network centric Security

June 2008

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

THE SMART, SECURE BUILDING

Planners seek to tie security systems to building automation

20

June 2008 Supplement to *Security Products*

network centric Security
WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

Content

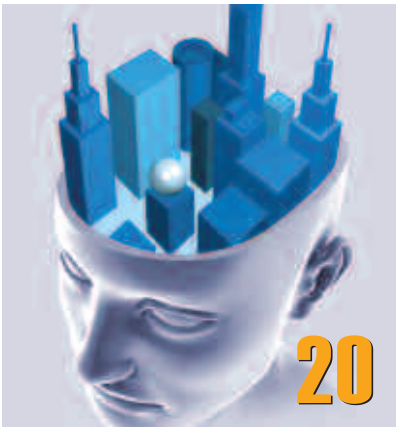
JUNE 2008 VOLUME 2 NO. 3

features

HEALTHCARE DATA SECURITY IN NEED OF CARE

By Sharon J. Watson

Convergence is largely an untested treatment as CSOs, CIOs and privacy officers often work in vacuums.



THE SMART, SECURE BUILDING

By John W. Verity

Planners seek to tie security systems to building automation.

CLEANING UP MONTEBELLO

By Steven Titch

Wireless video surveillance erases a graffiti problem

departments

Network-Centric Security welcomes vendor information and briefings. To arrange a briefing, please contact our editor, **Steven Titch,** via email at **titch@experteditorial.net.** Our agreement to accept or review product material or backgrounders is not a guarantee of publication.

Compliance For Its Own Sake

by Steven Titch, Editor

Here in the Lone Star State, public schools require students to take the annual Texas Assessment of Knowledge and Skills (TAKS) exam. The state uses the TAKS results to rate individual schools and to determine the state funding and support they'll get.

Some educators and parents criticize the TAKS exam, saying it encourages schools to "teach to the test," structuring classroom curriculum to ensure a high TAKS grade, while sacrificing instruction that would prepare students for the critical and analytical thinking needed for success in high school and college.

Similarly, when it comes to security, many enterprises have tended to structure their policies as if compliance were the sole end, while failing to address true security vulnerabilities. Like the TAKS situation, in some ways that's only natural. Individuals and organizations will act in a way that secures them the greatest award. Because compliance is necessitated by the force of law, that's where the incentive is and that's where the metrics will matter.

But compliance policies do not necessarily achieve larger security goals. Nowhere does this seem truer than in healthcare. In an industry overburdened with volumes of confusing and contradictory privacy regulations, hospitals and physicians often focus on meeting regulatory requirements rather than creating actual security.

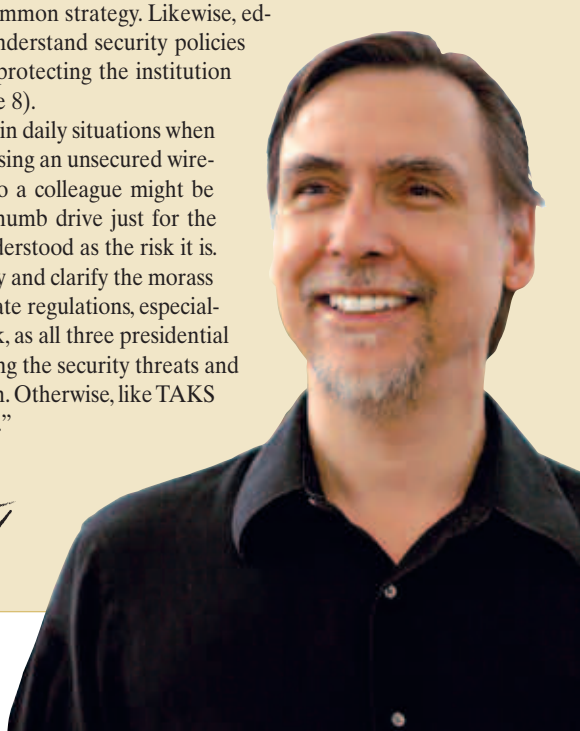
As Sharon Watson reports in "Healthcare Data Security in Need of Care" (page 16), when a patient is flatlining, and a physician needs access to a locked PC, policies and protocols about not sharing passwords become bureaucratic interference.

Yet, in defense of the undervalued CSO, surveys such as the 2008 HIMSS Analytics Report, "Security of Patient Data," find that most healthcare professionals do not comprehend their potential liability and associated costs if a third party were to access personal patient data with criminal intent.

Changing these attitudes will take a lot of work. Wiser healthcare organizations have attempted to bring together their CSOs, CIOs and privacy officers to forge a common strategy. Likewise, education is critical to helping employees in all industries understand security policies are not simply someone's "busy work," but are aimed at protecting the institution and its customers (see "Compliance Without Revolt," page 8).

That at least provides employees a framework to consult in daily situations when they must decide whether it is justifiable to ignore policy. Using an unsecured wireless connection in a life-or-death situation to relay data to a colleague might be necessary. Copying thousands of patient records onto a thumb drive just for the convenience of catching up on work at home would be understood as the risk it is.

Still, work must be done at the legislative level to simplify and clarify the morass of rules created by HIPAA, Sarbanes-Oxley and myriad state regulations, especially if the government mandates one large health IT network, as all three presidential candidates have urged. The clarity begins with understanding the security threats and matching them to policies that will reduce or eliminate them. Otherwise, like TAKS in Texas, all we'll be doing is designing security "to the test."



Compliance Without Revolt

by Steven Titch

With most new security threats coming from groups and individuals who don't need to set foot on corporate property to steal assets or damage resources, security organizations must create new strategies for communicating the importance of security policy compliance to ensure successful buy-in from the CEO on down, say two leading security consultants.

Speaking in separate breakout sessions at the 2008 Texas Regional Infrastructure Security Conference (TRISC) in San Antonio in April, Paul Williams, chief technology officer of Gray Hat Research Corp., outlined ways security officers can achieve greater success in gaining employee support of compliance policies.

Meanwhile, Joseph E. Krull, senior manager of Accenture's Technology Consulting Security Group, said employee education and threat awareness is much more critical because intruders, using phone, e-mail or simply an old-fashioned car break-in, can easily target and infiltrate the company from far outside the premises.

Both Gray Hat and Accenture's Security Group specialize in helping Fortune 500 companies adapt to new security threats. Using "white hat" techniques, they mimic the tactics of hackers, fraudsters and information thieves and evaluate an organization's response to them. From there, they can help security chiefs craft better policies.

Still, Williams acknowledged that cultivating a culture of security compliance can be difficult. Employees tend to see security policies as obstacles to their work. That's because CEOs rarely talk about security as a top priority.

