount to as much as $59 billion

> *An ASIS study of corporations suggests that losses of proprietary information cost companies $59 billion annually.*

annually. Companies also reported that former employees and on-site contractors were among the greatest risk factors for proprietary information and intellectual property losses, almost equal to the threat from foreign and domestic competitors. The most commonly lost information pertained to customer data, strategic plans, financial data and research and development.

Loss of information and intellectual property are not the only security concerns at commercial property. Violent crime near office buildings or in parking lots is also troubling. Year 2006 crime statistics from the FBI show the highest increase in the U.S. murder rate in major cities since 1991. In addition, news reports continue to focus on other critical concerns like large losses of personal data by both government entities and companies as well as the threat of additional terrorist attacks. In this environment, security will remain an important concern for building owners, operators and tenants. Manufacturers, mindful of these growing concerns will continue to offer an array of solutions, ranging from simple locks to complex biometric systems. Technological advances will also provide commercial office building owners and managers with even more innovative products to keep buildings and occupants safe. Increasingly, new security products are offering integration with other building systems as an important benefit. In fact, integration brings many advantages to building owners who understand that coordinating various security measures makes sense.
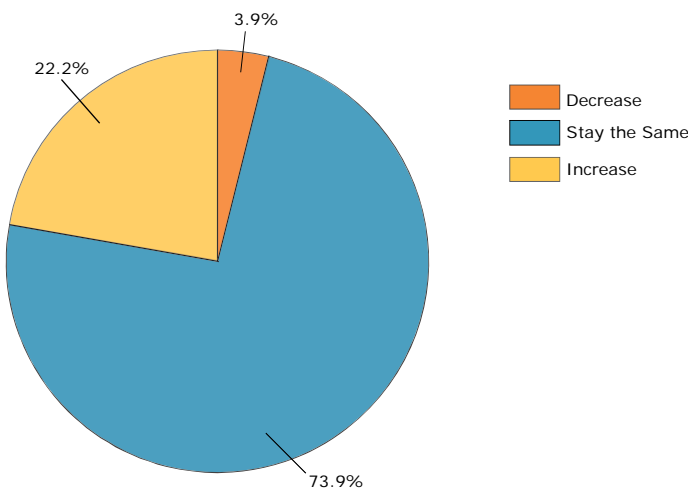

FIGURE 2
ASIS Survey of 2005-2006 Budgets for Security

Like all building investments, purchasing additional security systems must be justified and bring return-on-investment (either by loss prevention, premium rental income, or increased tenant retention). Seventy four percent of building owners surveyed by ASIS said they anticipate maintaining security expenditures at the present level in 2006 (see Figure 2). Hence, while security is important to commercial property owners, only about 22% of owners are increasing their spending. Purchasing a system with the most flexibility for integration lets management easily add components to increase security. Integration helps take full advantage of previously deployed sensors, cameras, and other devices. As a result, higher security can be achieved with the same budget year after year. Integration is the key enabler.

III. Moving Beyond Basic Security Technology

Regardless of the size of the office building or office park, its location or the level of security risks that need to be addressed, there are essential components of an electronic security system. These include **intrusion detection, access control,** and **video surveillance**. These three systems, in the hands of competent and capable security staff, apply technology effectively to reduce crime and protect people and property. We will examine each system individually, and then in combinations to demonstrate how integrating security into the building automation system leverages these systems in multiple ways, increasing security and reducing operating and training costs.

INTRUSION DETECTION

Simple intrusion detection is probably the most familiar concept of security to most people. Intrusion detection involves the use of door or window contacts, glass contacts, or motion sensors, in combination with some type of audible alarm that sounds when a person has forced entry into a building or room. An alert is sent to the police or security station to notify authorities of the time and location of the incident. Security officers respond in person to evaluate the situation.

This method of incident response can be adequate for detecting an event and quickly getting to the scene. But the effectiveness of the response at the scene and subsequent prosecution is dependent on several things; the proximity of security personnel to the incident; whether witnesses were present; the number of people involved; the seriousness of the incident, and other factors. Furthermore, with simple intrusion detection, there is little in place that would deter people from committing a crime the first place.

More information would be helpful, such as captured details of the situation that could lead to proper response and identification of perpetrators, thereby reducing the likelihood that a similar incident would occur again. Door and window contacts, motion sensors, and other devices already in use for alarming can be put to better use to help gather this information by triggering other parts of the security system.

