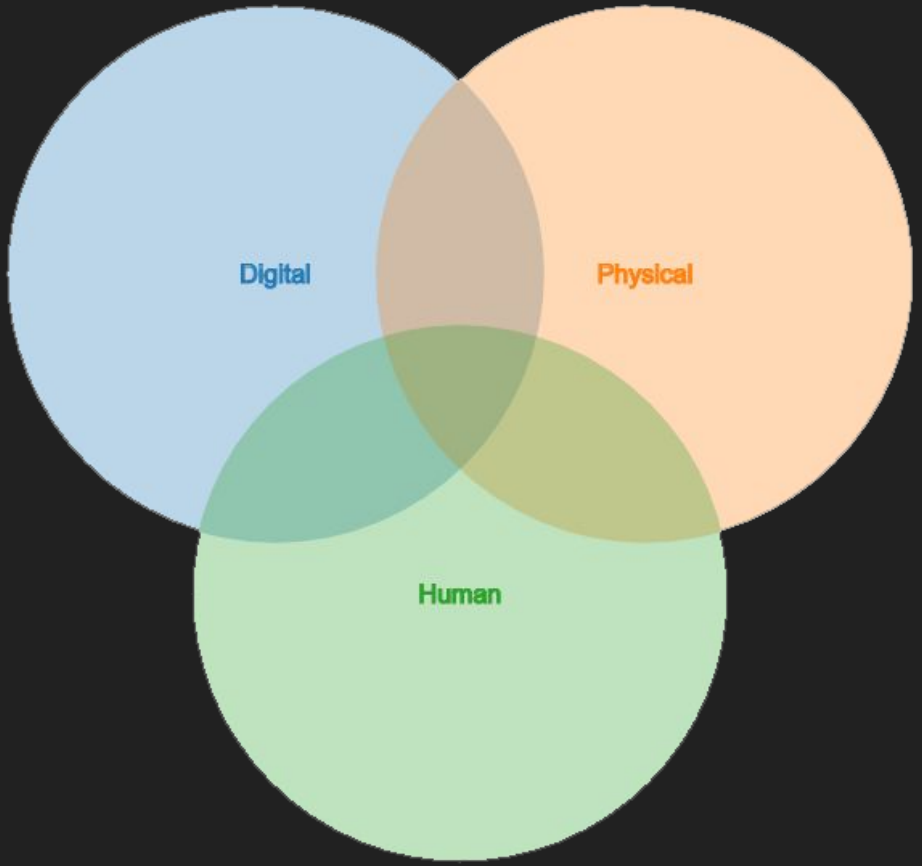
Data Center Security

The basics of securing your infrastructure and information

Three Elements of Security



Digital

Physical

Human

Physical Security

Why Physical Security?

If an attacker has physical access they can likely gain complete access, or can easily disrupt service

Most systems can be reset with access to the hardware, or provide local admin access for troubleshooting

Physical backdoors can be installed and hidden to give an external threat extended access to the environment

Physical sabotage is one of the easiest ways to ensure large scale extended impact to availability

Physical Security

The main goals of physical security as a whole are to:

Deter

> discourage from doing something by instilling doubt regarding possibility of success or fear of the consequences