Most CEOs, marketing, and research and development officers simply don't know the cost of a security compromise

"Whatever the CEO cares about, that's what employees care about," Williams said. Both speakers agreed that to get management's attention on security, CSOs and CISOs must present the costs and benefits of security policy in dollars and cents.

Most CEOs, marketing, and research and development officers simply don't know the cost of a

security compromise, Krull said.

"The loss of a patent application could be a multimillion-dollar breach if it happens before filing and registration," he said.

The theft of detailed design drawings, which feature specifications and assembly instructions laid out like a "how-to" manual, can save a competitor or foreign government months, if not years, in reverse engineering, he added.

The key to improving awareness and acceptance among mid- and lower-level employees, Williams said, is to communicate the security rationale behind the policy and the relative ease with which sensitive data can be compromised.

For example, nothing bothers employees more than a directive to change passwords, say, from six characters to eight, Williams said.

"People think there's little to be gained," he said. "We run the math. We say 'increasing our minimum password length from six to eight characters requires only a 33 percent increase in effort on the part of a legitimate user, but requires a 7,100 percent increase in effort by a password hacker.' "

Many users are equally unaware of how truly vulnerable laptops are. Along with a memo on laptop security policies, security officials should not be afraid to share what they know (see box).

This is all the more important because 21st century data networking technology makes many traditional physical security barriers irrelevant to attackers. Perimeter fences, lighting, vaults, badges and CCTV are no longer as effective because the intruder can accomplish his task by phone, e-mail or Internet, even from the other side of the globe. Yet most companies still focus their security strategy on trespassing, entry by intruders posing as outside maintenance or utility personnel, false employment or unauthorized use of cameras or recording equipment, Krull said. These ploys, although familiar enough to fans of spy thrillers, have been supplanted by new tricks, some of which are remarkably effective while being no more complex than their predecessors.

Krull outlined eight new threats that require revamped security strategies that emphasize more specific policies as well as greater education and awareness on the part of all employees.

1. **Social engineering.** Also known as "pretexting," Krull said. This involves a caller misrepresenting himself as a customer, vendor or partner in an attempt to access proprietary or guarded information, including usernames and passwords. In addition to education, the best defense is a repeated security reminder that under no circumstances should usernames or passwords be given out over the phone, he said.
2. **Bogus industry survey.** Similar to "pretexting," here the caller claims to be an intern from a major market research firm and will usually promise a reward

Eight New Security Threats

Threat	Complexity	Success	Defense
Social Engineering	Low	Low	Education and training; frequent security reminders
Industry Survey	Low	Medium	Education and training; company approval to respond
Trojans, Rootkits, Keystroke Loggers	Low to Medium	Medium	Policy, education, firewall and virus management
Spearphishing	Medium to High	Medium	Proper mail server configuration
"Free" USB Drives	Low	Medium to High	Policy, education
Bogus Internet Kiosk	High	Medium to High	Policy, education
Rogue Wireless Access	Medium	Medium to High	Policy, two-factor authentication
Stolen Laptop	High	High	Full disk encryption, security tokens, two-factor authentication

In some security tests, employees picked up as many as 18 out of 20 USB drives and plugged them into their office PCs

of cash or a gift card in return for responses to questions regarding sales, market share, products in development and so on. The best defense, Krull said, is a policy that prohibits any employee from answering a survey without management approval.

3. **Trojans, rootkits and keystroke loggers.** With greater frequency, these fraud tools are coming masked as attachments or are embedded in JavaScript on Web sites. While many organizations have made employees aware of the danger in opening unknown attachments, Krull said, fraudsters are getting craftier, often hoping to catch an emotionally reactive user by using a tagline message such as "You've been photographed naked on the Internet!" or "Look what we've caught you doing!"
4. **Spearphishing.** This takes phishing, the practice of enticing a user to reveal sensitive information with a phony e-mail claiming to be from a bank or credit card company, to a new level, Krull said. Although it does require some sophistication, spearphishing involves dummying up a fake e-mail message from the corporate CEO, usually directing the target to "forward" sensitive company documents. The target, of course, sends them to the phisher. Effective prevention is an IT task, involving proper configuration of corporate e-mail servers, Krull said.

Why Data Thieves Target Laptops

Laptops are rich targets for attack because they contain sensitive data and are literal gateways to a corporate network. Rather than simply issue directives on the use of laptops outside the office, Paul Williams, chief technology officer at Gray Hat Research Corp., suggests security professionals communicate the basic facts about the vulnerabilities laptops have. These include:

- Windows default installation implements an inadequate security policy.
- Windows installation enables unnecessary network services by default.
- Wireless network protocol security does not work.
- The current version of the Internet protocol lacks necessary security features.
- The current version of the Internet e-mail protocol lacks necessary security features.

5. **"Free" USB drives.** Krull said this low-tech technique, which can be accomplished by simply dropping thumb drives infected with trojans and keyloggers in parking lots and building lobbies, has proved surprisingly effective. Drives can contain programming to make PCs directly addressable, to upload data to specified locations or to initiate a denial-of-service attack. In some of Accenture's white hat security tests, employees picked up as many as 18 out of 20 USB drives and plugged them into their office PCs or laptops. Defense is relatively easy: Prohibit use of any foreign USB drive.
6. **Phony Internet kiosks.** A wireless Internet kiosk, often seen at airports and hotel lobbies, can be acquired on eBay for as little as $500, Krull said. Information thieves buy the equipment, haul it to a public location, advertise free Internet service and capture usernames and passwords of unsuspecting users. The thieves don't even have to provide connectivity; they can simply program the kiosk to display a 404 error page, Krull said. Users will often continue to enter other usernames and passwords in attempts to reach other sites. After a few days, the thieves return and remove the kiosk, which now contains a trove of sensitive personal data.
7. **Rogue wireless access.** Also known as the "evil twin," the thief sets up a wireless access point in close proximity to another public WiFi site, such as at a coffee shop, airport or hotel lobby. A nearby wireless user then connects through the rogue access point, which collects all the transmitted data. Krull advised his audience, when using unsecured public WiFi, to avoid accessing sites that require passwords. Companies who know employees must access their networks from the road should incorporate two-factor authentication, he added.
8. **Stolen laptops.** Lost or stolen laptops are proving to be the most costly liability in terms of information security, Krull said. Moreover, CEOs and corporate officers are now being targeted. A car break-in that results in a laptop theft may not have been the random smash-and-grab it appears to be. Thieves are going as far as casing their targets to see what type of laptop carrying case they have and purchasing the same model. After that, it's purely old school. Often using a partner, they distract the mark, switch cases and are gone. Good security defenses recognize that some laptops may indeed get stolen and require full disk encryption, two-factor authentication and use of security tokens, Krull said.

