Cybersecurity also includes protecting data rooms with code compliant physical electronic access control, often the weakest link in IT security.

FROM NETWORK'S EDGE TO SECURITY EDGE DEVICES:

Code Compliant Physical Electronic Security for Non-Enterprise Applications

By Kerby Lecka

From network's edge to security edge devices, there are a variety of cost-effective, low-power solutions to meet code compliance for electronic access control of door openings in smaller companies and single facilities. Physical electronic security begins with the protection of people by providing fire and life safety, preventing unauthorized access, and monitoring of activities and behavior of people more prone to unauthorized access. Then, physical electronic security is about the protection of assets—products, intellectual property, processes, equipment, facilities and data—including financial, personnel, customer, and even health records.

Physical electronic security is now as simple as tapping into the nearest Ethernet connection to power and control door access via Web browser and low-voltage access and egress devices. The following IP Security and PoE hardware applications are just a few of many possibilities:

Data Room/Private Cloud Computing Facility Security

No longer the exclusive domain of complex, enterprise-wide security systems, sophisticated and cost-effective electronic access control is now available for smaller companies and single facilities with the same need for protection as larger organizations. Data rooms are no exception.

Beginning at the outer door, to the inner door separating visitors from employees, to even the entrance to the "data" part of the center, low-voltage access control devices (PoE hardware) can be controlled via an IP controller connected to the PC network and accessed by web browser 24/7. This includes creating "mantraps," allowing only one door to open at a time and requiring authentication for booth doors. This can also include access control at the door to an individual computer processing room (data room) where the actual server, mainframe or other critical IT equipment is located. Even individual computer cabinets can be secured and connected to the network via low-power electronic cabinet locks.

Applicable, low-voltage PoE hardware solutions for access control include magnetic locks, key and exit switches, electrified exit devices, electric strikes, electrified locksets, electric bolt locks and cabinet locks—all connected by Ethernet cable to an IP-based access control.

Real-time monitoring, detecting unauthorized access or attempts, and keeping track of people—especially with a building evacuation in an emergency—are critical. Low-voltage keypads, card readers and proximity readers are popular key technologies for door access control, all tied to an IP-based controller that provides audit trails and user management to define who has access. These are also suitable for entrances like loading docks and other exterior facility doors.

Should the smaller company or single facility need to enlarge, these PoE hardware solutions and IP-based access controllers and software serve as a foundation for unlimited, cost-effective expansion. Instead of paying upfront for a large and expensive access control system, users can add security and protection incrementally as budgets and needs increase.

Generally, applying the principle of least privileges is appropriate. Physical security is the key to all other IT security measures. Unauthorized physical access to server and equipment is the weakest link in IT security and can have profound consequences.

Clean Rooms, Hospitals, Pharma Facilities

Clean rooms require rigorous controls placed on reducing environmental pollutants to pre-determined levels for the protection of products and processes from contamination by chemical vapors, aerosol particles, dust and airborne microbes. Prevalent in pharmaceutical, biotechnology, and high technology industries, clean rooms provide protection from contamination by equipment and staff, primarily by limiting physical access and logging all access and egress activity.

As with data rooms, most physical electronic access control systems have been designed at the enterprise level for large facilities and organizations. Yet, the clean rooms in smaller or single facilities must also prevent contamination using solutions within their budgets. Enter low-power PoE hardware devices and IP-based access control connected and powered with existing Ethernet connections.

Clean rooms typically use airlocks for entry and exit; a combination of mantrap with two doors interlocked to prevent simultaneous opening, and special timing functions to avoid unwanted passages between areas to maintain sterile and safe conditions. These procedures also maintain constant temperature, humidity and air pressure in the clean room. Access to these secure areas can be limited to authorized personnel through the use of low-voltage keypads, key switches and card readers. Of particular benefit is the use of proximity readers to provide touch-free high security and contamination avoidance.

As with data rooms, all access and egress activities can be controlled with low-voltage PoE hardware connected to and monitored in real time with an IP-based controller, and stored for future audit trails. While the protection of people for fire and life safety is foremost, physical electronic security of clean rooms can also ensure compliance with organizational policies and regulatory compliance with GMP and FDA 21 CFR Part 11.

With low-voltage, cost-effective physical electronic clean room security, consistent product quality can be ensured to prevent costly recalls and regulatory actions that may affect reputation and impact the bottom line.

The healthcare industry has a seen a disturbing trend towards visitor impatience, patients in behavioral health facilities being more easily upset, and staff unprepared to respond appropriately to bad behavior. This includes

All photos courtesy of Security Door Controls

Although it is generally not an accepted practice to lock entry and exit doors to everyone who enters a hospital, clinic or healthcare facility, it is acceptable to control access into specific areas. Physical electronic security applied to funneling patients and visitors into areas can provide them with a positive, safe and secure clinical experience.

access and egress of unauthorized people into higher-risk areas potentially leading to violent incidents. The trend can be particularly acute for small, single facility entities like urgent care centers, outpatient surgery centers, and rural medical clinics not requiring enterprise-wide security systems but still needing viable solutions.

