
Reliable *Report*

An informative publication for our friends.

April, 2005

A Day in the Life of an access Control System

In many organizations, the security director's position is a busy one. In the rest, the responsibility for security falls on the shoulders of someone already pressed by other obligations. For this reason, among many others, it is important to have tools that automate functions to the greatest degree possible. While some of the examples below may seem esoteric, they are demonstrative of real functionality incorporated in some actual access control systems installed in the Chicago area.

7:30am: Parking garage entrance - card presented - gate rises allowing entrance, parking allocation account debited "one use privilege" and vehicle owner registered as "On Premises"

7:40am: Front entrance to facility - card presented - door unlocks, system triggers HVAC system to bring owner's office to the desired 72 and turn on his office lights.

7:45am: Desktop computer - card presented - owner is able to log onto computer using access credential as secure password for network applications.

8:15am: Cafeteria - card presented - owner account debited for cost of large coffee and muffin.

8:30am: Office computer - access control system used to reserve conference room for high-level meeting. Unauthorized attendees will not be allowed access during meeting time.

8:45am: Office computer - use access control system to "validate" cards for meeting scheduled above.

9:40am: Office computer - automated morning activity report prints on desktop printer.

9:45am: Automated Report - indicates that a card reported "lost" was used at employee entrance at 7:53am this morning. Access was denied. Lists former owner of card and date card was reported lost.

9:50am: Office Computer - Review associated video from CCTV system (cameras associated with doors as assigned by access control system) displays video from employee entrance at time of attempted use of card.

10:00am: Office - Former owner of card called and asked to identify card user if possible. Clip of card use attempt emailed to former owner. Former owner identifies the user of card as ex-spouse with restraining order.

10:17am: Police notified of circumstances and provided with copy of video clip and access control report.

11:00am: Program elevated security procedures into system for "Major Event" scheduled for next week. Includes changes to automatic unlocking of doors, restriction of elevators to fewer floors, requires card use at all controlled doors at all times and reduces access level of all but most senior employees. Schedule changes to take effect Sunday at noon and expire (revert to normal) on Wednesday midnight.

11:46am: Print and prepare access cards for contractors for use during build out of 7th floor offices. Cards limit access in one elevator to first and seventh floors and only allow access after designated responsible party is registered as "on site".

12:07pm: Cafeteria - card used to purchase lunch.

1:25pm: Office Computer - email log report of production equipment usage by employee (based on card access system associations) to production department managers.

1:50pm: Access control software indicates that a number of fire alarm smoke detectors are generating “trouble” signals and displays their exact location. Fire alarm service provider contacted to schedule service call.

2:00pm: Computer Lab Door - present card and fingerprint at door to computer lab to attend meeting with IT manager.

3:30pm: Receives email with photo attachments of visitors from corporate for next week’s meeting and prints and programs their cards. Updates conference room listing to include cards of corporate visitors.

4:00pm: Enters asset containment tags into system and issues tags to maintenance for installation on new portable equipment.

4:30p;m: Review time and attendance and guard tour records of security guard staff.

5:15pm: Leaves office and uses card to exit parking garage. System records user as “off premises”, turns off lights in office and “frees” office temperature to preset range.

Of course this “Day in the Life” includes the integration of the card access system with many other systems. Among the other systems interfaced are the BAS (building automation system), the CCTV system, the asset management system, the HRIS system, the Fire Alarm system and even a limited financial transaction system. While all of these integrations on a single location may be unusual at this point in time, the capabilities all exist. The limitation on how much you can do with your access control system lies in large part with your imagination and your desire.

The real issue is whether your organization could derive value from improving the security of your facility and the safety of your staff. If you believe that an access control system could address concerns at your facility, please contact us for a consultation at 708-597-4600.