Chapter 3

Security Convergence: What Is It Anyway?

Solutions in this chapter:

- **Defining Security Convergence**
- **Functional Convergence Drives Security Solutions**
- **Security Convergence Is Changing the Security Culture**
- **The Convergence Role in Accelerating Security Solutions Worldwide**
- **Security Convergence Is Changing the Sales Channel**

Introduction

Security convergence has numerous definitions and involves the ability to leverage technology to improve the performance of the security function, both physical and electronic. It is a major trend in the security industry today, but as we try to define it, we must realize that it is a subset of a much larger global move toward collaboration as the result of a changing workforce. The new generation of corporate employee, police officer, or military foot soldier has been raised on interactive technology and gaming programs that promote the abilities to collaborate and share information in real time across limitless geographic boundaries. As this mindset penetrates the global workforce, the way in which work is performed will change. This phenomenon is occurring simultaneously and globally across both government and industry sectors. A traditional discipline such as physical security, which has resisted major technical innovations to expand services on a global and collaborative level, is changing quickly. Services as fundamental as physical security guarding will be significantly impacted by new technologies that provide more efficiency with less manpower, not unlike the business benefits derived from global outsourcing.

Electronic security software programs are also undergoing fundamental changes as global communications and mobile access create an environment whereby traditional policies to protect information assets are inadequate. It is with this global trend in mind that we attempt to define security convergence to determine what impact these changing technical, workplace, and social variables will have on the security industry in the twenty-first century.

Defining Security Convergence

Security and convergence in and of themselves are interesting concepts, and we need to examine them separately to gain a clear understanding of their combined business value. As we noted earlier, security is an age-old concept dating back thousands of years to the dawn of man. In many ways, it is innate to the human condition. A sense of security may be difficult to define, yet we know it when we feel it. In this regard, it is similar to the famous quote from Potter Stewart, associate justice of the U.S. Supreme Court, when attempting to define hard-core pornography and obscenity: "I shall not today attempt to define the kinds of material … but I know it when I see it." With our sense of security or feelings of vulnerability, it might be easier to define it when we don't feel it.

Whereas a sense of security may be individual, in many respects the common view typically involves a sense of well-being. Dictionary.com defines *safety* primarily as "the state of being safe; freedom from the occurrence or risk of injury, danger, or loss." Fair enough. Let's leave it at that for the moment.

Defining *convergence* is not so simple. It does not roll off the tongue as a ready answer that you hardly need to comprehend, much less give serious thought to. The Cambridge Dictionary Online defines *converge* as "the process of ideas and opinions gradually becoming similar; a convergence of interests/opinions/ideas." What is interesting, however, is this note,

"compares to 'diverge,' " which was defined as "to follow a different direction, or to be or become different."

The term *divergence* may actually be more synonymous with success in the security convergence model today. This ability to change, or diverge, follows a different path and is fundamental to business success. It provides a competitive differentiation and is one of the key benefits upon which selling a convergence model is based. It matters little what size business you have. When major manufacturers stumble and fail, upended by fundamental industry change and an inability to respond to that change in a timely fashion, their sales channels, supply partners, and customers feel the impact. In addition, the definition of *security* is "freedom from risk or danger, safety; to take precautions to guard against crime, attack, sabotage, and espionage." This ability to "secure" against threats would apply not only to human beings, but also to innate objects such as corporate data and personal possessions. In this regard, the full spectrum of a definition of *security* would involve both physical security and information security aspects. For example:

- Freedom from danger, risk, and so on; safety
- Freedom from care, anxiety, or doubt; well-founded confidence

A Three-Pronged Approach

In attempting to write our definition, we must realize that any discussion of security convergence must go beyond standard definitions to include an understanding of the impact of security convergence on individuals, because fundamentally, security convergence impacts people and their ability to perform their jobs. As emerging technologies (hardware, software, and networks) provide the platforms for security policy to be accelerated across a global enterprise, it is important not to lose sight of the fact that people are critical to successful deployments. The classic "guards and geeks" confrontation comes to mind; however, this is only one component of the people factor. New executive leadership roles will evolve internally, as will requirements to collaborate outside the organization. We will discuss these people dynamics in more detail elsewhere, where we talk about stakeholders; however, it is imperative that up front we recognize that security convergence involves not only technology and the application of a security process (physical and/or logical), but also the key roles and new responsibilities of the people required to effect successful organizational change and, ultimately, security convergence. Security convergence is a three-pronged approach composed of technologies, security processes, and people.

According to a report by Frost & Sullivan, the worldwide Internet Protocol (IP) surveillance market will grow to $6.48 billion in 2012 from last year's $435.8 million. Digital video surveillance—that is, using computers and networks to store, play back, and analyze surveillance video—is the security technology of the future. It is also a great example of how the convergence of information technology (IT) with a physical security operation (monitoring activity) is changing both the guarding service business and upgrading analog infrastructure to new digital communications.

Traditional video surveillance installations included analog cameras and VCRs, both which require heavy emphasis on manual observation and operation in the form of changing, erasing, and storing tapes. Although 80 percent of the surveillance market comprises analog cameras today, and newer network video recorder (NVR) technologies are being deployed, "green field" or new installations are almost 100 percent digital. Additionally, video images are migrating over IP networks to storage area networks (SANs) and network-attached storage (NAS) arrays already existing in the corporate IT infrastructure.

Suffice it to say that IP digital video surveillance equipment and analytics software are changing traditional video surveillance operations in the physical security industry. The video bank of monitors being watched by one or more security guards is being replaced by software that determines anomalies in the perimeter and alerts guards in real time. No longer do security operations have to rely on constant "human" attention to video monitors, the quality of which deteriorates significantly after 40 minutes have passed. These new surveillance technologies improve image clarity; accelerate search times; improve storage density, footprint, and recovery issues; reduce equipment and manpower costs; and can interface to other security solutions over an IP network. Time and distance obstacles are removed from the security operation as well. The flexibility and functionality of IP-based systems allow for the deployment of leading-edge digital security solutions into wide-area deployments that would have been technically prohibitive and/or cost-prohibitive with older technologies. Established integrators are finding these new technologies critical to addressing new, large-scale security opportunities.

Notes from the Underground…

Convergence Case Study: Lockheed Martin Selects New Technology to Protect NYC Commuters

In August 2005, New York's transit authority awarded Lockheed Martin a $212 million contract, which includes installation of 1,000 cameras and related equipment in city subway stations, on bridges, and in tunnels. As part of that contract, Lockheed selected leading-edge technology from a start-up company based in Silicon Valley. BroadWare Technologies is the network video systems company that provides standards-based platforms and end-to-end browser-based solutions for collecting, recording, routing, and managing live and archived surveillance video while optimizing the use of bandwidth. BroadWare's products integrate an organization's new and existing security equipment into one interoperable system that evolves as new IP-based technologies emerge. Lockheed Martin recently selected BroadWare as the core supplier of video surveillance and media integration components being

Continued

deployed within the New York Metropolitan Transportation Authority (MTA) Integrated Electronic Security System and Command, Communications and Control (IESS/C3).

The MTA oversees the New York City transit system, Long Island Railroad, Metro North Railroad, and MTA bridges and tunnels. As the prime contractor, Lockheed Martin is leading a team to design, develop, and deploy a critical infrastructure protection system that integrates command, communications, control, and security capabilities across MTA facilities. The BroadWare Media Integration Platform has been selected as a component of a video surveillance subsystem that will initially control more than 1,000 cameras coupled with motion and intruder sensors to protect subway stations, commuter railroads, bridges, and tunnels.

"Lockheed Martin chose BroadWare to ensure that the MTA would have a highly scalable video and media platform that fulfills all current requirements and is easily expandable to meet future requirements over the life of the system," said Bill Stuntz, CEO of BroadWare Technologies. "The New York MTA is one of our nation's highest-risk public environments, and this upgraded MTA security system will be one of the largest and most capable of its kind."

The New York MTA subways, buses, and railroads move 2.4 billion New Yorkers per year—about one in every three users of mass transit in the United States and two-thirds of the nation's rail riders. MTA bridges and tunnels carry nearly 300 million vehicles annually—more than any bridge and tunnel authority in the nation. This vast transportation network—North America's largest—serves a population of 14.6 million people in the 5,000-square-mile area fanning out from New York City through Long Island, southeastern New York state, and Connecticut. The MTA installation is one example of how new security technologies are being deployed to secure huge public infrastructures that play a critical role in the nation's economy.

Very well then. Let's agree in principal that convergence follows security from a historical perspective. In fact, compared to security, convergence is state-of-the-art conceptually. This combination of old (security) and new (convergence) is what may lead to the initial confusion expressed today around the concept of security convergence.

In computing history, security convergence may be similar to hardware predating the evolution of software. Yet in terms of the future of security solutions, the value of convergence may play a similar role to software when it comes to mass deployment and new innovations.

The strategic aspect of new-solution development is its capability to differentiate and provide innovation as a competitive advantage in a fast-changing market. After all, security cameras used for surveillance have been around for decades, yet only relatively recently has networking provided a cost-effective and global capability to utilize that traditional camera in innovative ways through hardware advancements and new software features. Future

applications are currently being developed around the concept of "video data vaults" whereby networking and storage expertise will become key technical and sales requirements in the future. Convergence and product innovations go hand in hand within the context of changing technologies. From a technology viewpoint, Voice over IP (VoIP) represents a tipping point in the evolution of two technologies converging and, in the process, combining to produce a measurable business benefit by reducing telecommunications costs.

