

When former IBM CEO Louis Gerstner, Jr. began his quest to turn around the once-troubled company, he asked an auditorium full of corporate customers what he could do to help them manage their businesses and technology platforms better. Someone from the back called out, "Slow it all down!" The group exploded in knowing laughter. Gerstner smiled, too, paused a moment, then said, "That's the one thing I can't do!" And so it goes with today's security landscape.



Eight Trends That Will Shape Security in '08

SUBMITTED BY ADT SECURITY SERVICES

If anything, changes in our industry will only accelerate in 2008.

Keeping up with it all in 2008 and beyond will be a tall order. Here are eight trends to keep in view:

1. IP VIDEO SURVEILLANCE

IP is one of those bedrock technologies that has truly changed the world. Not only did it provide the basis of the Internet, but by helping to join together other technologies, it has enabled a host of other applications such as IP video.

In recent years, telecom service providers worldwide have pumped mountains of capital into IP video for communications and entertainment

revenue purposes. Cable companies will eventually follow suit because of IP's inherent cost-efficiencies as well as its media-blending capabilities. Enterprises, meanwhile, have also expanded their IT network capacities to Gigabit Ethernet in the core, with 100 Mbps to the desktop. And 4G wireless data network architectures will become more symmetrical, so upstream bandwidth speeds are comparable to downstream ones.

All these, plus advanced quality of service and dynamic encryption, are helping to bring IP video to security applications. In fact, comparative studies show that the total cost of ownership of an IP video surveillance system can average 35 percent

less than an analog/DVR solution in deployments exceeding 50 cameras. Meanwhile, advances in video compression technologies are helping to conserve both bandwidth and storage requirements, although prices on these two commodities continue to drop with no apparent end in sight.

IP video is the next step in surveillance's evolution. It can leverage a company's IT infrastructure for video control, transport, storage and retrieval. As such, it can be centrally managed from anywhere in the world - even through a web browser in a Kathmandu Internet café. It can serve security and other business purposes such as process or traffic

controls. It can also provide data for business analytics like emerging retail applications that are starting to help optimize store layouts based on analyses of store traffic around merchandise.

2. IP ACCESS CONTROL, WITH BIOMETRIC OPTIONS

Most of today's access control systems share a common architecture: badge readers connect to a local controller, which then connects to a head-end server. Tomorrow's systems will dispense with the "middleman" controller. IP-enabled readers will communicate directly — wired or wireless — over a company's IT infrastructure to a central server or servers.

What is game-changing about this technology is its scalability, both up and down. For large, distributed enterprises with thousands of readers, the operational savings are obvious. But for the first time, IP access control will become

economical for small and medium businesses, even for homes.

Add to this scalability is the fast pace of biometric developments. Long-heralded techniques such as fingerprint, iris and voice recognition coupled with single sign-on capabilities are coming to the fore. That is because personal password libraries have grown so large as to become unwieldy and the passwords themselves increasingly defeatable. In addition, falling prices will make these systems and their applications much more economical.

3. PHYSICAL & LOGICAL SECURITY CONVERGENCE

As it relates to physical security, convergence takes two forms. Just like the examples above, one form applies information technology to physical security solutions to extend their reach. Consider today's advanced sensor technologies: When used within pervasive low data-rate wireless mesh networks, much more robust and granular sensing at the edge can occur. Other examples include the ability to tie into business environments such as building control systems and HR applications to build more highly integrated and effective solutions.

The other form of convergence is the meld of logical security — its information systems and data — with physical security. Bringing these together lets security be managed more holistically instead of in silos. Safeguarding sensitive data and fighting the rise in identity theft require both logical and physical security experts. Interestingly, this phenomenon could also spur new competitors from the IT security world into the physical access control space.

4. TRACKING ASSETS & PEOPLE

When shoppers walk Wal-Mart's aisles, they see vast expanses of low-priced goods. The reason for these low prices is that Wal-Mart itself sees not goods but data, which it manages better than any other retailer in the world, sharing with its customers the savings from both its best-of-class procurement practices and operational efficiencies.

Once upon a time, security was all about protecting these types of goods as well as people. What is changing fast is the means by which it is done. More and more, controlling assets and access is a matter of tracking them, not just responding to after-the-fact events like loss alarms. Technologies like RFID, GPS, and even cellular triangulation can track assets and people, in effect providing a data "presence" for either. This can be useful both in real-time and, because it is recordable, in forensic applications as well.