Detect

> identify the presence of unauthorized access and alert to potential threats

Delay

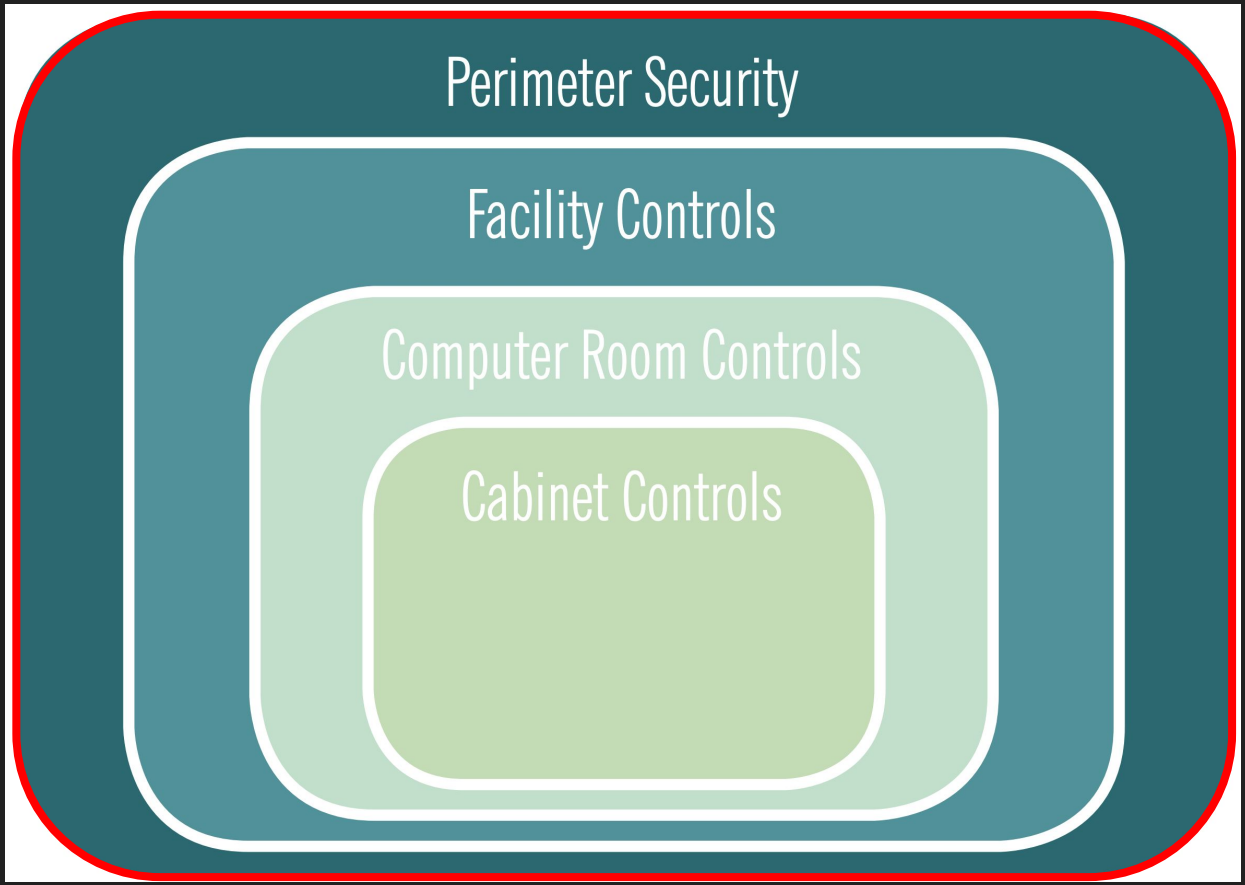
> ensure the time to bypass security gives security teams enough time to **respond** to the threat before the attacker reaches the facility itself

Verifying Identity

There are three basic methods for verifying someone's identity:

1. Possessing or carrying the correct key or token
2. Knowing predetermined private information
    - Password
    - Personal Identification Number (PIN)
    - Challenge Question
3. Providing information that is inherent and unique to that individual
    - Finger and Thumb Prints
    - Iris Scan
    - Vascular Patterns

Layers of Physical Security



Perimeter Controls

The main goals of Layer 1 (Perimeter) Security are:

- Provide the first line of defense for a facility
- Audit the people entering and leaving the grounds
- Provide an obvious deterrence for attackers by showing overt security implementation (i.e. Fences, Cameras, etc)
- Provide an open area between public and restricted space for ease of monitoring and control

Entry Systems

The ability to identify every individual that crosses your security threshold is mandatory (this includes vendors and third parties)

Examples of Physical Security

- Fencing at the physical perimeter
- Controlled parking
- Monitored public spaces such as loading docks and reception areas
- Layered boundaries – internal checkpoints
- Security guards and camera surveillance
- Lockable doors, windows (bars on first floor) and fire escapes
- Intrusion alarms – responded to by security