A natural second phase of the evolution of convergence within the IP model involves VoIP. In many ways, a similar value proposition exists in deploying a video file over the network to advance the ability to communicate, in this instance visually rather than verbally. Once combined, this powerful ability to utilize voice, video, and data across the same IP network lays the foundation for any number of innovative solutions to come to market and increase productivity through improved communication and collaboration. This innovation wave increases or accelerates the technical change and, in so doing, also increases confusion, as people try to keep pace with the advances which only a few years ago seemed like simple and mature technologies. A cell phone or CD player comes to mind; not only have these devices significantly increased their respective capabilities and performance levels, but in the process of technical advancement, the devices themselves have converged, and together have become a unified platform for still more innovation and services. The convergence cycle repeats itself over numerous technical platforms, from automobiles to wrist watches, as open source software development tools provide new solutions at record speed. No wonder people are confused.

This concept of change is second nature in high-tech circles, and the ability to embrace it quickly is the difference between success and failure. Conservative industries, such as physical security, need to understand computing history and leverage change to their advantage. They must accept business reality and focus their efforts toward a new converged security model and dedicate new resources to execute relentlessly. Likewise, the information technologist must realize that physical security is not some mindless activity that he can quickly accept responsibility for and learn on the fly. Losing data is one thing; causing loss of life through inexperience is quite a different situation.

The bottom line is that security convergence promotes confusion. In a real sense, when things converge they change form and/or function. For example, two separate streams converge into a larger river. In addition to physical iterations, the process of change, in and of itself, is difficult and creates confusion on the part of individuals. A technical example would involve a historically physical process—for example, the function of opening and locking a door—now being integrated over the IP network to be performed remotely and electronically. One key to reducing confusion during convergence is to realize how our roles and responsibilities with respect to physical and logical security can be aligned for the greater good. Better communication of a common goal is a good starting point, and that common goal is based on defending the organization. Individual responsibility and technology can advance in tandem to promote a holistic security policy.

One quick example to stress the point is the situation that results from a stolen laptop. The device has critical digital content, sales forecasts, or customer identity information, yet it also represents a physical asset and the act of having it stolen requires a criminal investigation. Whom do you call first? Who has the ultimate responsibility to solve the problem? How can these situations be mitigated in the future to best protect and defend the company and its secrets, customer information, and ultimately, corporate reputation? The answers require a close working relationship between both groups. The security issues only grow more complex from here as we witness the merger of physical security and information technologies across global operations.

Convergence, in a word, is collaboration. Collaboration means sharing. In its most basic form, this concept, as it pertains to security convergence, evolves around shared responsibility to assure a sound defense. The first line entry in Dictionary.com for the word *defense* is "resistance against attack; protection."

This interdependence between the physical (guards) and logical (geeks) around a common goal of defending people, property, assets (physical and digital), and corporate reputation forms a common bond that needs to be communicated frequently. At the end of the day, we all need to pull the rope in the same direction for the common goal of a unified defense. The fact that each group may have different values that they place upon security from an operations standpoint is secondary. Forrester Research sees a growing convergence market where roles and responsibilities cut across both the IT and physical security domains:

> Convergence is the integration of security functions and information onto a common IP network. As regulatory compliance, protection of personnel information, asset protection, and business processes become important factors in security decisions, physical security cannot sell just to physical security managers, nor IT security solely to the IT department. The market for converged security projects is growing rapidly, and within the United States is expected to continue at an annual 118 percent rate from 2004 to 2008.

Notes from the Underground…

Axis Communications: The IP Camera Solution

Axis Communications, headquartered in Sweden with offices worldwide, has 20 years of networking and IP experience and 10 years of video and imaging experience. The company understands how networked video surveillance can drive security convergence.

Continued

In 1996, Axis introduced the world's first network camera. The main application was to serve live images and video to Web sites, a quickly growing market back then. A technology timeline is explained by Fredrik Nilsson, general manager: "Network cameras first started to take off in the educational markets in 2003, and then government became a big market in 2004, partly because of actions and funding subsequent to 9/11, but more importantly because network video was the only solution that could scale to the kind of system sizes required by the government agencies. That was especially true in city [center] surveillance where wireless can easily be used with network cameras. In 2005, retail, which is the biggest vertical [market] measured in number of cameras, started to be penetrated by IP network cameras. In 2006, Axis saw the mobile transportation market segment take off, winning very large projects in Europe, in the aftermaths of the London and Madrid public transportation bombings. In 2007, further vertical markets such as banking and casinos are expected to be next." Axis has capitalized on high-growth segments by providing surveillance technology that is leading-edge and easy to deploy in both wired and wireless environments.

IP networks are flexible, powerful, and advantageous, and they are the key to providing wide-ranging possibilities in system design, applications, and solutions. Simply connect an Axis network camera (or video server that is attached to an analog camera) directly to a computer network by wired or wireless means, and you'll have access to live video streams directly from your desktop with the use of a standard Web browser on a local area network (LAN), or from any location in the world via the Internet.

The Dallas Police Department needed a covert surveillance system that officers could easily deploy for gathering intelligence before and during drug raids. The system also needed to be completely mobile and manageable from a remote monitoring station without distance limitations. The department worked with a local Axis integrator and created a system that enables Axis pan/tilt/zoom network cameras to send video wirelessly over the existing cellular broadband network. The system uses 3G wireless technology to transport surveillance video from Axis network cameras that are hidden in the area of the possible drug raid. The Dallas PD can set up covert surveillance near any location in which a drug search warrant will be executed. Live images from the site can be monitored 24 hours a day by officers in the field, at headquarters, or at home by those who are off duty. This is an example of security convergence providing new solutions to police departments by improving officer productivity and safety, and at the same time documenting evidence for prosecution.

"Since becoming the first company to launch a network camera in 1996, Axis has remained at the forefront of the fast-growing network video market," said Soumilya Banerjee, research analyst for Frost & Sullivan. "Through consistent performance and continuous innovation, the company has been able to build and retain its leadership position."

Obviously, the challenge of market convergence, divergence, or "change," to simplify it, is not new. But it is open to multiple definitions and is therefore confusing. Immediately preceding a recent American Society for Industrial Security (ASIS) International convention, an informal e-mail poll of 25 key luminaries representing both the physical security and the IT industries was conducted. The group included manufacturers, industry consultants, publishers and editors, sales and technical channel representatives, and end users. The question posed was simple: "What is security convergence?" The answers, as you may have already guessed, were as varied as the group members' professional backgrounds. The responses ranged from buzzwords such as *collaborative partnering* and *holistic security process* to comments such as "*I wish we could just forget about using the word* convergence *because it only confuses the issue*." As difficult as the process of defining security convergence may be, we can't just leave convergence out of the mix. After all, it is the convergence within the IT infrastructure that will finally elevate both physical and logical security solutions to the forefront of enterprise defense in the new millennium.

Although the future role of security across the organization is evolving to become a much more critical component of worldwide operations, an understanding of convergence in general depends on when you want to start. The Alliance for Enterprise Security Risk Management (AESRM) describes the origins of convergence in its 2005 market survey, "Convergent Security Risk in Physical Security Systems and IT Infrastructures," as follows:

> The term "convergence" has a long and varied history. The term originates from the fields of science and mathematics. According to the Oxford English Dictionary, its earliest use can be traced to William Derham, an English scientist from the 17th and 18th centuries (best known for his effort to measure the speed of sound by timing the interval between the flash and roar of a cannon). Usage in the 19th century broadened, such as the coming together of fields of endeavor. In later years, people applied the term to wind currents, mathematical series, nonparallel lines, and evolutionary biology (Charles Darwin used the term in the 1866 edition of *The Origin of Species*).

A little history is always good; however, rather than going back to the monkey trail, we will stay within the confines of more recent history. One of the pioneering industries deploying the convergence model on a global scale has been telecommunications. The advancements in the core technologies have been unbelievable to date, and really lead to the innovative development of business models such as global supply chains and outsourcing.

Fiber optics is a good case in point. The mass deployments of the technology worldwide during the stock market boom of the mid-1990s to early 2001 were unprecedented. Competitive selling and installation strategies were in double-time mode globally. Although the cost of the technology came down, the installation footprints went up. If you listened to the marketing and sales propaganda at the time, along with industry CEOs and Wall Street analysts, you might have believed there truly was no end in sight.

Of course, you may have also invested in those companies and technologies for good or bad, depending on your timing. At any rate, the bust finally did come to pass, and a glut of worldwide fiber optics was available for pennies on the dollar. Many smart emerging economies, without the anchor of legacy systems, took advantage of the situation to deploy leading-edge communications infrastructure as a foundation for global commerce. As we already know, innovative software solutions follow leading-edge hardware advances and the stage for convergence was set. New applications answered the need for innovative and cost-effective business solutions.