Overall, security tools exist to help counter these intrusion threats, Krull said, but education and policy are critical in bringing defenses up to date.

"There must be targeted education for senior management," he said. "Use short sentences and small words."

HEALTHCARE DATA SECURITY IN NEED OF CARE

CONVERGENCE LARGELY AN UNTESTED TREATMENT

By Sharon J. Watson

A thief steals a laptop full of medical records from a nurses' station. A veteran emergency department clerk text messages an accomplice the Social Security numbers of badly injured patients. A disgruntled former employee sabotages the network of a large healthcare provider.

Data breaches like these often grab headlines, highlighting the fact that healthcare providers maintain data ranging from credit card numbers to a person's most intimate health details. Yet while it may seem obvious such sensitive data should be treated with the highest levels of physical and virtual protection, many healthcare providers fail to do so.

A lack of coordination among physical, privacy and virtual security officers, a focus on regulatory compliance as compared to data security and a culture in which patient care must not be compromised are key factors in a slower move to convergence in healthcare than in many corporate settings.

"Physical security generally isn't connected to virtual security," says Lisa Gallagher, senior director of privacy and security for the Healthcare Information and Management Systems Society in Chicago. "Risk management is still nascent in healthcare."

MANY SPECIALTIES

Just as physicians practice various medical specialties, in many healthcare institutions, security issues cut across physical, virtual, administrative and clinical boundaries.

Healthcare's physical security demands are intense, encompassing the flow of caregivers, patients, visitors and support staff across buildings and grounds, parking lots or garages, gift shops and sometimes certain patient wards, such as the emergency department and maternity/pediatrics.

Meanwhile, many healthcare IT shops are charged with maintaining high-volume, high-bandwidth networks running vital clinical applications ranging from electronic health records to image-intensive radiology and lab results, and Web-based physician portals—in addition to critical business applications like patient administration and billing.

Next, many providers have a chief privacy officer responsible for ensuring the institution complies with federal and, increasingly, state laws governing the privacy of health information.

In this complex world, healthcare sources say it's hard to develop and fund converged security solutions unless security, IT and even privacy officers cooperate to coordinate technology requests, reduce duplicate efforts and present clear benefits to hospital administrators.

"IT and security are seen as expenses; they don't generate revenues," says Evelyn Meserve, executive director of the International Association of Healthcare Security and Safety, Glendale Heights, Ill. Meserve has worked in physical healthcare security for more than 15 years. "One way directors of these areas have been successful in funding new projects is by showing a business plan and return on investment."

The most effective plans, Meserve says, show potential losses from security problems, including problems recruiting or retaining personnel.

A cooperative approach between physical and virtual security is critical, says Bob Pappagianopoulos, chief information security officer and corporate director of technical services for Partners HealthCare in Boston. The integrated healthcare delivery system has about 60,000 employees and encompasses Brigham and Women's Hospital and Massachusetts General Hospital, along with nearly a dozen community hospitals and other clinics and physicians' groups.

Coordinating agendas, dividing duties and preventing duplicate efforts all come down to physical and virtual security experts having a strong working relationship, Pappagianopoulos says. "Success really depends on the people in the positions," he says.

Pappagianopoulos has worked with Bonnie Michaelman, Partners' director of physical security, for about 10 years.

"We've built on really good communication between our worlds," he says.

One joint project between his department and physical security has been researching means of securing physicians' laptops, such as encrypting data on them and potentially using location-based data measures to alert police if one is lost or stolen.

"We definitely partner anywhere data can sprout legs and walk away," he says.

DATA WITH LEGS

Mobile data device protection is one area in which physical and virtual data security convergence is necessary—and urgent, say consultants and providers.

"If there's patient data on those, you're in the newspaper," Gallagher says.

Healthcare providers increasingly use portable equipment to collect patient data, to access data and to signal caregivers. The range of easily lost or stolen devices and media includes PDAs, laptops, CDs and DVDs, flash and thumb drives and data cards.

Human behavior is a crucial factor in securing not just mobile data devices, but all healthcare data, say consultants and

hospital security sources.

"You can have the slickest physical security, the greatest technical measures in place, but if you don't have policies or they aren't followed, you're not secure," says Chris Apgar, CISSP, president of Apgar & Associates, a healthcare security consultancy based in Portland, Ore.

Healthcare security policies often are shaped by regulations designed to ensure data privacy, especially the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This federal law establishes security procedures and guidelines for maintaining the confidentiality of protected health information. Similarly, the healthcare industry's powerful accreditation body, the Joint Commission, now includes data privacy reviews in its credential reviews.

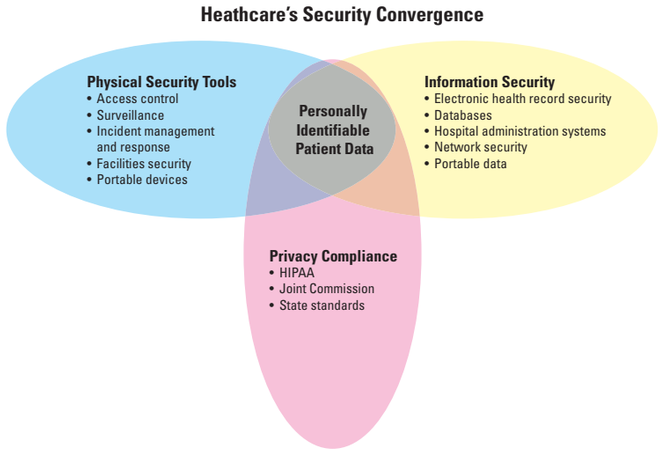
COMPLIANT, BUT NOT SECURE

While high data security might seem the obvious means of ensuring data privacy, that's often not the case in healthcare provider settings. Many providers focus on complying with regulations while remaining blind to their greater data security risks, according to the 2008 "HIMSS Analytics Report: Security of Patient Data," commissioned by Kroll's Fraud Solutions.

That report says "by and large, healthcare organizations have not been dealing with the area of accessing data with malicious intent." Yet simultaneously, the institutions are extremely familiar with, and in compliance with, HIPAA and other regulations affecting them, such as Sarbanes-Oxley and state or local regulations.

HIPAA in particular focuses on inappropriate or inadvertent access or disclosure of private healthcare data, such as by caregivers discussing cases in public areas or situating computerized medical records screens in visible areas.

"The institutions are focused on meeting the existing letter of the law versus risk management," says HIMSS' Gallagher. When an institution is declared compliant by a privacy expert or officer, CIOs often don't think additional data security measures are necessary, she says.