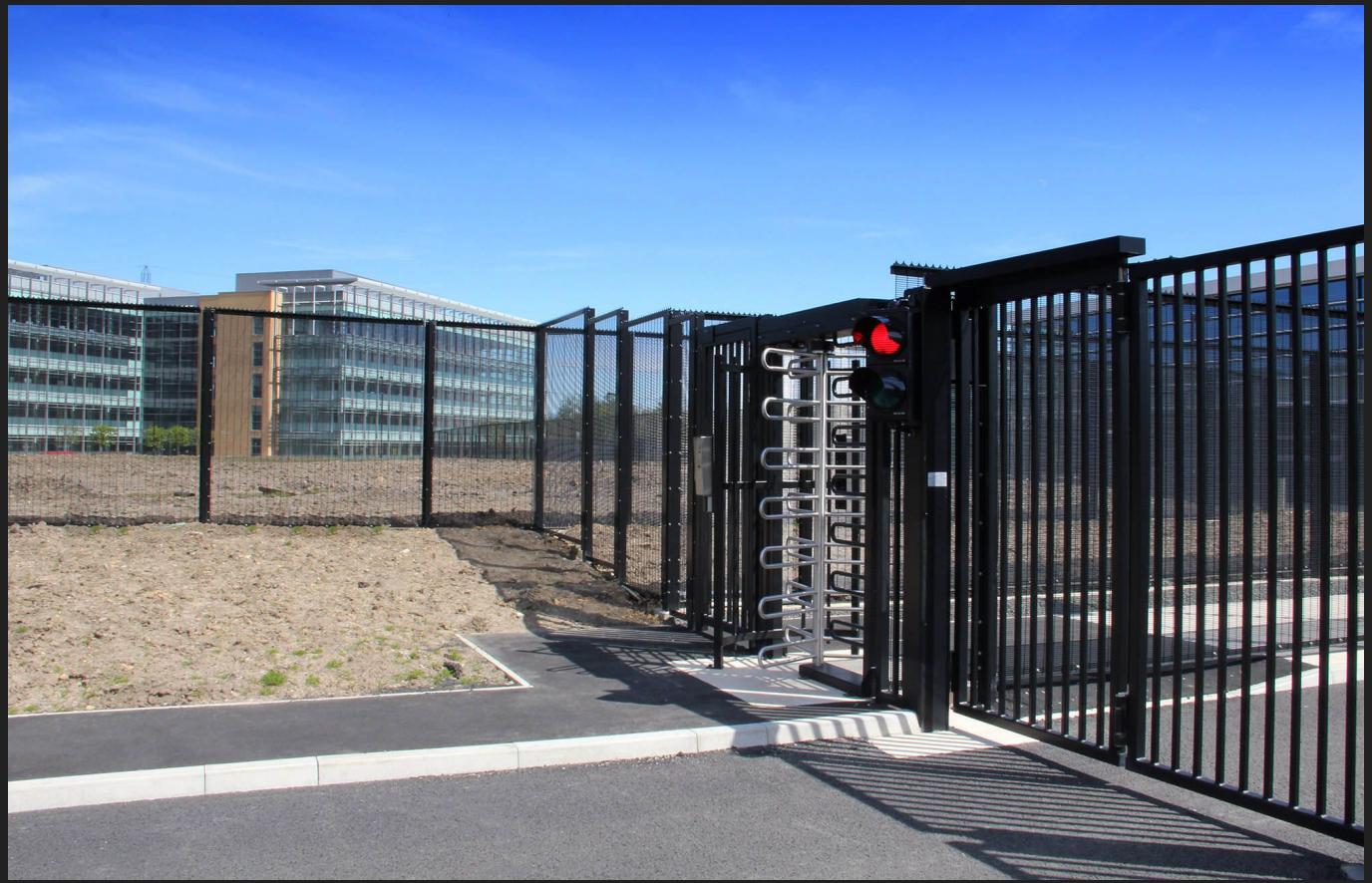
Location Location Location

Assessing whether a data center is secure starts with the location

A trusted Data Center’s design will take into account:

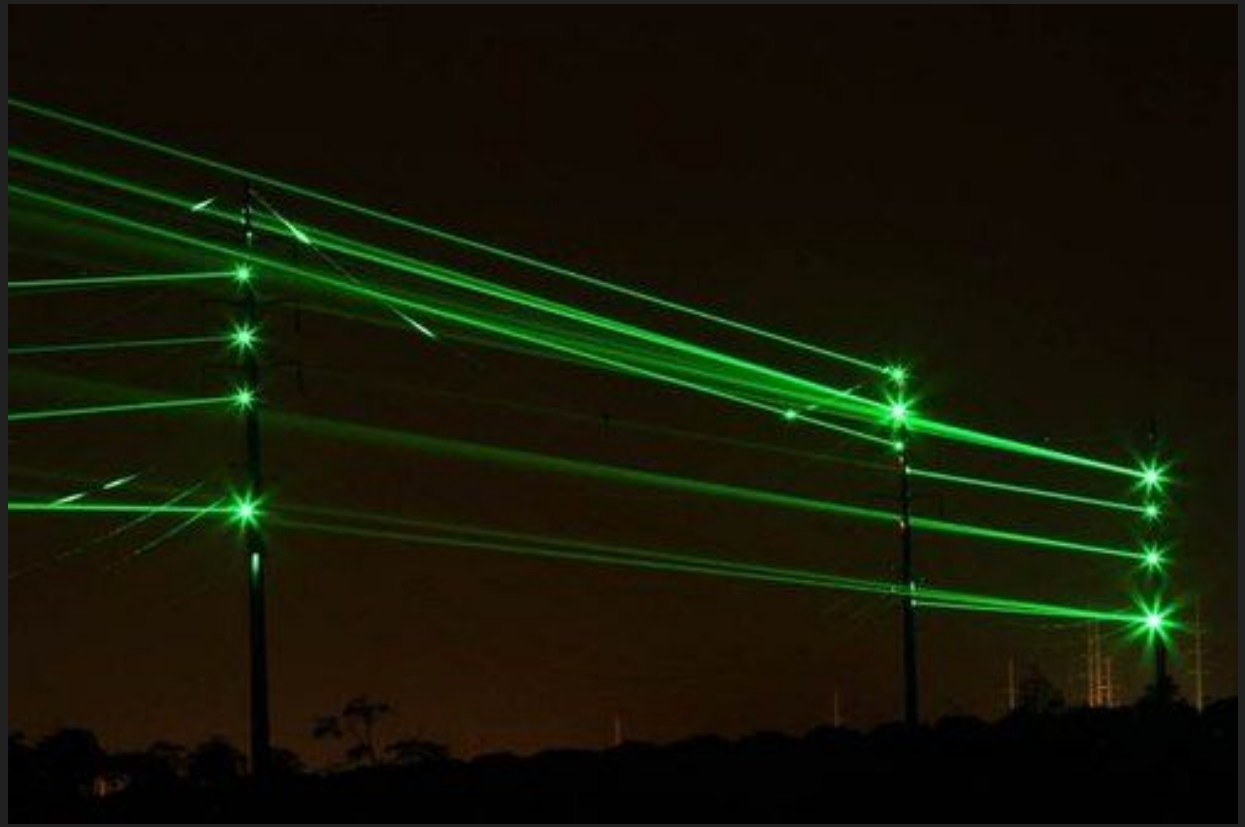
- Geological activity in the region
- Any risk of flooding, fires, tornados
- Other risks of force majeure
- Access to redundant utilities - power, fiber, etc...
- High-risk industries in the area
- Remote location to set up a wide perimeter