One misunderstanding in the subsequent deflation of the high-tech bubble was that business applications such as e-commerce came to a halt. Quite the opposite. The automation of previously labor-dependent processes has never stopped. If anything, during the tech wreck and subsequent economic downturn, global businesses looked to take more advantage of less-expensive labor markets and use technology to drive down costs. E-commerce, as an example, has not even taken much of a rest. The oversupply of cheap telecommunications technologies such as fiber optics has promoted convergence in multiple industries, from banks to boutiques, and has impacted applications from personalized data mining to online commerce. Part of the problem with convergence in general is the fact that there are too many examples. It is so prevalent that if we don't look hard, sometimes we don't appreciate how pervasive it is. In the case of a traditional industry, such as physical security, the capability of convergence to change the business model is occurring so quickly that many do not realize it is happening. It is like a strong undertow at the beach. Everything appears fine on the surface, until you swim out a little too far and realize that the circumstances call for new thinking and an immediate response; otherwise, you'll sink.

Functional Convergence Drives Security Solutions

Just as computing hardware inventions preceded application development, the process of technology convergence is a step ahead of security solutions. As hardware becomes a commodity and operating systems standardize, it is important to put the issue of convergence into perspective. It is a process that will never stop. In order to answer the question "What is convergence anyway?" we need a simple, everyday, mass-deployed example.

"Convergence is your razor." No, not your new five-blade shaving system, your Motorola cell phone, or whatever your preferred model of mobile technology may be. This example, applied to the latest phone technology, actually works well as a definition. In a cellular phone, multiple new technologies have combined into one device and, in the process, have completely changed the concept of a 100-plus-year-old invention called the *telephone*. If you think about it, how long will it really be before some innovative marketing executive decides to rename the device altogether so that *phone* goes the way of *cassette tape*?

"Convergence is action." Considering recent technical advances, this is just the beginning. New services that we can't even imagine today will be available on our cell phones

tomorrow and most will have nothing to do with making a phone call. Convergence has allowed customers to use cell phones for e-mail, Web searches, office applications, picture taking, and video streaming. We can now spend an equal amount of airport time today using our cell phones for activities other than voice calls—all-digital, all-wireless, anywhere, and anytime. Japan is one example of a society that is embracing and advancing the use of mobile technology solutions in everything from gaming to "quick scan" payment systems. As science fiction author William Gibson likes to say, "The future is already here; it's just not evenly distributed."

The cell phone example works because anyone reading a Syngress book today most likely does not rely on a rotary phone. This example also underscores a few important trends, which apply to convergence generally. The device consolidates multiple complex technologies into a simple and compact end-user device. The device is then the vehicle by which numerous companies can create new services and solutions to sell to us. This changes another fundamental in the selling cycle because now the technology is cheap enough to deploy en masse at the consumer level. In other words, we get to suggest or develop the new products and services.

This is quite a change from the way technology was typically evaluated and deployed through the IT department in corporations and then rolled out to end-user departments. How long was it before a police officer looked at a flip phone display and realized that he could view remote video from a handheld device? Or that he could download mug shots of suspects or crime scenes? How long before he realized video clips and photos could assist in the reporting of crimes and accidents while reducing paperwork and increasing patrol time? When did the emergency room doctor suggest monitoring vital signs remotely via a cell phone to accelerate medical responses? General Motors uses the wireless OnStar communications system of automated vehicle logistics and emergency response as a value-added selling tool for personal safety and security in the event of an emergency. Consumers are also in a position of defining innovative solutions to make their professional and personal lives more productive and enjoyable. In some cases, it even results in improving public safety and actually saving lives.

The cell phone is a simple example used to emphasize how **"security convergence"** will fundamentally change the direction of the traditional physical security industry. Conceptually, we will always need to be safe, but how we ensure the safety of our people, property, and digital assets across the company and around the world will require close collaboration among all types of physical and logical security solutions and the information infrastructure. The cell phone highlights the technical timeline of basic functionality coming to market prior to a security process being established. This has been true since computing broke the boundary of the glass house mainframe mentality. Once the technology became mobile, in the form of desktop personal computers, laptops, and now handhelds, security has been in catch-up mode. The mass deployments of mobile computing devices require new and innovative security solutions to protect and ensure that this new technology can reach its full potential.

As cell phones morph into mobile computing devices, security at the end point will be increasingly critical to preventing cyber attacks. Mobile threats can take on many forms, including malware, distributed denial of service (DDoS) attacks, and fraud. Although these attacks aren't new, their capability to leverage mobile devices is. The use of mobile devices continues to grow because of their increasing utility that makes them an indispensable part of our personal and professional lives. Because of this, criminals are discovering a greater number of targets than they previously had when their sole focus was on traditional computer systems.

With the proliferation of mobile devices, today's criminals have yet another attack vector to exploit their targets. But many mobile communication providers are unprepared to address these threats. Although there is much discussion as to where security should be implemented—at the mobile device, within individual organizations, or within the mobile solution provider's cloud—most experts agree that to be effective, much of the security must be in the cloud, although a layered approach is certainly the best in a perfect world. Thus, the notion of security services provided by mobile communication providers is rapidly becoming top-of-mind as customers demand better security solutions for their mobile devices.

Mobile Malware

> Sixty percent of enterprise data will be mobile by 2006.—IDC

> …device-side anti-virus (tools) for cell phones will be completely ineffective. The most effective approach to blocking mobile malware will be to block it in the network.—John Pescatore, vice president and Research Fellow, Gartner Research

Mobile malware is rapidly evolving. It is becoming increasingly sophisticated and can propagate much faster every day. In fact, experts predict that the evolution of mobile malware will outpace the growth of traditional Internet malware. Malicious intent ranges from sabotage to fraud, and because organizations and individuals depend more and more on mobile communications, the stakes are high. A pandemic-level attack could easily and quickly impact millions of users.

Smartphones are increasingly powerful and programmable. They run on operating systems including Symbian, PalmOS, and Windows Mobile. Many have open application program interfaces (APIs) and offer a number of connectivity mechanisms through which malware can spread or carry out malicious acts, including:

- Connectivity to mobile networks, the Internet, and organizational LANs
- Symbian installation files (SIS files)
- Short Message Service (SMS)
- Multimedia Message Service (MMS)

- Bluetooth
- Wireless
- Universal Serial Bus USB
- Infrared (IR)

> We have to acknowledge that today's mobile viruses are very similar to computer viruses in terms of their payload. However, it took computer viruses over twenty years to evolve, and mobile viruses have covered the same ground in a mere two years. Without doubt, mobile malware is the most quickly evolving type of malicious code, and clearly still has great potential for further evolution.—Kaspersky Lab

These devices are typically always on and boast higher mobile network speeds. That means complex malware can propagate more quickly. In just the past year, we have seen an increase in the number of mobile malware attacks aimed at both sabotage and financial gain. Threats have mushroomed from multivector worms using Bluetooth and MMS, to cross-infection attacks between mobile devices and PCs, to the first instance of mobile spyware in March 2006. Ultimately, these attacks can lead to denial of mobile resources, information theft or destruction, and fraud.

> The number of malicious software programs created for mobile devices is expected to reach 726 by the end of 2006, up from an estimated 226 at the end of 2005, according to McAfee.

Mobile solution providers are now concentrating their efforts on telecommunications-grade solutions that can efficiently and effectively identify and respond to abuse with advanced event correlation, anomaly detection, pattern recognition, and incident response solutions. Without these solutions, mobile customers are left to fend for themselves.

Notes from the Underground…

Swisscom Mobile Fights Malware

Swisscom Mobile is the leading mobile communications provider in Switzerland. It has deployed ArcSight ESM to correlate and identify patterns within its wireless access infrastructure for the purposes of malware and virus detection.

Swisscom Mobile chose ArcSight as part of its program to provide monitoring and filters for mobile malware countermeasures. Its solution is based on

Continued

ArcSight ESM capabilities in identifying varying usage and data patterns. Risks related to mobile devices prompted Swisscom to add new dimensions to its network security by leveraging ArcSight ESM.

"Mobile malware is becoming one of the largest single risks to mobile handsets, but our deployment of ArcSight ESM allows us to protect our customers and network," said Marcel Zumbühl, head of security for Swisscom Mobile.

Prior to pioneering this implementation, the main challenge Swisscom Mobile faced was to find robust software for malware detection that performed as a telecommunications-grade solution. The company chose the ArcSight solution because of its scalable and extensible architecture and its automatic pattern detection capabilities. It also has the capability to support the largest number of disparate devices and the power to accommodate telecommunications-grade traffic volumes from Swisscom Mobile's current customer base, as well as allowing for future growth.

"The fact that we are among the first mobile operators with this type of solution to specifically target mobile malware reduces customer risk. The advanced event correlation provided by ArcSight ESM allows us to react in a timely fashion [to] new threats," stated Zumbühl.

Security Convergence Is Changing the Security Culture

A *Wall Street Journal* article dated October 23, 2006 cited a recent survey by PricewaterhouseCoopers, *CIO* magazine, and *CSO* magazine that found that 75 percent of organizations have some form of integration between physical security and computer security, up from 53 percent last year and just 29 percent in 2003. In addition, 40 percent have the same executive overseeing computer and physical security, up from 31 percent last year and 11 percent in 2003. This trend is clearly obvious to John Moss, CEO and founder of S2 Security Corp., an innovator in the development of network-based integrated physical security solutions. These systems combine access control, alarm monitoring, temperature monitoring, video, and intercom capabilities. Moss sees security convergence aligning within the larger realm of a security policy and describes convergence as follows:

> Convergence (of IT and physical security) means the adoption by the physical security market of IT technologies and methods and the simultaneous support by the IT community of physical security application requirements. I think the concept is about management integrating their physical and IT security-related policies, expertise, systems, and responses to improve corporate security and to effectively use corporate resources.