This is not true for all institutions. At Partners, data security was the larger goal that encompassed privacy measures, Pappagianopolous says.

"I see data privacy and data security as tightly integrated," says Ronald G. Marcum, M.D., CISO and chief privacy officer for Oregon Health and Sciences University in Portland. "You cannot achieve one without the other."

Yet some caregivers concerned about privacy don't always appreciate its connection to security.

Convergence Cures In Action

Children's Hospital of Pittsburgh, owned by the University of Pittsburgh Medical Center, is deploying an IP-based network in a new facility that will include a variety of converged security measures, according to Chad M. Lawrence, regional manager fire and safety-East Central Region, at Milwaukee-based Johnson Controls Inc. Johnson Controls is the lead integrator on an approximately $55 million system integration contract for the project, about $15 million of which is designated for fire safety and security systems.

Children's Hospital officials declined to be interviewed. However, the hospital's Web site touts several of the security features and benefits of the new institution, scheduled to open in 2009. These include secure access to the hospital's wireless data network from anywhere in the world; an emergency department and house-wide patient tracking and child abduction system; and a visitor tracking system with status, alerts and centrally monitored video both in real time and from storage.

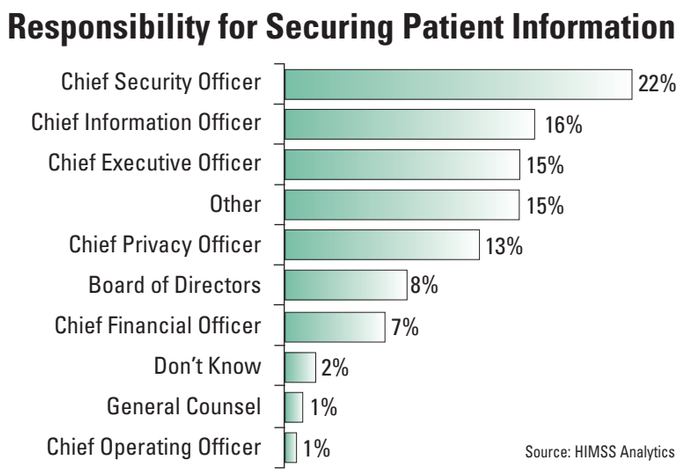
The project is designed to leverage the network's capabilities to make all hospital personnel more effective, Lawrence says. For example, the Children's Web site notes that the new facility's caregiver call system will be integrated with patient equipment, monitors, and patient and family communications. "Calls will go directly to care provider wireless phones to facilitate a more timely response," according to the Web site's Advanced Technology section.

Similarly, nurses will have access to video images to help them manage access and workflow, Lawrence says.

Tying "security" solutions such as IP-based video to a wider goal, such as better workflow and enhanced patient care, will be critical for adoption of converged security solutions, say healthcare industry sources.

Such solutions need to be presented to hospital management as enterprise-wide solutions, not silos, says Evelyn Meserve, executive director of the International Association of Healthcare Security and Safety, in Chicago.

"This will be critical, and it'll be the only way budget dollars will be allocated for these projects," she says. "If you're working in tight seclusion, your project will not be successful."



"It's tough getting the connection between privacy and security in a physician's mind," Apgar says. "That's slowly changing, but it's slow."

PATIENT CARE VS. SECURITY

That resistance may come because caregivers sometimes view security measures as interfering with their ability to deliver care. In the corporate world, a lost or forgotten password is a nuisance. In healthcare, being unable to log onto a PC with health records literally could be fatal to a patient.

So it's common for caregivers to share passwords, use a group password or fail to log off so another caregiver may have quick access to data. Using strong passwords has to be balanced with access needs, say healthcare security experts.

Healthcare provider sources cite other examples of how the unique nature of their work strongly influences their security measures. Biometrics has not gained a large following in healthcare because most providers are gloved. Video surveillance would need to be vetted to ensure its viewing area was in compliance with privacy laws.

Integrated physical and virtual access control, such as a badge reader that must verify users before they can access the hospital network, is rare, say healthcare security sources. They point out most hospitals are open facilities—and, in fact, see openness as part of their mission.

"Changing that means changing culture and workflow," Gallagher says. She and others note that vendors trying to enter the healthcare security market need to recognize the potential impact of their solutions on a provider's patient care flow.

"We on the security side are trying to be more business-friendly," Pappagianopoulos says. He says physicians are becoming more technology and security savvy, yet ease of use is still their top priority. His department tries to supply secure but workable solutions physicians will use, not work around.

Finding that balance is critical to building a foundation of trust between patient and healthcare institution, Marcum says.

"Patients need to feel their data is being appropriately used and disclosed," he says.

Or put more simply: "If you don't do security right, you can't do good patient care," Pappagianopoulos says.

Securing Patient Data: Beyond Regulatory Compliance

Healthcare institutions of all sizes tend to fall into a compliance trap, focusing on privacy measures to meet regulatory requirements and relying too much on personnel policies and procedures for data protection, failing to recognize and address the potential for malicious, criminal attacks on sensitive information.

Those are among the key findings in the 2008 "HIMSS Analytics Report: Security of Patient Data," commissioned by Kroll Fraud Solutions. HIMSS Analytics is a wholly owned not-for-profit subsidiary of the Healthcare Information and Management Systems Society, based in Chicago.

For the survey, HIMSS Analytics spoke with 263 healthcare executives, all of whom were knowledgeable about their institutions' security practices.

The report notes that the patient data hospitals collect "is the most valuable and content-rich for fraudulent use and profitability." The data often includes the "golden combination" of name, Social Security number and date of birth as well as mailing addresses, insurance policy information, medical history and even credit card and financial data.

However, the report found that respondents did not seem to comprehend their potential liability and associated costs if a third party accessed this personal data with criminal intent. It found that just 18 percent of respondents who had experienced a fraud-related breach believed it had a financial impact. That fact, concluded the study, was consistent with the findings that "awareness in the healthcare industry around the impact and implications of a data breach…is low."

Sharon J. Watson is a journalist based in Sugar Land, Texas. She can be reached at sjwatson@experteditorial.net.

THE SMART, SECURE BUILDING

PLANNERS SEEK TO TIE SECURITY SYSTEMS TO BUILDING AUTOMATION

By John W. Verity

Architects and engineers first envisioned "smart buildings" about 20 years ago. In these structures, access and safety alarms, heating and ventilation, lighting and elevators all would be controlled from a common point. Among the potential payoffs, promoters said, would be streamlined management of subsystems, lower costs, more efficient use of energy and greater convenience for tenants and visitors.