Perimeter Security

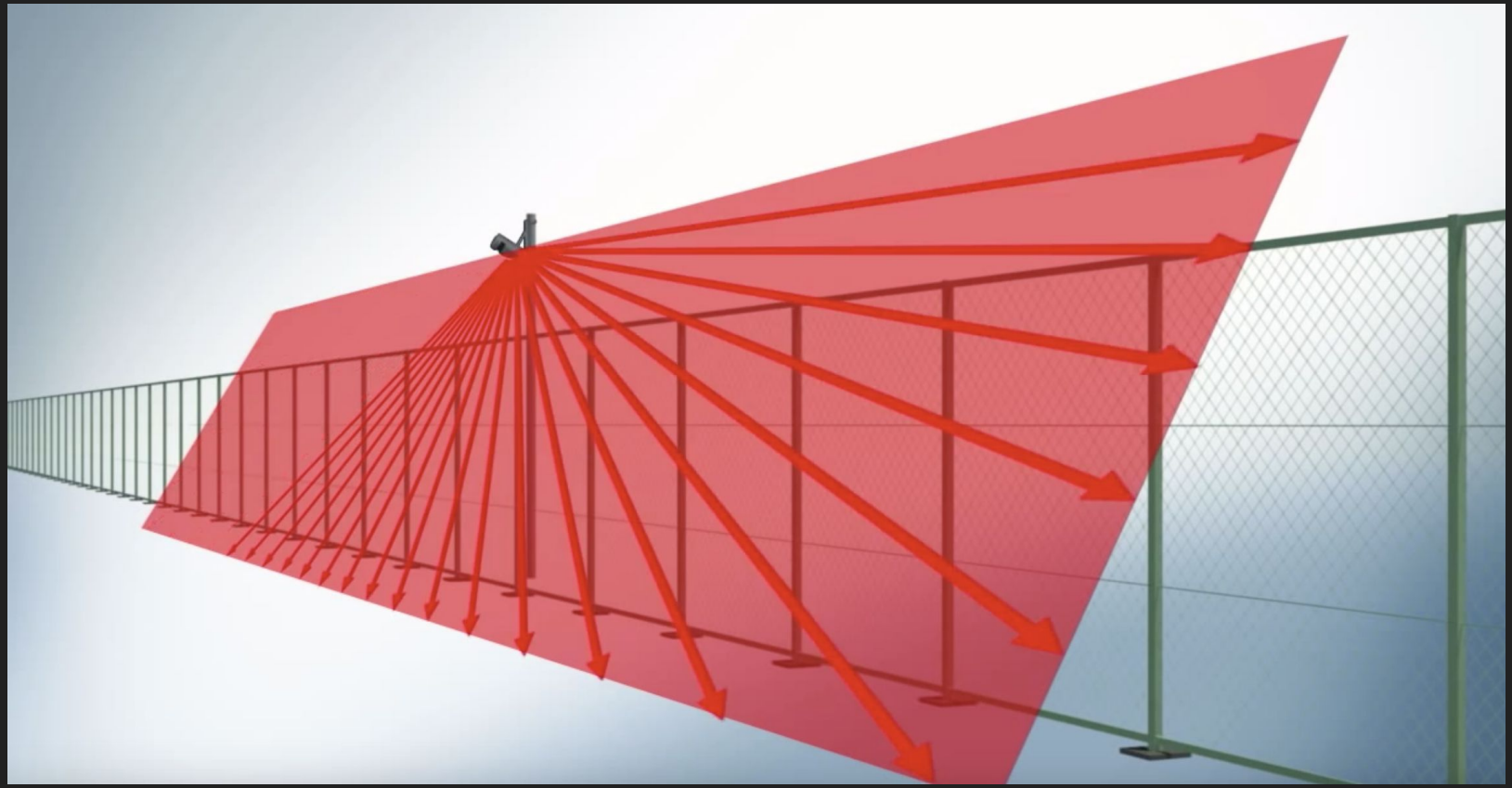


Perimeter Security

Laser Fences!