As security policy gets more attention from senior management, who have a detailed understanding of the annual costs involved within the corporate IT infrastructure, it makes sense for alignment between the physical security and IT organizations. The same cost benefits can be derived from security consolidation as any other business unit, and the additional government reporting requirements can be automated and streamlined for compliance reporting.

With more than 32,000 members, ASIS International is the preeminent international organization for professionals responsible for security. ASIS International defines convergence as "the identification of security risks and interdependencies between business functions and processes within the enterprise, and the development of managed business process solutions to address those risks and interdependencies."

ASIS feels that this definition captures a significant shift in emphasis from security as a purely functional activity within an enterprise, to security as a "value add" to the overall mission of business. This is an important observation because it essentially changes the way the concept of security is positioned within the enterprise. This impacts everything from security policy, to organizational responsibilities, to funding priorities.

One company that has displayed a knack for understanding the mission of its worldwide customer base over the years is IBM. When it comes to the security convergence market, it is no surprise that IBM's presence is the direct result of customer expectations. As Eli Primrose-Smith, vice president IBM Global Security Solutions, explains:

> We don't get into businesses lightly. Customers are asking for this. We are increasingly seeing a convergence in the market of IT security, with physical security and the need for tying it all together in an end-to-end, comprehensive system.

As IBM enters a new market opportunity that it clearly believes has tremendous upside for the long-term value add of its professional services organization, it has also simultaneously deployed a core of key technical visionaries. This advance team evaluates products and creates partnerships to align IBM with the best solutions available in the marketplace. One such self-described "evangelist" is Len Johnson, an 18-year IBM technologist who travels worldwide to craft the digital video storage solution strategy for the IBM Systems & Technology Group. Johnson sees the convergence of digital video content creating new markets in the future:

> Convergence to me equals opportunity. As the security industry transforms from being based on proprietary custom hardware with limited data access to one that is based on an open-standards-based IT infrastructure, there is huge opportunity for growth. As the actual video data moves from videotape formats to file-based formats, the opportunity to exploit this data in new and very interesting ways creates business value. The industry is beginning to recognize that the new IT-based security and surveillance solutions of today can be a mix of components from several vendors to provide the robust

> solutions needed to support new and growing uses of the video asset. Servers and storage from very traditional IT companies, [and] the video management software from companies [that] specialize in that area, are becoming the norm in the acquisition process. Video analytics and integration with various sensors are becoming almost commonplace as this software matures. By keeping video longer and using sophisticated video analysis tools, new and different trends can be uncovered. Video data mining is on the brink of being real.

You can imagine the formidable one-two punch that IBM and Cisco Systems provide when partnering in the market of video surveillance. As Johnson, the visionary, describes new application areas emerging today involving video mining, John Chambers, CEO of Cisco Systems, believes his company will impact traditional physical security vertical markets "one billion-dollar industry at a time." Cisco routers will incorporate digital video technologies. The technology will enable Cisco to bring the home alarm industry into the digital age. Indeed, the company thinks it could create a billion-dollar market for gear that transmits video from your baby's crib to your cell phone, or from a break-in to the local police station. To put it simply, the traditional security alarm business will never be the same again. In fact, in a few short years, you may not even recognize it.

When it comes to convergence between high technology and traditional security businesses, consider the recent announcement from Cisco Systems and ASSA ABLOY, the world's leading manufacturer and supplier of locking solutions. Their collaboration will result in a "networked door" that combines new Cisco patent-pending IP-based converged access-control technology with ASSA ABLOY'S door lock components featuring the Highly Intelligent Operation (Hi-O) lock-technology standard. This combined solution simplifies both the installation and the operation of badge readers, electromechanical locks, and other door security components and enforces integrated network and physical security policies. Historically, physical and network security systems have been independent and isolated from each other. Cisco and ASSA ABLOY see the value of enabling security applications to operate on a converged physical security and IP-based infrastructure.

Sandy Jones, president of the security industry research and consulting firm that bears her name, has seen numerous convergence cycles over the past two decades:

> It's a very fundamental issue, and in my opinion, convergence is no different [from] any other phase in the advancement of technology. We went through this when we integrated (or converged) access with video, and burglar alarms with fire alarms. As in the past, we are taking advantage [of] and leveraging new technologies and the world around us. And again, when we do so, [we] are disrupting current organizations, methods, means to market, and relationships.

Perhaps this last point is the key to understanding the slower pace at which security convergence is proceeding in the physical security market when compared to its high-technology peers. A legacy customer base upon which physical security solutions rest and where

product upgrade cycles are measured in six- to 10-year periods are essentially not an issue for high-tech companies entering the market. Because the physical security market has experienced convergence before, it assumes a similar pace of change. However, this will prove to be a critical flaw in business judgment because this convergence cycle involves high-speed networking technologies. The IT manufacturers and their channels entering the security business today are more experienced in managing rapid technology cycles. They are experts in moving customer bases from legacy systems to new platforms through integration projects based on productivity improvements and return on investment (ROI) calculations. In doing so, these IT vendors are positioning the convergence to new technologies as a competitive advantage for their customers. These customers are accustomed to three-year depreciation cycles on their technology investments. This may in part explain the speed at which security convergence is accelerating across the enterprise and why at the same time the traditional physical security firms tend to be slow in recognizing the pace of change, falsely assuming convergence to be five years away when in fact the cycle will be mostly completed within that time frame. In point of fact, the physical security market understands and has experienced convergence cycles in the past. However, the major problem is a misunderstanding of the accelerated pace security convergence is experiencing today due to its limited understanding of current networking technologies.

Putting the past into perspective is important when we want to get a grasp on the future. One cannot assume new convergence cycles will proceed at the same speed as former ones given the extreme advances in core technologies such as networking and storage. Twenty years from now, we will look back and realize that this new era of convergence between IT and physical security actually improved upon the common definition of safety for individuals and organizations. The increased focus on accelerating the deployment of both physical and logical security solutions across the extended enterprise will emphasize the use of industry standards and strategic "best practices." Securing everything from mobile handheld devices to data resting within huge SANs will become standard operating procedure. The installation of security software across the organization will take on a more strategic nature, rather than having multiple vendors providing similar solutions to numerous departments without the ability to share data effectively. This is simply an extension of how many corporations have already deployed software solutions across the enterprise in departments from engineering to accounting. New versions of Enterprise Security Management (ESM) software will serve as the control centers to optimize and automate network security, integrating physical security access control with video surveillance and emergency response alarms, for real-time threat management.

These changes occurring across the enterprise will improve overall security and provide a more manageable environment from which to administer a strategic enterprise policy. Once established, these "best practices" can become a benchmark by which to judge and manage third-party supply chain partnerships and promote trusted and secure relationships. The improvement of security policy, both internally and externally, will extend a competitive advantage to the corporation and support a strategy of continuous innovation through the

convergence of new technologies and solutions. The future is very bright for the role that security will play in the twenty-first century.

As security solution innovations take on a "what if" mentality, maybe that marketing executive will turn the cell phone we know today into the virtual security pod of tomorrow—the sPod, if you will. Perhaps there is a future definition for security convergence in there somewhere. It would not be out of the realm of possibility to imagine that Steve Jobs, CEO of Apple Inc., might figure out a way to capitalize on securing the worldwide supply chain. After all, the iPod already has a video, audio, and storage capability with a sub-$100 price point. How difficult would it be to apply global positioning system (GPS) and sensor technologies to the device and mount it on every shipping container on every plane, train, truck, and boat in the supply chain? As chemical compounds emit characteristics in transit, the sensors alert global positioning devices and intercept cargo prior to its intended destination. Maybe this is far-fetched and physics will allow you to miniaturize only so much; however, Apple seems to be a good example of utilizing technical convergence to enter new markets. The iPod is a great example of how a digital IP device and marketing strategy took 40 percent of Sony's handheld music market in just 18 month's time. The engineers and executives at Sony are not stupid people, yet they were looking at traditional competitors when the real threat came out of left field. It was a pure IP play, and it hit the market in months, not years. That is the power of IP digital networking leveraged with a convergence business model, and Apple lives for it. If Steve Jobs has his eye on Hollywood, why not the security market?

The point is that the coming security convergence market will introduce new competitors from places where you least expect. The ASIS trade show in Dallas in 2004 was an interesting event. Stanley Corp., a 100-plus-year-old manufacturer of hammers and saws (among other products), announced the formation of the Stanley Security Solutions Group. Fast-forward two years: It has purchased numerous companies, primarily in the physical security market, and the division is approaching $800 million in annual revenues (at last count). The company uses the following statement on its Web site to describe the Security Solutions Group: "An integrated team of twelve specialized businesses with more than 3,000 employees, 50 divisional offices, and 600 service vans, we can respond to your needs in ways no other security provider can." We can argue the future of this strategy, but this is certainly an example of a brick and mortar manufacturing company addressing a new market. However, a new market requires much more than additional bodies to provide services. That model is also changing as a result of technical convergence. The advent of wireless video solutions is only one of many new security opportunities that physical security integrators such as Stanley Security Solutions hope to capitalize on in the face of new competition from IT vendors and integrators. But will they execute?