Since then, buildings have certainly grown brainier, but technology has lagged behind vision and synergies have been slow to materialize. Intelligence has ended up scattered across disparate networks of sensors, logic and actuators. Badge readers don't talk to chillers, which don't talk to elevator controllers, which don't talk to surveillance cameras. Alarms, video and other data may be consolidated to show up on a shared console, but that's only a small step forward.

But now, with energy prices skyrocketing, building managers are exploring the potential of the Internet protocol (IP) and Ethernet networks that snake through their properties to integrate the functionality of different systems.

THE IP ENGINE

Building management system vendors already have been scrambling to push IP closer to the edge of their networks to harness its ability to link potentially any and every electronic device, from clusters of servers to fans and blowers to individual locks and light switches. With convergence grows recognition of the fact that, by virtue of its ability to record and store the identity and, sometimes, the location of individuals within a facility, access control and management systems have a logical and valuable fit into the IT system of a large building. Yet they remain a largely untapped source of real-time information that could benefit and support both building operations and the occupants' enterprises.

"Physical security has always been thought of as a necessary evil, but now it's seen as a key part of making many other systems work together more efficiently," says Vishal Mallick, CEO of Performance Buildings Ltd., a Regensdorf, Switzerland, software firm specializing in building system integration, especially for tenants who plan, arrange and host regular meetings that involve outsiders as attendees as well as suppliers, such as caterers.

Also, as the move to IP gives IT departments a stronger say in all aspects of enterprise security, those departments are moving to leverage their experience and expertise in weaving together traditionally isolated applications. These include security, facilities management, energy and traditional IT systems like human resources and enterprise resource planning, analogous to what Wal-Mart and other retailers have accomplished with their complex supply chains. Meanwhile, a bevy of start-ups is applying advanced software ideas, originally developed for the military, to the problem of how to collect, interpret and automatically act on the rivers of sensor-generated data that are cascading through and between large buildings and far-flung corporate campuses.

"Integration will enable customers to reuse the same sensors to address four different issues: operations, safety, security and accountability," says Sandeep Gulati, chief technology officer and vice president of product development at ViaLogy, Altadena, Calif., which specializes in integrating sensor networks. "Harnessing combinations of sensors means a better payoff and return on investment for security investments."

GREATER SAFETY, SAVINGS THROUGH INTEGRATION

Ajay Jain, president and CEO of Quantum Secure, a physical security startup, describes a possible scenario: A multinational company's security operations center in California receives fire alarm signals from

one of its labs in Japan. The lab's access control system shows that 15 employees are in the building. Automatically, an integration server like Quantum's might alert each of those persons with a cell phone text message: "A fire has been detected in your facility. Reply '1' if you're safe and secure, '2' if you require help."

At the same time, the platform could command electricity to be shut off at the fire's location, get fire dampers closed and rev up smoke extraction fans. Video cameras might zero in on the fire, their image-frame rates automatically upped for better quality. Furthermore, with officials on the scene and back in the United States needing to view those enhanced video streams, the company's network routers could be requested to allocate additional bandwidth.

ADDRESSING TECHNICAL CHALLENGES

Physical security and IT directors ready to pursue security and building system integration will find a market in which underlying technologies, product offerings and building-specific technology standards are evolving and where newcomers are trying to wrest market share from established players.

> As the number of sensors in buildings grows, new opportunities arise for analyzing and acting on that data near-instantly.

In addition to security benefits, vendors promote energy and efficiency savings. They envision buildings smart enough to adjust lighting, temperature and elevators in response to employees' badging into a building. The integration necessary to realize this scenario can pay for itself in as little as 18 months, according to Paul Ehrlich, president and founder of Building Intelligence Group LLC, a St. Paul, Minn.-based consulting firm.

"The paybacks are great, especially when compared to the 10 years it can take for solar panels to pay for themselves," Ehrlich says.

By helping to fulfill the promise of "sustainability," these savings also can increase a building's appeal to the growing cohort of "green"-conscious tenants.

More efficient building operations is another key benefit. With the right analytics in place, notes Bill Jacobs, director of global risk technologies and head of internal security at Cisco Systems, security cameras can improve a tall building's elevator service. When a camera detects too many people waiting in the lobby for too long a time, the system can automatically be directed to bring down an empty car or two and alleviate the crowd.

Likewise, air-flow measurements normally monitored by a building's HVAC system can help in determining if a particular door has a broken lock or is being buffeted by a differential in air pressure.

"Integration can save energy, cut costs and improve business efficiency," Jacobs says.

The good news, says Building Intelligence's Ehrlich, is that "the building automation industry is transitioning to look a lot more like the IT industry."

Proprietary technology is giving way to open, industry-defined standards that could enable a rich, plug-and-play future. Customers and system integrators want the freedom to mix and match best-of-breed products as they choose. This demand is pressuring established suppliers, which have traditionally emphasized an ability to provide broad ranges of compatible products, to tout their adoption of industry standards and work closely with selected newcomers.

Technical challenges abound. That badge readers, video cameras and air conditioners can share a building's Ethernet network is no guarantee that they can make sense of each other's data. Even the servers to which each device sends its data may not have much in common. Established suppliers of building management systems, such as Honeywell, Siemens, Bosch and Johnson Controls, emphasize their ability to bridge these gaps and translate data between disparate systems. They've also thrown their support behind industry-defined schemes such as BACnet, LONworks and oBix, which describe how different building automation and security devices and networks can exchange data and commands.

SENSORS SOUND OFF

Entirely new technologies may find a key role, too, particularly in the area of data fusion. As the number of sensors in buildings grows, and as these sensors generate more types of data, new opportunities arise for analyzing and acting on that data autonomously and near instantly.

Improving techniques for rapidly combining and interpreting masses of signals from multiple sensors to achieve a better understanding of an event or a developing situation has been the focus of intense research by the military, in pursuit of the so-called "intelligent battlefield." The challenge, obviously, is how to triangulate on several signals at once to identify significant events amid a flood of noise and false alarms. These sensor fusion techniques are aiding industrial applications such as managing buildings, tracking assets with RFID tags, improving physical and IT security and detecting fraudulent financial transactions.

Today, each of the established building automation players sells its own software or console for collecting, recording, analyzing, and presenting alarms and data from different sets of sensors. Honeywell's Tridium subsidiary offers Niagara, for instance, while Johnson Controls markets a scheme called Metasys.

And now, a handful of smaller companies are developing software, called integration platforms, that promises to take building automation to a new level. Companies such as Augusta Systems Inc., Proximex, GridSoft, ViaLogy and Quantum Secure have designed these products to help enterprises cope with the coming floods of data that thousands of sensors, devices and

machines will be generating primarily for consumption by other machines.