ACCESS CONTROL

Access control is the means by which people are granted or denied access to restricted areas, such as office suites, storage facilities, or parking garages. Office buildings can either house individual tenants and companies in a multi-use property, or be owned and occupied by a single company. Varying degrees of access are required depending on use, and administration of access control for personnel can be distributed amongst several individuals.

With different needs for owner-occupied and tenant-occupied buildings, how does management begin to evaluate the various types of access control systems that are available? Furthermore, in a growing and changing office environment, what is the best kind of access control to meet future needs?

A flexible form of access control uses cards with magnetic card readers, proximity readers, barcodes, or smart cards with embedded microprocessors. Card access control at many large office buildings is common today, and there are a variety of systems with different levels of sophistication. There are many advantages to card access control. Employees can be coded with access to specific areas depending on their need, company affiliation, or any number of factors. Individual privileges can expire on a given date if desired. And in areas where tighter security is required such as labs or IT rooms, management can install keypads, keypad/card combinations, or biometric devices that can scan fingerprints or handprints.

When used as a stand-alone system, card readers and other electronic access devices offer a cost-effective and flexible way for owners of office buildings to control who has access to the various areas, with the system recording who has gone where, and when. The sequence of operations is for the access device to trigger the door lock, entry is granted, and the event is recorded by the central system. But if a device can trigger the lock, why not use this inherent ability to trigger other security devices as well? As a stand-alone system, access control does its job, but does not fully leverage the connected sensors for broader security objectives.

VIDEO SURVEILLANCE TECHNOLOGIES

Video surveillance has evolved significantly in the last decade. Older video systems needed banks of video tape for continuous recording, and required manual administration to swap tapes periodically during the day. Record keeping was prone to errors and finding specific incidents on tape was time-consuming. **Digital Video Recorders (DVRs)** made significant advances in features and functions, taking advantage of fast computer processors and high density storage media to digitize, compress and record video from analog cameras. Newer cameras today have embedded processors that enable video to be compressed within the device and transmitted real-time over IP networks to **Network Video Recorders (NVRs)** that centrally manage video feeds from many IP cameras.

DVRs and NVRs have many advantages over older analog recording technology. Streaming video can be continuously recorded and discarded in cycles of days, weeks, or months if no security incidents occur. If an incident does occur, disk indexing and time-stamping make it simple to find video from a given date and time. In addition, because the video is digitized, it can be exported and distributed via email or backed up on CD, DVD, or other digital media using common computer backup programs that are widely available.

Digital video surveillance is cost-effective and sold by many vendors in a highly price-competitive market. If purchased as a separate system to meet the needs of a security plan or upgrade, a DVR or NVR may be adequate for immediate surveillance objectives. But if this digital video recorder is integrated with an organization's access control and intrusion detection system (as part of the broader building automation system), the user improves surveillance and reduces the need for additional security personnel.

Integrated with access control, video verification, for example, allows a user to see live video as well as the cardholder's picture when a given access card is presented at a reader. The security staff can verify that the person presenting the badge is the actual cardholder. Another example of video verification effectiveness occurs in identifying individuals who are "tailgating," or when one person swipes their badge and gains access to the facility and another person follows them in without presenting their badge. The integrated system allows organizations to visually identify, verify and capture security breaches at access points.

VIDEO ANALYTICS HELP SPOT INCIDENTS

The advent of **video analytics** brings additional flexibility and increased productivity of security staff that monitor many cameras. Video analytics is a technology applied in software that examines the video camera's field of view for patterns of movement that match real-life events, such as falling, fence climbing, lurking, and trip-lines. Video analytics provides a means by which the user can focus only on what is truly important, managing surveillance by exception events rather than all events.

A DVR or NVR can be configured to only display a camera's video if a specific event or alarm occurs. At an office for example, foot traffic on a sidewalk near a back entrance may be deemed normal, and not trip an alarm according to video analytics assessment. However, stepping off the sidewalk and crossing left-to-right across the field of view to a window or restricted-access door may trigger an alarm. Additional alarms can be escalated if video analytics detect loitering near the window, or someone climbing a fence.

Video analytics software tracks people or objects, and can alarm on types of behavior

These are examples of how expanded use of video surveillance technology can increase security at office buildings without requiring an increase in security personnel.