The real question is how fast will they integrate true IP-based and wireless convergence solutions and partnerships into their business model? Time and revenue will tell. Large physical security integrators such as Stanley Security Solutions have many challenges ahead of them. Not only must they execute a merger and acquisition strategy quickly and efficiently—never an easy task—but they also must have the right combination of physical and

IT skill sets. The IT functionality side of this model is not something that Stanley Security has a business background in, hence the acquisition strategy.

This fact extends beyond Stanley Security Solutions to the entire physical security integration community. These physical security integrators must be certain that the acquired companies have new skills, and not simply more of the same from a physical security standpoint. This may be outside of their traditional comfort zone, but it is critical to long-term competitive success.

Equally important to a successful security convergence strategy is having executive-level IT sales experience, a fact often overlooked in the rush to acquire IP networking and storage-related expertise. Both of these areas, IT sales and technical experience, are not issues of concern for traditional IT integrators. The fact that the decision cycle for security products (physical- and IT-related) is migrating more toward the IT executive is a welcome benefit to the IT industry, which has been cultivating these relationships for decades. The IT vendor and integrator channel needs to acquire physical security expertise in a reverse M&A strategy to that of Stanley Security Solutions, but it has the advantage of actually requiring fewer new skill sets. Future support models will be Web-based and softwarecentric, as many problems are diagnosed and fixed in real time. There will always be a need for installation support, but many in this field will migrate their skill sets toward a true integration capability based on interoperability and ease of administration. Software will be king. IP networking and storage expertise will run a close second. The integrators that understand how an enterprise security policy aligns within the process of IT governance will be worth their weight in gold. Security is the future, but the future will look very little like the past.

The Convergence Role in Accelerating Security Solutions Worldwide

In November 2007, Cisco Systems reported record quarterly revenues of $8.2 billion, a 25 percent increase year over year, and $19.5 billion in cash and equivalents.

It has taken an industry-leading role in the security convergence marketplace. When an organization of its size and stature enters a market so aggressively and visibly, it is important to understand the ramifications on related industries. Very simply, Cisco Systems has a strategy to run all unified communications over a single IP network: one IP connection for e-mail, instant messaging, project collaboration, physical security, and private branch exchange (PBX) phones. It believes that the annual market for unified communications will reach $10 billion within three to five years. The interesting thing to note is that this is the same time frame that many executives in the physical security market think it will take before security convergence actually gets off the ground.

Steve Hunt is a leading security industry consultant and founder of 4A International. He formerly led the security research teams of Forrester Research and Giga Information Group. For 24 years, Hunt's career has spanned the breadth of the security industry: physical, home-

land, corporate, and data security. He comments on the emergence of the IT majors and their designs on the physical security market:

> Highly competitive IT manufacturers are ready to spend hundreds of millions [of dollars] to expand to new verticals, and the $120 billion physical security industry is their prime target. The optimal solution is to converge the two industries.

It is interesting to note the industry agreement that up of 50 percent of this total market is composed of traditional physical guarding services. As innovation technology is deployed in its initial stages within military applications to provide force protection technology, it finds its way to the commercial environment in phase two. This migration from military soldier to guard services will change the face of traditional physical guarding in the near future.

Guarding services is one of the oldest of the physical security professions, and it will leverage these new technologies to improve productivity. As innovations move forward to protect foot soldiers and improve their lethality, a full range of capabilities also improves. Wireless video surveillance and night vision capabilities, lightweight body armor, wireless communications, GPS and radio frequency identification (RFID) tracking, and handheld WMD sensors all become available to public service and commercial organizations to reduce crime and control fraud. These latest military technologies not only enhance their ability as first responders, but also can improve communications and accelerate training time. Additionally, these applications increase collaboration across wide areas and can be applied to securing corporate supply chains from the aspects of electronically tracking inventory and physically securing lost or stolen property.

The convergence of physical security with technology will fundamentally change the guarding services business, reducing the number of physical guards while simultaneously upgrading the effectiveness and professional skill sets of future security guard services. Professional guard services will take on a much more technical role and become embedded into the business processes of the corporation. The guarding profession will move to a model where few actual guards are employed; however, the guards will be of superior quality and effectiveness and will be relied upon for additional key services to their global clients. The ultimate image of the guarding industry and profession will be upgraded and enhanced.

The convergence of real-time, state-of-the-art technologies with security solutions changes the focus of the traditional physical and logical security businesses. This impact is huge for one simple reason: Convergence requires businesses to change, and change impacts corporate culture. This type of cultural change requires executive leadership and middle management execution. One without the other will get the organization only so far down the convergence path. The corporations and government agencies that can leverage both of these skill sets will be the winners, and they will be in the minority, but they will win very big. The major success factor in the security convergence model is accepting change as an opportunity to be embraced and not as a situation to be ignored or avoided.

Leadership and change are topics that world-famous management consultant, Peter Drucker, wrote about extensively. He authored more than 30 books published in the fields of

business management, entrepreneurship, and economics. *BusinessWeek* magazine referred to him as "the most enduring management thinker of our time." His wisdom is certainly applicable to the topic of security convergence:

> Problem solving, however necessary, does not produce results. It prevents damage. Exploiting opportunities produces results. Above all, effective executives treat change as an opportunity rather than a threat. They systematically look at changes, inside and outside the corporation, and ask, "How can we exploit this change as an opportunity for our enterprise?"

This issue of change and executive leadership was discussed in detail in 2005 at the ASIS International annual conference, where the excellent industry study, "Convergence of Enterprise Security Organizations," compiled by the AESRM and Booz Allen Hamilton, was discussed in detail. Christopher Kelly, a vice president at Booz Allen Hamilton, noted a cultural change in leadership mentality when he stated:

> Convergence is requiring our security leaders to learn much more about the business and change their perspective of their position, from a functional subject matter expert to a business person with functional knowledge.

Recognizing change as an opportunity and establishing the new structure required to embrace it is the responsibility of executive leadership. Security convergence requires collaboration between traditional IT companies and their physical security peers. In both instances, these respective organizations need each other's industry expertise. A logical step toward this mutual business dependency is partnering. However, for a partnership strategy to pay off with increased business revenues, it requires a major commitment from both parties. In fact, one of Drucker's earliest works, "The Concept of the Corporation," was a study of GM and its legendary CEO, Henry Sloan, who ran the organization for 23 consecutive years. Sloan's wisdom holds true today for companies entering security convergence alliances and partnerships:

> Strategy follows structure; you cannot effectively plan and then execute if the organization is not properly set up to begin with; performance flows from planning and execution.

We can make an argument that perhaps nothing is more important to an organization of any size than security. This would explain its roots dating back to the days of Sun Tzu. However, if we look at physical security within the context of technology and deployment of those solutions across an enterprise, they are a day late and a dollar short compared with every other department in a corporation. In fact, physical security is the last one to the party. Many physical security devices in 2006 continue to have proprietary designs and 10-year depreciation cycles, and are sold as standalone (silo) configurations. As a rule, the worldwide channel of physical security integrators continues to be more focused on traditional installa-

tion and service procedures than in learning the IP networking and technical skills required for a convergence environment.

One example is the fact that the preferred mode of video surveillance continues to be analog cameras hung off coaxial cable and requiring hours and/or days of manual labor to install. The basis of this mentality is that 80 percent or more of the video surveillance deployments today are analog cameras and that labor-intensive coaxial cable installations provide good margins. However, this reluctance to look beyond current technology and clearly see the IP future is dangerous. The situation is really no different from that experienced by the minicomputer market in the 1980s. While these worldwide billion-dollar corporations refused to accept interoperability and open systems as a business reality, they planted the seeds of their eventual demise. Today that entire industry segment is gone. *Open systems*, *standards*, and *interoperability* are new words in the vocabulary of many physical security manufacturers and their channel partners. The good news, in some respects, is that the traditional security market is not in the leadership position regarding innovation in the security convergence market today. That responsibility rests where it has historically, with the leading-edge practitioners in our nation's military community, large defense integrators, and innovative start-up companies focused on the homeland security market.

One example of a key integrator is Science Applications International Corp. (SAIC), a Fortune 500® company with more than 43,000 employees in more than 150 cities worldwide. SAIC provides scientific, engineering, systems integration, and technical services and products to all branches of the U.S. military, agencies of the U.S. Department of Defense (DoD), the intelligence community, the U.S. Department of Homeland Security (DHS), and other U.S. government civil agencies, as well as to customers in selected commercial markets.

Phil Lacombe. senior vice president and general manager, Integrated Security & Systems Solutions, explains his preference for dealing with multiple executives on the convergence issue:

> We have concentrated our business on the government side because this segment has a higher level of appreciation for security concerns. In both government and private sectors, there has been an overlap between physical and information security. It's clear from an operation or business perspective that you have to protect information and provide physical security, which means interfacing with both CSOs and CIOs.

The U.S. government has embraced physical and logical security convergence. It recently declared that all individuals accessing DoD systems must possess common access cards (CACs). These cards are used for physical access to DoD facilities as well as to information systems. This leading-edge work is providing the foundation for "smart card" technology. This initiative results from Homeland Security Directive 12 (HSPD-12), issued by President Bush August 27, 2004, which requires all federal agencies to use secure, reliable, and common ID standards for their federal workers and contractors. Eventually, more than 50 million government cards could be issued. The Lehman Brothers Annual Security Industry Report 2006 states:

> We believe that the HSPD-12 program, which will likely create a standardized biometric/RFID contact-less ID card for all federal agency government workers, appears to be the first significant reference site that commercial enterprises need to determine whether biometrics (and RFID contact-less smart cards) can work on a massive scale in the private sector. We estimate that the biometric- and RFID-based smart card market will experience rapidly accelerating growth in the next three to five years, with the key driver being government-driven initiatives mainly via the HSPD-12 directive.