These platforms are designed to gracefully handle massive volumes of data, even when that data is encoded in many different formats. On the fly, the software can normalize this data by translating it into a common format. Then, it can scan the data and, in real time, recognize patterns and make correlations between signals that may identify significant events that wouldn't be detected otherwise.

In a high-rise building, a motion detector's alarm might be analyzed with video and badge reader data to determine how many people are in a conference room and decide if the air conditioning should be upped a notch. Likewise, as soon as an unusual spike in network traffic is detected, correlating data from several different kinds of sensors can distinguish a physical emergency situation from an outbreak of computer viruses.

One area where the new integration companies differ from established players in analyzing masses of real-time building data is in their use of distributed architectures. Instead of bringing all the unprocessed data to a central location for analysis, their software can inspect signals both centrally and toward the edge of the sensor network. With processing taking place throughout the network—Augusta's analytics can actually run on a simple circuit card inserted in a standard IP network router—these setups can greatly reduce net traffic and thereby handle many more sensors and process much more data than earlier centralized systems.

Carter Williams, CEO of Gridlogix, says his firm's EnNet platform "can listen to thousands of buildings and millions of data points at once." That scale of real-time monitoring is proving necessary, he says, as global companies seek to integrate all of their security and building management systems with their traditional enterprise software apps.

ACTING ON DATA

Once significant information and insight have been derived from sensor data, what to do with it? Here, too, the independent integration platform companies claim to bring something new to market. They describe their software as enabling customers to prepare complex policies and response scripts that automatically send commands to the full range of building automation systems. These policies are entered and maintained through graphical drag-and-drop programming techniques.

Should a building's fire alarm go off, its air dampers will open, secure access doors will be unlocked and surveillance cameras will zoom in on trouble spots.

Because their systems are open, integration platform makers see established building automation suppliers as natural partners. Still, companies like Proximex find themselves often doing a hard sell.

"A big challenge for us is to find partners with a holistic view of the market and opportunity," says Larry Lien, vice president of product marketing at the Sunnyvale, Calif.-based company. "We need to educate the entire industry."

Industry executives say corporate IT managers are beginning to fathom the long-range implications of building system integration and are shepherding vision into reality. At Ave Maria University in Naples, Fla., Bryan Mehaffey, vice president of technology and engineering, was asked to create a facilities infrastructure for the 600-student, nine-building campus before it opened last year.

"I sat down with pen and paper and worked it all out from scratch," Mehaffey recalls. The result: a 762-page RFP that called for physical security systems to work intimately with both human resources and building automation systems. Beating out two competitors, Johnson Controls won the deal "because they understood our vision," Mehaffey says.

Full integration is not complete, yet, but soon physical security and fire alarm systems will be programmed to work directly with building automation. Should a building's fire alarm go off, its air dampers will be directed to open, extra fans will kick in to extract smoke, secure access doors will be unlocked and surveillance cameras will zoom in on trouble spots.

SMART PLANNING

Customers seeking to integrate security into building and enterprise systems like HR and enterprise resource planning will do well to start their planning as soon as possible and to involve all interested parties: architects, engineers, contractors, facilities managers, IT and security, at least.

"All of these organizations have different budgets, play different roles and have their own priorities. You have to get them all in the same room so they can work things out in a structured way," says Jim Dagley, vice president of channel marketing and strategy at Johnson Controls.

Early planning sessions, says Terry Hoffman, director of marketing at Johnson Controls, give all parties "an opportunity to work off each other" and overcome their natural "fear of the unknown."

IT managers, for instance, are often concerned that an abundance of security cameras will hog network bandwidth and compromise data flow. However, by "focusing on commonalities first," says Hoffman, later discussions, which typically center on aligning costs with budgets, will be much easier. The results will be a solid road map and many fewer review cycles that risk delaying construction.

Smart planning, it seems, makes for smarter buildings.

John Verity *is a freelance journalist based in Maplewood, N.J. He can be reached at john@verity.com.*

A WIRELESS VIDEO SURVEILLANCE SYSTEM ERASES A GRAFFITI PROBLEM

By Steven Titch

In the city of Montebello, Calif., it can be said that video surveillance works like a sponge.

Montebello, situated between East Los Angeles and Whittier, faced a graffiti and vandalism problem in its central business strip and surrounding public parks. City officials in the town of 50,000 residents—whose daytime population swells to 110,000—feared the pervasive vandalism was driving away commercial traffic and eroding quality of life.

The city responded with the installation of a video surveillance system combining Internet protocol-based cameras, wireless connectivity and a special audio sensor designed to respond to the hiss from a can of spray paint.

"The city wanted to cut down on graffiti to encourage more commerce," says Gary Pak, vice president of sales with Axium Technologies Inc., the systems integrator who handled the project.

'BROKEN WINDOW' THEORY

In addressing graffiti as a quality-of-life issue, Montebello officials applied the "broken window theory" popularized by urban consultant George L. Kelling, who has worked with city governments in New York, Boston and Los Angeles. Simply put, the theory states when repairs are neglected on a building with a few broken windows, there is a tendency for vandals to break more. Eventually, according to the theory, they break into the building, causing more damage. The theory has been applied to litter, subway "turnstile jumpers" who evade fares and graffiti in public places.

"Deal with the small problems, and the big problems will take care of themselves," Pak says. Clean the graffiti, and it won't accumulate. Parks and neighborhoods look less run down. Residents and business owners don't move out.

Still, cleaning didn't come cheap, especially when taggers were persistent. Graffiti incidents had reached 400 a month, and Montebello was spending $600,000 a year in paint removal, Pak says. When the costs of police overtime and court appearances were factored in, "it was a $1 million a year problem," he says. The city began to look at more cost-effective ways to address the problem and, ideally, preempt it. That's when video surveillance came up.

Two surveillance pilots in nearby Los Angeles proved influential and encouraging. In 2005, the Los Angeles Police Department placed cameras in the Hollywood entertainment district and the Rampart section, including MacArthur Park. Together, the areas saw a 45 percent decline in criminal activity, the biggest single-year drop in LAPD history.

"Citywide surveillance is a relatively recent phenomenon. In 2005, I think there were only 20 locations in the United States," says Pak. "It's becoming more commonplace now."

For Montebello, Axium installed a wireless Ethernet system from MicroTek Electronics of Lake Forest, Calif. The initial installation, in October 2007, featured 16 Pelco Spectra IV cameras; the number grew to 120 cameras when the system was completed last April.

The $836,000 project will pay for itself in three to four years, says Pak.

