Physical Security on the Edge

Long before our first exposure to the wonders of the Internet, along with its drawbacks such as computer viruses, pharming and phishing attacks, enterprise security has been an important business priority. In most organizations, however, physical security is managed by one department, while data security is attended to by the corporate IT department. As a consequence, security administrators are left with multiple user databases, redundant and/or disconnected security policies and totally independent systems and technologies. The net effect of the gaps created by this model is that the enterprise remains vulnerable to both physical and data security breaches.

As IP communications have become pervasive, the possibilities of the convergence of physical and logical access have grown. This next wave of security is closer than you might think. The technology is now in place for today's building management systems to operate in essentially this manner with a computerized "backbone" that oversees and connects all security functions -- from physical security that opens doors for authorized employees to logical security that grants computer system access.

While traditional solutions for integrating physical and logical access have historically been intrusive, difficult to deploy and very costly, a new generation of access control solutions that are IP-enabled are paving the way for organizations to make what once was a futuristic scenario a viable reality. HID Global is meeting these security challenges head on with its new Edge Family of IP-based access solutions.

Benefits of IT Managing and Deploying Physical Security

As a leader in physical access control, HID Global is developing solutions that help integrate physical access (PACS) and logical access (LACS) systems. This integration provides a layered enterprise defense. More importantly, these solutions leverage the combined assets, budgets and skills of both IT and security personnel.

The following are some reasons why it is attractive to have IT play an integral part of managing and deploying physical security:

- **IT Manages the Budget:** Given IT's mission to use technology to manage, store, protect, process, transmit and retrieve information, its reach is felt throughout the organization. Because many functional areas of a company, such as communications, data processing and finance, have found ways to use technology to make their operations more efficient, reliance on the IT department has given it significant scope and influence in budgeting decisions. Because IT is commoditized in its hardware choices, its purchasing can be more cost effective.

- **Standards, Standards, Standards:** The success of IT's objectives relies on standardization—standardization of technologies, processes, architectures, cable, installation practices, network hardware, PoE switches, etc. So when designing a new office, IT is often one of the first consulted to evaluate the feasibility of setting up the site. Mass-production and standardization have greatly reduced costs and standard IT equipment is available nearly everywhere. In order to adapt to a number of circumstances, IT multi-use components are designed to come off the shelf as the best-fit for any situation. Standards have also allowed IT to re-utilize much of its initial hardware investment when migrating from one software platform to another. Without standards, this would not be possible.

- **It Already Exists:** Leveraging the IT infrastructure for cost savings is key because companies already have it. Companies have already invested in network infrastructure. They have IT closets where there is already investment in the switchers and power supplies (the UPS).

- **Changing Installation Dynamics:** Physical security has always been closed wiring/closed systems. Until now, one door may have required as many as 16 different wires running back to the controller in the closet. IT wiring, typically CAT-5 cable, uses four pairs of "smart" wires: two pairs for power and two pairs data communication. This cabling is easier to install and more powerful than proprietary physical security wiring. Wouldn't it make sense that the physical security system leverage that standardized wiring?

- **Technology-Enabled Power Considerations:** Physical security can benefit from recent IT-enabled advancements in power distribution. PoE (Power over Ethernet) provides additional electrical power, along with data, to remote devices over standard twisted pair cable in an Ethernet network. Before PoE, Ethernet cabling just carried data, and additional power supplies and cables were required to power the physical security field devices. Utilizing PoE reduces cost, installation time and complexity of the installation.

- **Performance:** Because the network carries the information that runs the business, IT protects it better. The IT network infrastructure is fully monitored and more hardened because it carries critical data and is backed-up by UPS power.

Convergence is Possible with the Edge™

The above benefits of the IT system can be tapped into by the physical security system via HID Global's Edge family of IP-based access control solutions. The HID Global Edge platform is an IP-enabled access control processor and host interface solution. It is designed to provide a complete and full-featured access control hardware/software infrastructure and contactless smart card read/write capability at "the edge" of the network -- right at the physical door.