In fact, security and its issues are important enough that the government is extending its reach into the entrepreneurial community. The CIA actually has its own internal venture capital fund, In-Q-Tel (*www.in-q-tel.org*), headquartered in Virginia and well positioned on Sand Hill Road, in the nexus of Silicon Valley's venture capital neighborhood. In-Q-Tel is looking for new products and solutions that will provide value to the agency first, and then extend profitability into commercial markets. In-Q-Tel was established in 1999 as an independent, private, not-for-profit company to help the CIA and the greater U.S. Intelligence Community (IC) to identify, acquire, and deploy cutting-edge technologies. To date, the firm has generated more than $1 billion in private sector funds to support technology for the CIA and the IC.

Another leading firm is Paladin Capital Group (**www.paladincapgroup.com**), a private equity investment company based in Washington, DC. Paladin's Homeland Security Fund is focused on investments in existing companies with immediate solutions designed to prevent harmful attacks, defend against attacks, cope with the aftermath of attack or disaster, and recover from terrorist attacks and other threats to homeland security. Two principal players in the firm are retired Lt. General (USAF) Kenneth Minihan, former director of the National Security Agency (NSA); and James Woolsey, current partner of Booz Allen Hamilton and former director of the CIA. These are two examples of leading-edge strategies to deploy advanced technologies into government agencies, which will then migrate to commercial businesses for mass deployments.

As we examine the impact of technical convergence on the physical and logical security disciplines, it is important to understand how corporations have addressed it to date. The consolidation of standard business applications and processes across worldwide IT infrastructure is nothing new to major corporations. Consider the finance department for a moment. How confusing would it be if every department had a different accounting software solution deployed over proprietary networks and databases unable to share information? A separate vendor for each remote location would also support each department. What a mess; no one would be paid on time or consistently.

The truth is that this scenario is not far off the mark when examining physical security installations of video surveillance and access control, or the numerous copies of multivendor security software for antivirus and intrusion detection deployed around corporations today. Security convergence needs to collapse and consolidate this multivendor silo approach to security solutions and replace it with the standards-based open and interoperable advantages

that other departments in the organization already enjoy. In doing so, not only will the deployment of security gain exposure and recognition across the enterprise, elevating the stature of all security practitioners, but also in the process, it will return the ROI the executive staff is looking for in justifying enterprise security policy.

One example of where the security department can turn to benchmark a process is the engineering department. More than 20 years ago, vendors designed and sold the first iterations of 3D computer-aided design/computer-aided manufacturing (CAD/CAM) software. The idea behind it was to consolidate engineering brainpower and collaborate to stop reinventing the wheel, literally, in different design departments across the organization. This powerful software would improve upon 2D design functions and replace existing drafting tables. The productivity improvements would be off the charts as the cumulative brainpower of engineers from across the corporation and around the world focused on improving productivity by automating the process of product design. Certainly, this technical leap was not an easy change, but it was well worth the effort.

The two constants that always involve most new innovative solutions is the impact on network bandwidth, always at a premium, and organizational change. However, think for a moment where organizations would be today if they let technical and business change remain stagnant. The fact is that network bandwidth is one of several technologies (CPUs, semiconductors, storage) that continues to advance to meet the demands of new solutions. And change is another constant. Change is always a major impediment to deploying new tools and solutions to established concepts of work because human beings are involved, and our first inclination is to resist it. Some folks on the final lap of a career oppose change simply because it is change, and therefore, they are averse to learning anything new. This is a management issue. Most of us come around, or there would still be a market for rotary phones. Today, could you imagine the design process in a major corporation still being accomplished on drafting tables, or software development being done without collaboration?

The same way engineering management collaborated with the IT department to deploy a worldwide design process to improve productivity is how both the physical and the logical security departments need to approach their relationship with IT regarding convergence. The goal is to embrace the IT department as a trusted partner in the deployment of security solutions across the infrastructure and in alignment with the stated security policy of the corporation. Security needs to become a customer of the IT department, not an adversary. In this way, a partnership can develop based on the mutual need to protect the assets of the corporation. By attaining "customer" status within the organization, the security department becomes similar in function to other corporate entities such as engineering, finance, and sales, in that the performance of the security group's function depends on professional and timely support from the IT organization. In this way, the potential for the IT group to block the deployment of security solutions (such as video surveillance) because of concerns over network utilization can effectively be neutralized in favor of deploying an enterprise security policy within the IT infrastructure.

Security is better positioned to attain its goals and elevate its stature by becoming a demanding partner, rather than a political opponent to the IT organization. By tying the

physical security department's success to the IT group's ability to support the operation, a win-win scenario is established and a true partnership can flourish. This does not mean security gives up decision-making responsibility; it means the IT department becomes a support partner in security solution deployment. Only then can security truly enjoy the value and productivity advantages that technology brings to the process. Can you imagine the ROI calculation a company realizes when its engineering or development resources worldwide can follow the sun and continue to work on product design or software development projects 24 hours a day in an integrated process that eliminates redundant effort? Now apply the same model and thinking to physical security applications such as a common identification and access control card, or video surveillance. Open systems and interoperability need to standardize on applications, training, vendors, and digital formats enabling data delivery, development, search, and alarm notifications. In the security realm, time and money calculations aren't all that matter; this convergence can result in protecting a corporation's reputation or brand as well as saving lives. Sometimes the most critical variables are the most difficult to calculate with a standard ROI model, or measure with a performance metric. How do you put a dollar calculation on someone's life?

The impact of this convergence of information technologies in the development of numerous industries and general process improvements has been clear over the decades. However, in today's global threat environment, there may not be an industry more critical to the future than that of security:

> The farther backward you can look, the farther forward you are likely to see.—Sir Winston Churchill, statesman

Look back over the timeline of technology and you will see many examples of high-tech companies succeeding and failing at recognizing and adapting new technical trends to their existing business models. The successful companies identify customer need and respond. The failures are slow to let go of the old cash cows.

The minicomputer industry once dominated Route 128 in Massachusetts. Today those billion-dollar firms are out of business. Why? No interoperability outside of their own proprietary operating systems. I guess they figured it just was not important. When it came to a new "open" operating system called Unix, one minicomputer icon, Ken Olsen, founder and CEO of once-mighty Digital Equipment Corp. (DEC), referred to it as "snake oil." The sight of 90 percent margins on DEC's proprietary operating systems blinded perhaps Olsen, and the entire minicomputer industry. Change is rarely comfortable, but neither is extinction. However, when you examine the rapid changes that new technologies cause to industries, companies, their partners, and customers, you see the key role that leadership plays in the success factor. DEC did not have it when it needed it most. IBM did.

Consider the history of IBM over the past two decades. IBM was once a huge dominating mainframe company, and the old phrase "You never get fired for buying IBM" was alive and in practice among the largest corporations worldwide in the mid-1980s. Things were very good for a very long time at Big Blue. The problem was that the company that

manufactured leading-edge technology did not do a very good job of considering how its products worked outside of its own internal universe or within its own product family. A stubborn attitude and lack of innovative vision crept into the once-proud organization. As a result of this cumulative effect on its products and culture in the decade of the 1980s, IBM lost its way. In fact, by early 1993, some industry pundits actually started counting the months until IBM would go out of business completely.

What was once thought to be an impossibility was fast becoming a potential reality. IBM had to do something different, so for the first time in its history, it went "outside" for a CEO. An industry outsider, Lou Gerstner, with a background at companies including RJR Nabisco, American Express, and McKenzie Consulting, took over as CEO and brought IBM a much-needed customer perspective. As Gerstner explained in his 2002 book, *Who Says Elephants Can't Dance?*, he demanded to know why (as a customer spending tens of millions of dollars with IBM annually) the product line had interoperability issues both internally and externally. He saw IBM's core problem as a customer satisfaction issue and he wanted the situation fixed. As a result, the IBM Global Services Group was born. More than any other division, it saved IBM and today generates more than $50 billion in annual revenues. New thinking created a new division, which in turn saved the company and created a lucrative IT services market industrywide. This vision leverages new technologies to promote collaboration for continuous innovation across all industries. In fact, the IBM services model may be the best example yet of using convergence to execute an integration services strategy.

To quote Lou Gerstner, then ex-CEO of IBM, during an address to the Harvard Business School in 2002, "Transformation of an enterprise begins with a sense of crisis or urgency. No institution will go through fundamental change unless it believes it is in deep trouble and needs to do something different to survive."

This might also serve as the best possible advice to the physical security industry and its IT counterparts regarding convergence. September 11, 2001 was the wake-up call that changed the definition of the security business. Today commercial industry is too slow to embrace security convergence in a significant way and we are less prepared than we should be. A lack of technology is not the issue in solving the problem. A collaboration of effort around the concept of establishing a "mutual defense" is required. Both physical and logical security expertise needs to be leveraged across standard IT infrastructure and platforms within an enterprise security policy that highlights "defense" as a common bond and promotes "best practices" among trusted partners. Thankfully, the military complex with its large research projects and defense integration community is leading the way in technical innovation, which at its core is a convergence strategy.