BOULEVARDS AND PARKS

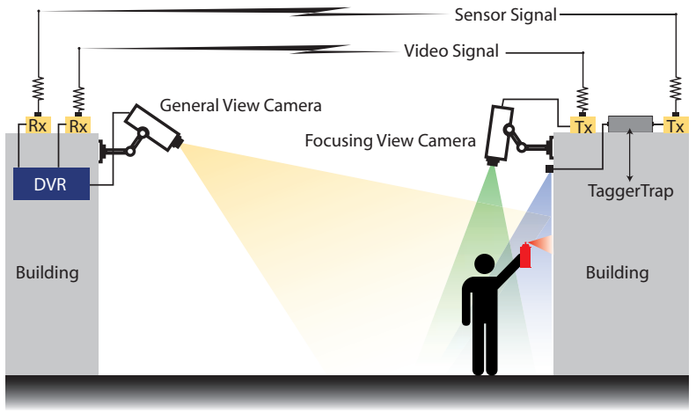
Along Whittier and Beverly boulevards, Montebello's two main thoroughfares, the city installed cameras on traffic lights on every block. Three cameras were deployed per access point. Each access point connected to a T1 (1.5 Mb per second) line. The wireless system uses unlicensed frequencies in the 5.8 MHz band. Radio signals use the 802.11a protocol, commonly known as WiFi. All traffic is IP Ethernet.

Additional cameras were placed in eight public parks, as well as an area that was routinely attracting illegal dumping. The wireless cameras have a transmission range of 2,500 feet to two miles, depending on the radio environment, says Jon Epperson, the sales manager with MicroTek who worked on the Montebello project. Optically, the Spectra IVs have 35x zoom capabilities and can capture a clear image one-quarter mile away in low light.

The unique feature of the system is Axium's TaggerTrap, an audio sensor developed by the integrator that networks into the camera platform. Monitoring and recording conversations alongside video surveillance is illegal. TaggerTrap does neither. Its sensor is attuned to the 40 KHz sound made by an aerosol spray can. When the TaggerTrap registers the sound, it signals the camera to focus on the source (see diagram). TaggerTrap literally catches the violator in the act, providing a time-stamped video image that can be used as evidence. It works with a stand-alone network DVR using Axium-developed software, Pak says.

Since its deployment, the video system has resulted in a number of arrests. But more importantly, it has proved a strong deterrent for would-be taggers.

"The decline has been significant," says Pak, who cites unofficial estimates of a 30 percent decrease in graffiti incidents. Before the cameras were installed, the



Axium's TaggerTrap senses the sound from a can of spray paint and signals a nearby camera to focus on the source. In the Montebello application, the camera sends an image via an 802.11a wireless IP network to a DVR (shown) or backhauled on a T1 line to a control center.

number of graffiti incidents had been going up every year, he says.

LOCAL AWARENESS

While the cameras themselves are quite visible, Montebello, for its part, wanted to make sure local awareness was high.

"We wanted people to know they were there," Pak says. "We've gotten a lot of press about it, including articles in Chinese- and Spanish-language newspapers."

Next steps for Montebello, Epperson and Pak say, will be upgrading video systems at the city's police headquarters and installing a new surveillance system for City Hall. These will come under a separate contract. Plans call for introducing BlackBerrys and other handheld devices, adapted for public safety purposes, for use with technologies like voice over IP. These will replace the traditional analog two-way radios the police department uses now, Pak says.

As for the MicroTek equipment, Pak says the performance of the wireless system has been "phenomenal." Pak notes that radio engineering requires a degree of expertise, which he says Axium brought to the project. Nonetheless, the system, set up in point-to-point configuration, had no engineering flaws.

"We could do a camera installation in less than a day," he says.

There were more problems with other aspects, including long waits for T1 lines. In addition, the Pelco Spectra IV SE cameras, among the company's workhorse models, were often on back order.

MicroTek was founded in 1992 and specializes in wireless Ethernet technology, video, voice and data access control. It has supplied wireless surveillance installations to diverse customers, including the city of Baltimore, the Marine Corps base at Camp Pendleton, Calif. and the Las Vegas Motor Speedway.

A chief advantage of radio is its cost over laying cable.

"There's the cost benefit of not having to trench. You don't have to tear up streets," says MicroTek's Epperson. "But you can put the cameras where you need to put the cameras." In addition, Epperson says, the plug-and-play simplicity of 802.11 and IP make the technology easy to work with once it's online.

Prospective customers, from large cities to homeowners' associations, are "more and more interested in video surveillance," Epperson says. "Wireless is becoming more accepted as a means of transmission."

Steven Titch *(titch@experteditorial.net) is editor of Network-Centric Security.*

IT Departments Seek Wireless Skills

Go wireless, young IT staffer, says the Computing Technology Industry Association (CompTIA).

A recent worldwide survey of more than 3,500 information technology (IT) managers found that wireless and RF mobile technology expertise is the skill set expected to increase the most in importance over the next five years.

Among specific industries, 63 percent of IT managers both in healthcare and education were more likely to identify wireless technology expertise as the skill that will be most important five years from now, the study found.

What's more, wireless expertise, combined with security systems experience, may prove a winning career mix. Security remained the top IT skill sought, with 74 percent of the respondents rating it 6 or 7 in importance on a 1-7 scale. Skills with general networking and operating systems garnered a 6 or 7 rating from 66 percent of those polled.

"The knowledge of how to successfully design and implement a wireless system is a valuable skill set within the IT and traditional security realms," says Jon Epperson, sales manager with MicroTek Electronics. "As wireless technologies have improved in reliability, they have become more accepted as a standard transmission method. Wireless technologies provide a cost-effective alternative for data transmission when cabling is not possible or is cost-prohibitive."

The respondents were 3,578 IT managers. All are responsible for the hiring and/or managing of at least three IT employees at companies with 10 or more employees. The survey sample was comprised of a minimum of 250 IT managers from each of the following countries: Australia, Canada, China, France, Germany, India, Italy, Japan, The Netherlands, Poland, Russia, South Africa, the United Kingdom and the United States.