INTEGRATING INTRUSION DETECTION, ACCESS CONTROL, AND VIDEO SURVEILLANCE

Today's access control and video surveillance systems can work together in an integrated BAS to provide a holistic solution at commercial office buildings. Keeping intruders away from property, limiting access to facilities that house expensive equipment, and remotely monitoring secluded areas to reduce the risk of crime. This is why more and more offices now rely on CCTV as part of their overall security solution. Using an integrated system, security staff at a central monitoring station can view live images from surveillance cameras, control pan-tilt-zoom cameras, or search for video clips stored on digital video recorders (DVRs). When an alarm is triggered by another part of the BAS, it can command the DVR to begin recording, display live video from a linked camera at the location, map the alarm location, and send an e-mail to an administrator all at the same moment.

CCTV cameras are an important security component at office buildings, in hallways and parking areas. With an integrated approach, when an employee contacts security, lights and surveillance cameras can be activated to monitor the scene to observe the emergency, and officers can pinpoint where to intervene to thwart an attack.

IV. Benefits of Integration

For owners of commercial office properties and the companies and tenants that work in these buildings, integrating the security system with the BAS offers numerous advantages. Foremost, integration provides for reduced installation and operating costs because it eliminates component redundancy and allows customers to streamline operations. Furthermore, it reduces training and empowers system operators by allowing them to perform their duties more efficiently. Enhanced safety, security and comfort for building occupants can also have a direct and positive impact on work efficiency. Such integration supports the goals of building owners and their tenants to be more productive, profitable and agile.

Benefits of Integrating the Security System with the BAS

- ✓ A site-wide single-seat interface enables one person to be trained on multiple security systems.

- ✓ Security components become multi-use. For example, a motion sensor can be used for lighting control during occupied hours, and intrusion detection during unoccupied hours.

- ✓ During design, flexibility, efficiency, and economy provide room for additional security expansion or integration at the lowest cost.

- ✓ Better and more flexible response to occupant needs, offering tenants greater security and peace of mind.

- ✓ More information put to effective use, which gives property owners solid ground to stand on for prosecution and proof of loss. CCTV records also aid law enforcement authorities in finding criminals.

- ✓ Vendor independence, allowing the customer to choose among best-of-class security products.

- ✓ Single-source responsibility, whereby one integrator is held accountable for all the components of the security system.

INTEGRATED SECURITY AND LIGHTING CONTROL

By way of example, consider the benefits of simply installing a lighting control system versus integrating it with security. In an office building, the lighting controls will enable the operator to maintain comfortable lighting levels and use preset schedules to control on/off periods. This ensures the lights are only on when and where they are needed, saving energy and related maintenance costs. If, however, there is a security breach late at night, without integration, personnel will need to locate switches or issue commands to the control system to switch on lights in the affected area. If the lighting controls are integrated, the scenario after the security breach is much different. The lights are automatically switched on in the area where the security breach is reported, and cameras are activated to record movements of the intruder. The operator has a single console to assess the situation and to ensure the appropriate reaction from building security or police.

With an integrated security and BAS, it is possible for building operators to control entire facilities from one workstation via a networked computer. From this single browser interface, operators can manage diverse building functions, such as environmental control, access control, video surveillance and alarm and

event monitoring. Building staff can view live or recorded video, open or lock a door, grant access to service technicians for emergency situations and handle visitor management. These tasks can be accomplished onsite or remotely at any time, whether during business hours, at nights or on weekends.

<div>

Integration Improves the Bottom Line

In an independent case study involving a 145,313 square-foot office building with 1,500 occupants, a research team examined the installation costs of the components of a *non*-integrated BAS versus that of an integrated BAS.

Systems integrated:

    Lighting Controls
    Building Controls
    Security
    Fire and Life Safety
    Metering and Monitoring
    Structured Cabling

$2,464,693   *non*-integrated BAS
$1,868,166   integrated BAS
$596,527   difference = savings

As the results show, the cost-savings were significant – **over 24 percent**. Findings also show that an integrated approach offers a broad range of commercial and technical benefits, including a single vendor point of contact, efficient project management, easier equipment deployment and investment protection for future upgrades.