We have heard many times that security professionals are conservative by nature, that security is too important to constantly risk upgrades to new and unproven technologies. After all, lives are at stake! However, technology also changes the nature of traditional security practices. It is unfair to suggest that the traditional physical security market does not have its share of visionary thinkers and innovative practices. An early example of a traditional physical security industry utilizing technical convergence is the New York Police Department (NYPD) of the early 1980s.

Although physical security has been around forever and expertise is fundamental to everything we do, successful security convergence is not all about IT driving change and taking the leadership role in transforming business operations. Mutual respect for both groups' talents is a basis for successful convergence. The 1998 book *Turnaround: How America's Top Cop Reversed the Crime Epidemic* highlights how then-New York City Police Commissioner (and now Los Angeles Police Chief) William Bratton pioneered an early vision of security convergence strategy. In doing so, he significantly reduced both overall felonies (50 percent) and the city's murder rate (68 percent) in only 27 months. This success landed him on the cover of *TIME* magazine and is a great example for both physical security and IT departments regarding how collaborating on security convergence can return unbelievable results.

The now famous system, known as COMPSTAT, represents an innovative process of integrating IT systems with real-time police procedures. It was the first IT-based (DEC) system to utilize geographic information system (GIS) software to map near-real-time crime patterns with arrest statistics to determine patrol activity. It aligned police resources with automated crime pattern data, right down to a square-block area and time of day. Equally important is that the system drove collaboration among the multiple precincts and various departments required to guarantee success. This cooperation actually led to a change in the culture of the NYPD. People in this large organization had to think differently about how to do their jobs and embrace new technology:

> We did things a certain way because we had always done them that way. We had to banish the phrase "we have always" from our vocabularies. We had to start asking "how should we do it?" and "how can we do it better?"—John Timoney, formerly New York City first deputy commissioner and currently Miami police chief

One thing we all realize about the future is that there are no guarantees. The security convergence wave will carry some companies to the crest of new heights and will wash away others in a tsunami of missed opportunity. The difference will be time to market. Speed is the critical component to a successful convergence strategy, and yet this is the vital element that the conservative-thinking security industry tends to overlook. This cultural deficiency in physical security companies opens the door of opportunity to the IT industry where innovation and business change are embedded in their corporate cultures. The first phase of security convergence is collaboration through partnering—taking the valuable skill sets each respective industry has to offer to combine them in a better system and process for securing the defense of people, physical and information assets, and corporate reputation. The key ingredient is to recognize where the industry is heading and to position partnership opportunities accordingly.

Security Convergence Is Changing the Sales Channel

When hockey great Wayne Gretsky was asked about his game strategy, he replied, "I skate to where the puck is going to be." He could see the ice and anticipate, based on experience, how things were going to unfold. By positioning himself in the right place to succeed, he broke every scoring record in hockey.

There are similarities between sports and business history. It seems that the greatest players, teams, CEOs, and corporations rise to the challenge of changing environments and leverage new opportunities to their advantage. Andy Grove, founder and former CEO of Intel Corp., is a case in point. He is one of the true pioneers of Silicon Valley and is a high-tech industry icon. He has decades of experience in addressing technical convergence issues and is keenly alert to major trends:

> I'm a great believer in, particularly, being alert to changes that change something, anything, by an order of magnitude, and nothing operates with the factors of ten as profoundly as the Internet.

In today's environment, several technology areas are promoting major changes which are impacting the future of security convergence. IDC research tells us that today, worldwide Web-hosting revenues exceed $20 billion annually, wireless communications represents an annual market greater than $46 billion, and the revenues from Linux open source software development will grow from $15 billion in 2006 to more than $37 billion in 2008. In summer 2006, laptop sales surpassed those of PCs for the first time. These trends point to the development of next-generation applications hosted on wireless devices accessing real-time search engines and databases. GPSes, sensors, and open source software will provide instant video, voice, and data services over IP. They represent just a few of the "Big" changes that will change something "Big" in the security convergence model moving forward. These new technical breakthroughs will be critical to new-product development to answer the threats of "extreme" corporate risk scenarios.

The future belongs to companies that correctly anticipate trends and quickly respond to new business opportunities by creating partnerships. As technology advances, it becomes impossible to have all the expertise required in-house. The ability to develop solutions to customer problems through collaboration with partners is what drives a successful convergence business model. The fact is that large IT vendors require a limited scope of partnerships. The rationale is that as the largest IT manufacturers enter the security convergence market, they need to partner with perhaps only 20 percent of their physical security industry peers to be successful. This partnership strategy is based on accelerating their own time to market to aggressively compete against other IT manufacturers. IBM worries more about beating HP to the security convergence market than it does that Honeywell will be too formidable a competitor over time. As mentioned earlier, the traditional physical security market is late to

address the convergence opportunity through partnerships. Additionally, these IT vendors are focused on emerging software firms developing open system solutions and leveraging technical trends to deploy wide area security solutions. These huge IT organizations (Cisco Systems, IBM, HP, Microsoft, Oracle, and EMC) already have worldwide sales and support organizations, leading-edge research and development staffs with plenty of cash on hand, and established end-user relationships at executive levels. Security convergence to the IT industry represents a new, high-growth market opportunity that aligns nicely with the technology sweet spots of enterprise infrastructure, new innovative solutions, and integration services.

The Pareto Principal originated in 1906 from Italian economist Vilfredo Pareto's observation which essentially said that 20 percent of the wealthy owned 80 percent of the land. It has been modified through the decades, and today we understand it as basically that 20 percent of the people/tasks are vital and the remaining 80 percent are trivial.

This principal also accurately reflects the current and future states of the security convergence market. The largest vendors on both sides of the convergence model are deploying strategies around security convergence. Five years from now, 80 percent of the traditional physical security vendors, large and small, and their channel partners will be marginalized or out of business. They will be displaced by the accelerated focus on open systems, standards, and ROI models being promoted by IT vendors and increasingly being purchased by their decades-long contacts within IT and senior management. Major IT vendors control the enterprise purchase cycle. Agree or disagree, the funny thing about the 80/20 rule is that basically everybody thinks they are in the top 20 percent. This, of course, is impossible.

Large high-technology vendors have executed a business model of introducing new solutions to improve their customers' business practices while simultaneously upgrading the infrastructure to allow those new solutions to operate effectively. It is no surprise that the voice, video, and data over IP strategy that Cisco deploys will require more bandwidth and networking gear. Or that the security surveillance and video mining applications that IBM promotes will require large IBM blade server configurations and multiple terabytes of storage. Network bandwidth, storage, CPU, cache memory, whatever the problem, IT vendors and their huge sales channels have an upgrade strategy for it. One key point is that this is predicated upon a three-year product depreciation cycle, by which the IT industry sets its internal clock.

Along the way, the IT vendors have even assisted in the creation of new technology positions and career paths within their client organizations. Network, storage, database, and system administrator positions have provided a promotional ladder to vice president titles and CIO positions. This personnel situation evolved over decades and provides IT vendors a unique selling advantage in regard to product evaluations, requests for proposals, and ultimately, purchase decisions. This position is enhanced as more responsibility for security solutions migrates toward the CIO organization in search of a senior-level executive to drive policy across the executive ranks. Whereas the IT industry vendors aggressively compete with one another in this environment, this sales cycle is new to the traditional physical security vendor. With the decision point moving toward the IT department, these security vendors need partnerships not just to collaborate on solutions, but to leverage these IT partner

buying relationships. Enterprise security policy is focusing on alignment with and deployment over the worldwide IP network and IT storage infrastructure.

One important aspect to successful partnerships is having some resident support expertise in the basic technologies behind networking and storage. This is a major credibility factor in securing a revenue-generating partnership in phase one. However, far too many organizations ignore the initial phase of hiring resident expertise in the physical or IT discipline to provide the needed experience required for successful third-party collaboration. This is a fundamental lack of understanding of the mutual benefit behind successful partnering. Collaboration is more than sharing industry expertise. It is the equal distribution of resources dedicated to bringing in the business. If your initial attempts to recruit meaningful partnerships expose a lack of resource commitment, it is a direct reflection upon a lack of genuine interest on the part of your executive management. Convergence success requires leadership and commitment to new markets and new resources. At the end of the day, strategic partnerships will provide the opportunity for large enterprise deployments of security solutions. This increases the visibility of security and brings the value of security convergence into clear focus for the senior management of the company.

We care about security convergence because it represents a huge market opportunity in a critical area that is virtually untapped in regard to leveraging information technology across wide area networks (WANs). The physical security industry is currently transitioning from a historically analog infrastructure to the new IT infrastructure based on IP. As the earlier cell phone example illustrates, we are just in the beginning stages of understanding how powerful, miniature computing devices, mass-deployed and hosting new and yet-to-be-invented solutions, will be deployed. It is a truly exciting time to be at this apex of security convergence—perhaps just in time to secure people, property, and assets from the increasing threats of fraud, violence, and terrorism being confronted on a global scale.

In general, security convergence plays to the strengths of the IT industry: buying relationships, infrastructure understanding, faster product development cycles, better sales organizations, and innovation embedded into a corporate culture. Technical convergence has an established track record across most of the internal departments in the corporation. Although these statements point to definitive advantages of IT as an industry and department within a corporation, one fact is clear: Security can turn to these inherent advantages to leverage and accelerate security policy across the organization.