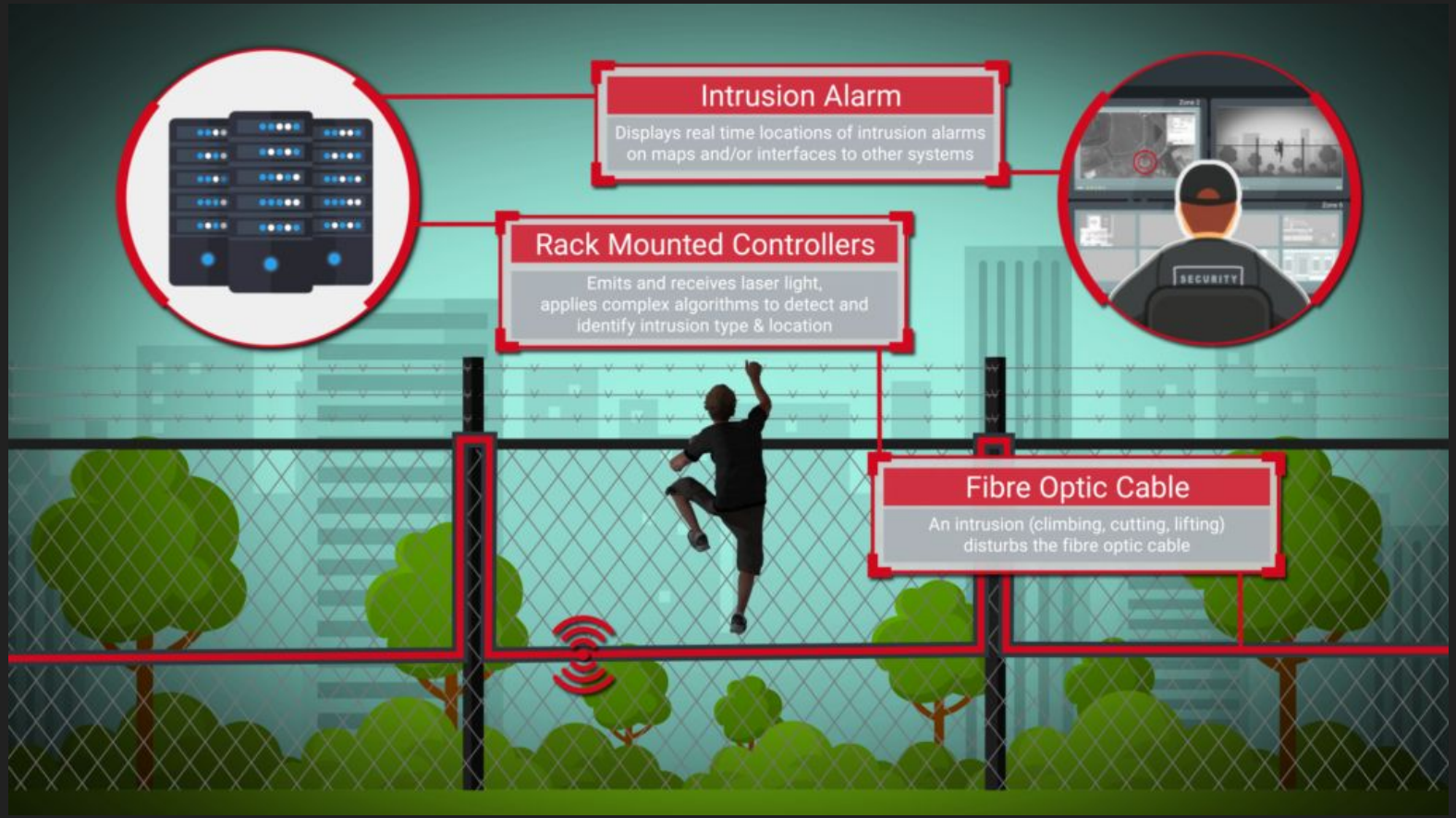


Laser Fences



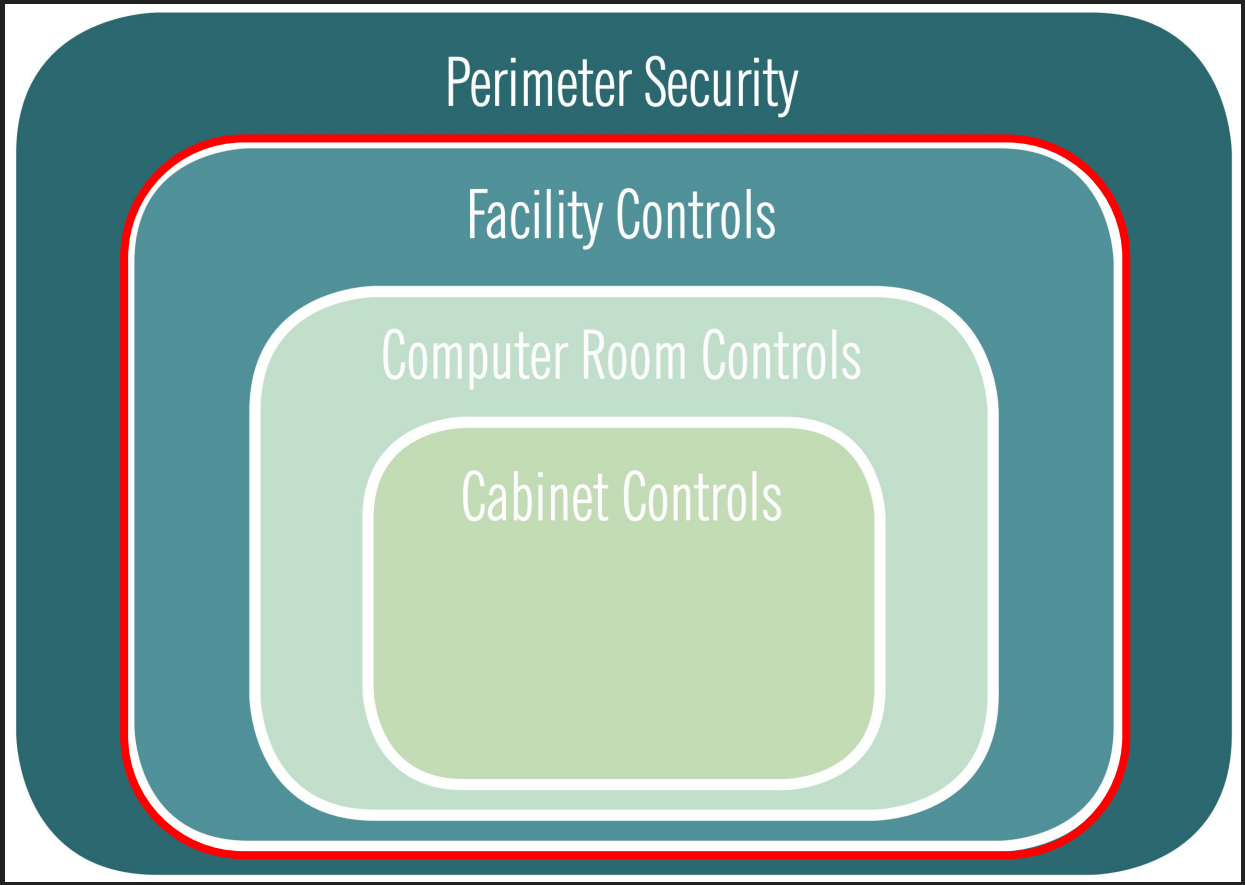
Thermal Cameras

Perimeter IDS



Intelligent Security Cameras

Layers of Physical Security