Again, low-power PoE hardware devices and IP-based access control connected and powered with existing Ethernet cable offer a practical alternative. Although it is generally not an accepted practice to lock entry and exit doors to everyone who enters a hospital, clinic or healthcare facility, it is acceptable to control access into specific areas. Physical electronic security applied to funneling patients and visitors into areas can provide them with a positive, safe and secure clinical experience. Restricting access into high-risk areas is also part of a well-designed program. High-risk areas may include:

- Emergency Room
- In-house Pharmacy
- Maternity
- Pediatrics
- Geriatrics
- Behavioral Health

Using low-voltage, PoE Hardware and IP-based access control for physical electronic security in healthcare is one of the easiest and most cost-effective means for preventing healthcare crime and violence.

Pharmaceutical facilities have come under increased inquiry and examination by the FDA and DEA, and increased pressure to comply with good manufacturing practices (GMP), good distribution practices (GDP), good storage practices (GSP) and international World Health Organization (WHO) standards. Additionally, physical security and access control regulations from the Department of Homeland Security (DHS) and the DHS Chemical Facility Anti-Terrorism Standards (CFATS) must be adhered to in an effort to minimize access to dangerous chemicals by terrorists.

The small pharmaceutical manufacturer, wholesaler or logistics provider has few alternatives for lower-cost physical electronic security than the large, enterprise systems currently offered them. Yet they must also meet the many guidelines of FDA Title 21, Subchapter C, dealing with the security of facilities which "must be secure from unauthorized entry" and whose "access from outside the premises shall be kept to a minimum and be well controlled."

As you may surmise, low-power PoE hardware devices and IP-based access control connected and powered with existing Ethernet cable is a viable alternative for the needs of the small pharmaceutical facility. Physical electronic security can restrict access to sensitive areas in a cost-effective manner while still providing the fire and life safety to meet local and national code requirements. Real-time monitoring and audit trails via an IP-based access controller can provide 24/7 protection of vulnerable areas inside manufacturing and distribution facilities. These areas include warehouse, vault and temperature rooms, packaging and chemical rooms.

Data rooms and clean rooms are commonly found in pharmaceutical facilities and physical electronic security solutions as previously described are equally as efficacious here. Also, the protection of people—researchers, corporate executives, managers—is foremost, followed by the facility's critical assets including the processes, research/intellectual property, and raw materials used to develop and manufacture the final products. As with other facilities, all perimeter exit doors, and loading entrances can be included in a physical electronic security solution via PoE hardware and IP-based access control.

Tenant Improvement

The world is wired. Ethernet cable is everywhere. Buildings are smart. Imagine the savings in cost and installation time by not having long cable runs and power supplies for every door by simply tapping into the nearest Ethernet connection. Low-power PoE-capable locking hardware connected to IP-based access control does just that by allowing easy integration and connection to a physical electronic access control system.

Physical electronic access control solutions are particularly suited to tenant improvement and retrofit projects, providing the ability to purchase and install just what's needed without having to invest in a more costly, enterprise system designed for larger facilities. The beauty of the PoE hardware and IP-based access control approach is that it is easily expandable as needs grow without the front-end commitment to an over-sized solution.

As with any tenant improvement or low-voltage implementation via Ethernet cable, we recommend that installers are comfortable with Ethernet network best practices, and test any installation using an Ethernet cable tester before start-up. Also, by following industry standards—ANSI/TIA-1005 – M.I.C.E and ANSI/TIA-569C.0 (cable lengths)—many issues can be eliminated that may be residuals of previous installations.

Without a doubt, using viable, legacy Ethernet cable with PoE hardware and an IP-based controller will save cost, time and manpower when retrofitting for physical electronic security. Plus, the building or facility can remain operational without the need to remove, install and recycle cable.

Security Regulations Compliance

Physical electronic security via PoE hardware and IP-based access control can also meet the compliance requirements of many regulations not typically associated with access control. Again, there are many smaller organizations seeking compliance, but they haven't had access to simple, cost-effective physical security

Low-power physical electronic perimeter and gate security for energy and chemical facilities can ensure plant entrances are safe and secure as well as meeting many homeland security and anti-terrorism standards.

Renovation and retrofit of buildings using existing ethernet cabling to connect low-power physical electronic security solutions is a cost-effective way to ensure compliance with building codes.

solutions until now. All listed below also require Physical Security as part of meeting compliance:

- **HIPPA + HTECH** – Health Insurance Portability and Accessibility Act + Health Information Technology for Economic and Clinical Health: hospitals and health care facilities must comply with these two acts for the protection of personal health information and electronic health records, including *limiting physical access* to information systems, equipment and IT operating environments to authorized individuals.
- **Sarbanes-Oxley** – abbreviated as SOX, requires all organizations to store specific financial information in an auditable trail, have *physical security*, and a system for monitoring and reviewing access on a periodic basis.
- **PCI-DSS** – Payment Card Industry Data Security Standard covers all businesses that accept credit card payments: Requirement 9 states that any *physical access* to data or systems should be appropriately restricted, and entry controls used to limit and monitor physical access to systems that store, process or transmit cardholder data.
- **SSAE 16** – is an auditing standard issued by the American Institute of Certified Public Accountants that restricts physical access to data centers through a combination of *physical security systems* and biometric identification.

The smaller organization or facility can now meet many of the particular physical electronic security requirements of their industry with lower cost, low-voltage, easy to install and operate PoE hardware and IP-based access control solutions, using existing Ethernet cable and avoiding heavy cost commitments in complex, oversized, enterprise-wide systems. ■

KERBY LECKA is Director of Marketing for Security Door Controls. He can be reached at kerby@wmwinc.com.