Edge products also incorporate a multi-platform technology called OPIN™, an open architecture allowing it to be fully integrated into any host access control system utilizing an IP network software interface. Through HID's network of solutions partners, a wide variety of OPIN integrated solutions exist today. Bringing intelligence to the door, the flexible design includes an integrated iCLASS® reader or allows connection to any Wiegand or most HID clock-and-data readers.

A perfect solution for new building installations, Edge products require less wiring, are cost-effective and are ideally suited for today's IT-centric security environment. For legacy systems, Edge solutions' new OPIN API permits future host software choices without the need to install new hardware and makes the system adaptable to an organization's changing security needs.

The Edge family includes the Edge Solo solution for enterprises with multiple- or single-door installations. With its built-in user interface, Edge Solo can work without a host application. Due to its OPIN technology, the Edge Solo can be easily upgraded to tap into a host-based system should an enterprise need to migrate it onto a larger system. The family also includes the Edge Host solution, which is designed for larger systems with hundreds of doors and multiple facilities and ties back to an enterprise's host software. For both Host and Solo versions, HID offers an integrated card reader and access controller all-in-one unit: the EdgeReader, in ERW400, ER40, and ESR40 versions. HID also offers the EdgePlus E400 and ES400 access controllers, allowing end-users to select the card reader of their choice.

Why is Edge the ideal platform to enable the convergence of IT and physical security?

- **Extend the Network Wiring Out of the Closet:** IT closets are valuable real estate. People are fighting for wall space. Under the old paradigm, physical security needed to coordinate with IT to get room on the wall. With Edge, you do not need that wall space anymore, just a CAT-5 cable going out. If you have PoE and UPS power on your network equipment,

it doesn't require another power supply. Edge enables physical security to extend the network wiring out of the closet.

- **Pay Less Per Door:** With Edge, you can leverage the cost savings of the IT environment to fulfill the needs of physical security (secure more doors). With a fixed cost per door, physical security pays less per door. Organizations can obtain more security for the same amount of money.

  Before the Edge platform, if an organization wanted to add one door, the first thing the physical security team needed to know was, "Is there room on one of the panels to add another door?" If not, the end-user had to buy another panel to add this door, making the first door very expensive. With the next door, the cost per door spikes down, due to having spare ports.

  With Edge, organizations get a fixed cost per door. It's easier to budget, and the cable and installation cost less. An added benefit is more flexibility in the installation because the network is always nearby.

- **Increased Physical Security Focus:** The physical security department still manages the access control. However, with Edge, physical security becomes leaner and more efficient. They can focus more on access control (instead of installation issues) because the majority of power, capability and capacity issues will be managed by IT.

Additional benefits of installing Edge at the door:

- **Bi-Directional Communication:** Having the intelligence in the closet does not allow organizations to take full advantage of the capabilities of today's readers. Higher functionality like writing to smart cards, key replacement or reader configurations, can only be done over a data network. Wiegand communications to a reader are fine for sending uni-directional card transaction information to a controller but will not allow the higher function capabilities. With Edge, organizations now have the intelligence and the data network right at the door.

- **Compliance:** Integration makes security and compliance policies more effective and easier to enforce. Being able to track both physical presence and logical access helps flag and avert potential problems. For example, if a user is physically checked into the building, there is no reason to expect that same user to be remotely logging in via VPN.

- **Distributed Processing:** Rather than having multi-door controllers in a closet, the decision-making and database can be distributed on a per-door basis. This configuration removes the single point of failure for multiple doors and offers greater flexibility in the deployment of access control.

- **Global Provisioning/De-Provisioning:** First day provisioning and last day de-provisioning of employees and contractors continues to be a major problem. Multiple enrollment steps, databases and procedures are not only redundant but also often lead to serious security gaps. Physical access for a departing employee may be terminated but user access may continue for some time thereafter and vice versa. By connecting physical and logical access, the process is streamlined and security is enforced since all access can be terminated at once.