—Steven Titch

Applications, Strategies, & Solutions

1 Video Management Software

On-Net Surveillance Systems Inc. (OnSSI), has released version 6.5 of NetDVMS, its network video recorder (NVR) and camera management software, a key component in the newly launched OnSSI Ocularis platform. NetDVMS 6.5 adds two-way audio functionality to the bundled NetGuard-EVS video client. Users are able not only to monitor and record audio from camera-connected microphones, but also stream audio from the control room to camera-connected sound systems, allowing two-way audio interaction with video-monitored persons. The new version supports different frame-rate video streams for live monitoring and recording, resulting in efficient data transport and reduced CPU loads on the video servers while maintaining the quality of the recorded video. In addition, version 6.5 adds support for the MxPEG compression format, with H.264 and MPEG4 ASP planned for future releases.

www.onSSI.com

2 Ethernet Switch

The Hewlett-Packard ProCurve Switch 2610 Series consists of five switches; the 2610-24 and 2610-48 (pictured) provide 24 and 48 ports of 10/100 connectivity. The 2610-24 is fanless, ensuring quiet operation and making it ideal for deployment in open spaces. The 2610-24/12-PWR, 2610-24-PWR and 2610-48-PWR are IEEE 802.3af-compliant for Power over Ethernet (PoE) and provide up to 15.4 W for 12, 24 and 48 ports. The 2610-24/12PWR has 24 10/100 ports and provides 12 ports of PoE. All switches include two 10/100/1000Base-T ports and two mini-GBIC slots for gigabit uplink connectivity. An optional external power supply is also available to provide redundancy in the event of a power supply failure. With static routing, robust security and management features, free lifetime warranty and free software updates, the 2610 series is a cost-effective solution for customers who are building converged enterprise edge networks.

www.hp.com

3 RAID Hard Drive

Samsung Electronics' Spinpoint F1 RAID Class 3.5-inch SATA hard drive offers 1 terabyte (TB) of capacity and is specifically designed for enterprise storage and surveillance applications. Offering the world's highest recording density using only three platters and running at 7,200 rpm, the RAID drive features a 16 or 32 megabyte (MB) cache and is ideal for use in video surveillance and similar environments with critical features such as high reliability in heavy-duty, 24/7 operations, low power consumption, improved performance, high capacity and A/V streaming firmware command set. The three-platter structure provides a higher data storage density per platter, resulting in faster data processing speeds when compared with other 1 TB drives.

www.samsung.com

4 Wireless Video Deployment

NASA Dryden Flight Research Center at Edwards Air Force Base, Calif., protects its highly specialized research aircraft with a wireless video surveillance system. To deploy a security system from the ground up in 60 days, the center's security department turned to AgileMesh, a provider of rapidly deployable video surveillance, and Firetide, a developer of wireless mesh networks. The wireless system transmits evidence-grade video from the perimeter of the facility to the on-site security operations center. The video is monitored in real time; personnel patrolling the perimeter can respond to incidents within seconds. The system also provides evidence for security and safety.

www.agilemesh.com

www.firetide.com

5 IP Storage

Intransa's EdgeBlock scalable IP storage provides full RAID support and delivers advanced data protection and high fault tolerance. Intransa IP storage scales modularly from as little as 4 terabytes (TB) through to 1,500 TB in a single, easy-to-manage system. Intransa offers affordable, plug-in modules for any future growth requirements. With scalable performance of 200 to 3,000 Mb/s and support for common 1 and 10 gigabit Ethernet infrastructures, the storage is ideal for the smallest through the largest industrial video needs.

www.intransa.com

There's Value in Integrated Security

By Marleah Blades

When Mike Howard became director of corporate security for Microsoft in 2003, he had to upgrade the company's global security monitoring hub.

Microsoft wanted effective, integrated security and life safety monitoring—watching cameras and access control events, performing dispatch, enabling seamless emergency response and continuity—to protect corporate assets and nearly 80,000 employees around the world.

"As we started to do some due diligence into the center," Howard says, "we realized that it was made up of a bunch of proprietary systems that didn't integrate well with each other and were not scalable. In terms of real global presence, it was global in name only."

The three Global Security Operations Centers that Howard and his global security team have worked for the past three years to develop—one at Microsoft headquarters in Redmond, Wash., one at the Thames Valley campus in the United Kingdom and one at the Hyderabad, India, campus—are based on a variety of Microsoft and third-party applications that integrate with Microsoft products, backed by a technical infrastructure from Lenel Systems International. The GSOCs have built-in interoperability and redundancy, so if one center goes down, all functions automatically transfer to another campus. Operators can easily pull up and view every camera location at each connected campus, and events can be monitored from anywhere.

A recent initiative at the software giant offers valuable lessons for companies of any size

Many companies won't have the capital or technology available to create a system this elaborate to monitor remote offices or locations. Yet the lessons learned from this project apply to security for companies of all types and sizes.

Use technology as a force multiplier. "For smaller companies and for us, the idea is to leverage personnel in strategic hubs and use technology as a force multiplier," Howard says. "So instead of, for example, having two or three guards in Dublin, you have remote monitoring via cameras that give you the same views of entrances and exits and garages without having to have personnel there."

Howard notes that the GSOCs have allowed Microsoft to reduce the guard force at one U.K. campus from four to one, and they also were able to give the old monitoring room to one of the business units for other uses.

continued on page 34

Evangelize security. "Our team has worked hard to get senior leadership support for the GSOCs," Howard says. "The first part was just to acquaint senior management with what we're doing here in global security and our strategy. To a lot of people five or six years ago, we were the guys who ran around in uniforms on campus. There was no knowledge of our investigations, threat analysis, handling of international events, etc."

After the team briefed the managers on the security program, they focused on the inadequacies of the current monitoring center.

"We wouldn't have been able to do this if we hadn't gotten to senior leaders and been very open about the gaps," says Howard, who took managers to the center to see the issues for themselves. "We were at a parking garage level, the room was very small, and I could take them around to see bundles of cables spliced together and stacks and stacks of servers that were running out of space. Once they saw that, it hit."

Tie new projects to business value. A security leader will more easily gain support for any big project if he or she can show its business value—not just how it may improve security, safety and productivity, but also, where possible, how it may be used by other groups to improve efficiencies or create new opportunities. Because the Microsoft GSOCs are built on Microsoft applications, the global security team works with Microsoft's sales and marketing departments to perform demonstrations for potential customers who might be interested in similar technologies.

"A typical example involves a scenario in which an earthquake in Redmond shuts down the operations center," Howard says. "We'll turn the lights off for our viewers and shut down the computers, and we move load sharing from Redmond to the United Kingdom. Then there is a fictional employee here on campus who can't get out of his office. We are able to show that the U.K. center can see every camera view on our campus and can dispatch responders in Redmond to take care of that situation."

These demonstrations make security more than a cost center.

"We're contributing to the bottom line by influencing revenue, bringing in potential clients and having technology keep employees safe and maximize use of limited manpower," Howard says.

Marleah Blades *is senior editor for the Security Executive Council, an international professional membership organization for leading senior security executives spanning all industries, both the public and private sectors, and the globe. For more information about the council, visit www.SecurityExecutiveCouncil.com/?sourceCode=netcentric.*