5. DATA ANALYTICS

With powerful software tools, companies can mine both security and business data for hidden patterns that can help uncover both risks and opportunities. Anomalies can indicate security violations or insecure environments vulnerable to violations. They can also determine probabilities of various market behaviors or situational outcomes. Retail data analytics are gaining traction in that market, but the tools are applicable in any security environment generating data flows.

Overall data analytics can make security operations much more predictive and, therefore, proactive. They can also open doors for security



▲ Author: Nick Samanich, Director, Commercial Product Management, ADT Security Services, Tyco International

professionals to conversations in parts of an enterprise that might have seemed frontiers to them not too many years ago.

6. DISTRIBUTED SECURITY & MANAGED SERVICES

Traditionally, security has been largely premise-based and geographically bounded. As the IP-driven convergence of physical and logical security continues, these constraints continue to be stretched, even broken — yet security remains intact, if not enhanced. Two technologies are helping drive this change toward a distributed security model: the Internet Protocol version 6 (IPv6) and unified communications.

Under the current IPv4 specification, our world has been quickly running out of available IP addresses, as just about every electronic device from the fuel injectors in your car to the toaster in your kitchen seeks Internet connectivity. IPv6 provides virtually unlimited number of IP addresses for devices of all kinds, including those equipped with next-generation biometric authentication and validation.

IPv6 will also help unleash unified communications, a big trend in itself that combines PC and phone capabilities. Through a single interface — which could span multiple devices, including your PC at work or home, your PDA, your TV or any other networked device — users can access voice, data and video for communications, information, entertainment or some mix of the three. And, thanks to high-speed, wireless packet networks, they can get all this while on-the-go. In 2008, we will see the emergence of a new and important feature into unified communications:

the security credential.

Distributed video security services is one example of how the extended security model can play out. Over a secure network, video inputs from many sources — in-building, in-vehicle or on-the-street — can be centrally managed from a video management server controlled by command center. The command center can relay visual output in real- or non-real-time over wired or wireless networks to the PCs, cellphones and PDAs of those who need to know, also providing relevant analytics and alerts.

An obvious derivative of distributed security is third-party managed security services. These reflect the classic outsourcing model ranging from assigning an outside provider some services such as badging and access control management to allowing a full assumption of a company's security operations.

7. POWER TO THE PEOPLE!

Ironically, protecting small and medium businesses as well as homes has largely left out a central character in the security environment: the customer. Typical security systems today stand sentinel, ready for an alarm event, rarely engaging customers except for activation or deactivation. That should start to change in 2008, especially given trends in physical and logical convergence as well as in distributed security just mentioned. In effect, customers become “users” of security services instead of bystanders.

In emerging integrated security environments, users can gain access to all sorts of security resources. These could include those of their service provider, their fixed home systems, extended home systems in their cars or carried with them, and third-party data sources providing news alerts, weather advisories and



▲ Safeguarding sensitive data and fighting the rise in identity theft require both logical and physical security experts

other trends important to them.

An extended home system, for example, could provide school notifications and community alerts while users are away from home. For small and medium businesses, owners and management could see, both literally and figuratively, what is going on in the front-office, back-office, warehouse and as many points in-between as desired. Eventually user-defined data analytics can help show security vulnerabilities, too.

To access and control the features of their security environments, business and home users can log into secure, web-based client portals. Software wizards can help them define specific rules to automate responses to threats or events as appropriate — via the rules or in real-time.

8. GLOBALIZATION

Going back centuries to Marco Polo if not before, globalization has exploded in the last 30 years as China opened its markets, India came of age, and other developing nations joined international agreements to lower or eliminate barriers to trade.

Despite the race to globalize, a company's security has stayed mostly a local matter. That is because of the maze of building compliance codes — both in-country and from country-to-country — along with provincial technical solutions. To date, managing security on a global scale has been difficult if not nearly impossible.

That is changing fast, however. Now more and more multinational corporations are taking a global

approach for many reasons. One is to control their risk profile better. Others are to improve safety, security and business efficiencies through greater consistency and simplicity.

AND ONTO 2008...

Year 2008 promises to be a watershed year for the security field. Business imperatives along with technology developments will continue driving change. Even more, both drivers open doors of opportunity for security professionals to engage their enterprises at higher organization levels and across a broader scope of its operations. As the Chinese proverb says, "We live in interesting times." This year will be among them! **AS**