Just as the buying requirements for security solutions are changing from independent departmental installation(s) and/or standalone (silo) island mentalities, the actual number of vendors combining to answer enterprise requirements is increasing. Cross-industry partnerships and merger and acquisition activity are becoming normal operating procedure for companies that want to quickly capitalize on security convergence. Examples of these fundamental "channel changes" are occurring every month and have been accelerating throughout the 2006 calendar year. Significant industry changes will continue as major IT vendors pursue opportunities in the security market. Large physical security manufacturers and integrators will need to quickly adjust go-to market strategies and product plans in order to compete against new IT-centric competitors. The convergence of video-based solutions over

IP networks running data and voice applications is expanding the requirements for bandwidth, storage, and integration services.

These primary business drivers are the focus of continued entry into the traditional physical security market by IT vendors and their sales channels. The IT market's historic tendency toward centralizing enterprise solution and support models will fundamentally alter both security installations (physical and logical) and buying requirements. Examples of competitive positioning to address these new market opportunities have been accelerating throughout the 2006 calendar year. For example, these headlines occurred between April 17 and April 21, 2006 and appear here exactly as they appeared in the press. They are in no particular order of importance, but they all have an impact on the security industry:

> "Cisco to invest US $16 million in Video-Encryption Company WideVine Technologies"
>
> "GE Security selects Sun Identity Management Suite to deliver combined IT/Physical access solution; OEM relationship to deliver seamless security solution for Fortune 100 companies and Department of Defense"
>
> "Tech Data U.S. Helps IT Resellers Break into Physical Security; Physical Security SBU Established and Leading Manufacturers Signed"
>
> "Big Brother Goes Digital" (industry cover story)

Let's review:

- A major IT gorilla, Cisco, continues to buy leading-edge technology firms in the sweet spot of the physical security market. This trend continues.
- A former, yet still formidable, IT gorilla, Sun Microsystems, is partnering with a major physical security provider, GE Security, to establish OEM ties and sell solutions through mutual channels to Fortune 100 and large government agency accounts.
- One of the largest IT distributors worldwide, with a $20-plus billion business and more than 90,000 customers, has established a security convergence business unit (SBU) to assist IT integrators in selling physical security products.
- The cover story in *VARBusiness* (a leading publication for IT value added resellers) warns its large IT integrator subscriber base not to miss the new and growing opportunities that security convergence offers their businesses.

Although one week in April 2006 was a good indicator of vendor activity around security convergence, it was hardly vacation time during the summer months:

- In August, L1 Identity Solutions was established as a business entity resulting from the combined acquisitions of biometric software players Viisage Technology, Identix Inc., Integrated Biometric Technologies, SecuriMetrics, and Iridian. L1 Solutions has a market cap of approximately $1 billion.

- Also in August, IBM announced a $1.3 billion acquisition of Internet Security Systems Inc. (ISS), a publicly held firm based in Atlanta. ISS products protect against Internet threats aimed at networks, desktops, and servers and are installed in more than 11,000 worldwide companies and governments. This purchase effectively launches the Global Services Security Division into the managed security services business.
- In September, EMC Corp. completed the purchase of RSA Security for $2.1 billion and announced a $150 million acquisition of Network Intelligence. EMC's chairman, president, and CEO, Joe Tucci, announced, "The additions of RSA and Network Intelligence to the EMC family enable us to execute on our informationcentric security strategy to help organizations around the world secure their information throughout [their] product life cycle and reduce the associated cost of regulatory compliance."
- Finally, as we enter fall 2006, Siemens Building Technologies decided to get into the act as well. It purchased VistaScape Security Systems, a leading developer of automated video analytic technology software designed to protect critical infrastructure from a broad spectrum of threats. Terms of the deal were not disclosed, but the strategic intent is obvious.

What the headlines reflect on a continuous basis is an industry convergence between physical security and IT that is simultaneously changing the competitive landscape. New roles and responsibilities within major corporations are changing the traditional purchasing cycles for security products and impacting vendor-selling relationships. A new era of collaboration is accelerating the trend in cross-industry partnering.

In addition to this, an active merger and acquisition cycle is evident in the physical/logical security industry. As Dennis Moriarty, senior vice president for Diebold's Security Division, states, "The new formula is to purchase for expertise, not simply scale."

All of this change points to a need for substantially upgrading to new skill sets across organizations within both industries to accelerate deployment of a consistent security policy across the enterprise. Although cultural differences between physical security and IT continue to exist, executive management demands cooperation in providing a cost-effective security solution. This fact is not lost on either department. Whether the solution is video surveillance, access control, or the broader area of enterprise security management, security solutions now cross multiple corporate departments and require collaboration. The career-limiting decision for department heads now is *not* collaborating. With the merging of business interests (and budgets) among the traditional security organization, IT, finance, and just about every department in the company with a security concern, the ability to promote cooperation and mutual interest is a key management talent. By demonstrating an understanding of the larger security issues facing the overall business and detailing a compelling ROI, a security policy can become a value add to the corporation.

The age-old problem with this model is that the centerpiece of the strategy is change. History tells us that organizations steadily and sometimes staunchly oppose anything new. In this business environment, your executive leadership and middle management win the business battle. In the era of security convergence, the winners recognize industry change early and execute new strategies quickly. This new era in the security market is occurring during an unprecedented combination of advancements in technology and a continuous global focus on world events which are altering the traditional definitions of corporate risk. The early stages of the twenty-first century are positioning security as a priority issue for government agencies, commercial enterprises, and individuals alike.

Summary

Today the world faces what James Canton, Ph.D., CEO and chairman of the Institute for Global Futures, refers to as "an era of extreme threat." He states, "An entirely new definition of risk is emerging, made up of a totality of threat factors, from collaborative global networks of terrorists and organized criminals, to cyber attacks and identity thefts." His conclusion is that the "smart technologies" such as video analytics, biometrics, nanotechnology, and mobile robotics will play a vital role in securing the future. It appears that the convergence of physical and logical security is only in phase one. The only constant will be change in the security industry.

This is essentially a new state of security where organizations must prepare against the real possibility of a major terrorist attack against our country and economy (read supply chains) while simultaneously our traditional risks to people and assets (physical and digital) are rapidly increasing. Our security risk is compounding annually. It is against this backdrop that security convergence is critical. The problem is that the physical security and IT industries are not collaborating to bring the best security solutions to market as quickly as possible. As large security initiatives move from big government projects (smart cards) to large commercial enterprises, leading-edge vendors see convergence offering huge opportunities. This means partnering to combine skill sets. It also means IP takes center stage because the fastest way toward mass security solution deployments is over a common worldwide networking infrastructure.

As ASIS concluded in the Convergence of Enterprise Security Organization's report (November 2005): The increasing focus on security from an enterprise perspective has led to a new way of examining risks that institutions face as a whole. This, in turn, is leading to innovative approaches that emphasize integration—specifically, the integration of the risk side of business into the strategic planning side in a consistent and holistic manner. The surveys and interviews presented clear evidence that as leaders in the business, security professionals need to move from a "command and control" people model to an empowering and enabling model, and develop an enterprisewide view of risk rather than an asset-based view.

In attempting to define security convergence, we have essentially opened the proverbial "can of worms." The definition does not fit into one easy sentence or clean paragraph. On

the one hand, security and convergence both have long-established histories, and yet this new era of "extreme risk" changes the timing of how we prepare and respond to these new global challenges. In order to keep pace with these threats, whether they result from internal/external hackers, traditional retail theft, acts of nature, or deliberate terrorist attacks against our citizens and economy, the new order of the day is an accelerated security risk policy across the organization and outward to trusted partners and suppliers. Security convergence requires a baseline of communication and agreement within all of the organization for a shared responsibility to the concept of defense.

New corporate organizational charts are being created as security policy becomes the issue of the day for executive staff and shareholders alike. Leading-edge security technologies migrate from government-funded defense agencies and their integration channels partners, as well as presidential directives, into the commercial marketplace where significant installations are pending. This creates a competitive advantage for commercial organizations worldwide as security policy across the enterprise is positioned as a measurable business value.

The answer to the question "what is security convergence?" may ultimately be as personal as your sense of security. But one thing is certain: It is not business as usual in the security industry moving forward. The physical security community needs to accelerate its embrace of enterprise technologies from IP networking to mass storage strategies and all the solutions in between. The security software vendors need to streamline application deployments and provide better interoperability and management tools to improve administration support across enterprise networks. The new threat landscape envelopes the entire corporation and its third-party partner networks. Finally, the people factor is the most critical ingredient to success. The new era of securing an enterprise and establishing trusted external relationships requires collaboration, innovative thinking, and above all, leadership. New corporate structures to support new business models will mean new skill sets and new thinking. All of this revolves around cultural change within the organizations that will ultimately win in the age of security convergence.

Just as network technology spans the global workforce today, security convergence will expand to involve numerous stakeholders worldwide with various levels of security involvement from executive decision makers, to partners and customers, and eventually impacting shareholder decisions. Technical convergence will propel enterprise security into a leadership role in the years ahead. This is an exciting time for security practitioners and IT professionals alike, as they create new solutions to answer new challenges.