Source: Strategic ICT Consulting, April 2005

</div>

CONVERGENCE: THE FUTURE IS HERE

Changes in how and where companies do business, along with rapid technological advances, are driving innovations in the security and BAS industries that are beginning to impact commercial office buildings as well. These forces of change are moving in the direction of integration and convergence of technology, including BAS, security systems and IT networks.

Important trends driving change are the convergence of the enterprise network and the building's IT network. This is created by the need to share corporate information, such as human resource facility data, with the security staff and other groups within an organization. In addition, owners of multiple commercial properties want to interconnect facilities spread over different geographical locations to access real-time data over the Internet. This information can be used for remote monitoring, facility management, analysis and control.

Using one, integrated system reduces overall hardware and software requirements, including the number of workstations needed on the operator's desktop. It also causes fewer training issues, lowers training costs, and reduces the number of staff required to effectively and efficiently manage many buildings. All of these benefits ultimately result in an increased return-on-investment for a building's owner.

V. Examples of TAC Customer Solutions

TAC provides comprehensive, effective, and innovative building automation solutions for thousands of commercial office owners worldwide. Below are some examples of TAC's security solutions, and the benefits gained by the property owner.

The Principal Financial Group

The Principal Financial Group, a diversified family of financial service companies, chose TAC to provide security for its corporate headquarters in Des Moines, Iowa, and the 6,800 employees who work there. The company required a user-friendly, flexible, multi-function system that could seamlessly interface with other security products.

Solution

A TAC partner installed an integrated security system at the corporate complex, which contains close to 2 million square feet of office space and includes six separate buildings connected by a LAN network. A six-workstation security system controls 274 doors with card readers and it monitors 135 other doors, some in the complex and others at several remote sites connected over a WAN. In addition, the system interfaces to the company's 185-camera CCTV system. TAC created a corporate command center that serves as the hub for all security control and houses two central workstations, a file server, and a badging center.

Gains

Currently, the system stores data records for approximately 19,000 cardholders and bridges onto the company's mainframe network. The Principal Group's human resource department can automatically download data to its database, such as new hires, terminated employees and other relevant personnel information, eliminating tedious and redundant manual data entry by busy security personnel.

Rockefeller Center

Situated in the heart of Manhattan, Rockefeller Center is one of the world's most famous landmarks, and was also one of New York City's first high-rise commercial sites to replace its security system after the September 11 tragedy. The building's management team turned to TAC to provide an integrated security solution.

Solution

TAC installed a system to control access for hundreds of entry points spread throughout 10 midtown Manhattan buildings that host more than 200,000 occupants and visitors each day. A high-speed fiber optic network links the system between buildings to provide both local and centralized control. Using newly installed turnstiles, along with picture ID proximity cards, barcode temporary badges, and video image verification, Rockefeller Center now tightly controls access at all times to its elevators, tenant floors and stairwells. The TAC solution records more than 15,000 cardholder transactions per day, as well as thousands of other system events.

Gains

TAC's integrated solution also provides the extra safety features the owners of Rockefeller Center demanded, improving overall security operations at the building.

INTEGRATION: THE FUTURE OF COMMERCIAL OFFICE BUILDING SECURITY

VI. Conclusion

A well engineered and maintained building automation system provides a solid return on investment over many years and delivers the highest level of security. The best security in commercial office buildings involves more than just good choices of alarm systems, cameras, and other security devices. A security system integrated into a flexible and scalable building automation system allows the building owner to use multiple security systems at once, expand applications of security for least cost, and protect the security system capital investment from becoming obsolete in the near future.

An integrated building automation system should not be confused with separate security systems that have been linked together by interfacing various manufacturers. An integrated BAS helps the building owner adapt to changing uses of the building and also enables additional control applications linked to security that involve HVAC, lighting, elevator control, and other systems in the building.

Choose the best security components from multiple manufacturers, and have an integrated BAS solution provider like TAC design them into a cost-effective security application to meet your current and foreseeable plans for the property. The best plan for maximum security is a blending of physical security, policies and procedures, as well as technology to obtain a safe and secure environment.

TAC is a leading expert in integrated building security systems, with customers in 75 countries and more than 500 offices around the world. As a company of Schneider-Electric, TAC brings the resources of a $14 billion parent company with 92,000 employees to help meet the requirements of any power, control or security need. To learn more about how TAC can help you ensure the security of people and property in the commercial office market, visit www.tac.com or call 1-866-TAC-INFO.

t.a.c
by Schneider Electric