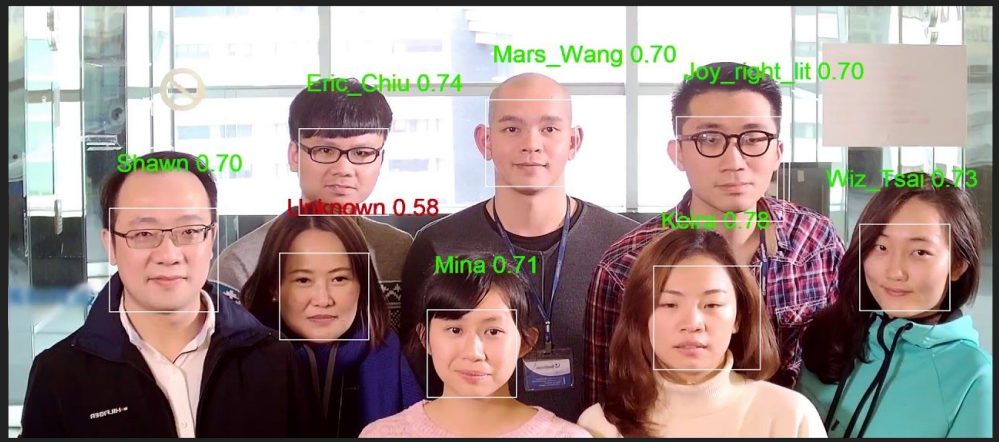
Facility Controls

The main goals of Layer 2 (Facility Controls) are:

- Further restrict access if a breach has occurred at the perimeter
- Strike a balance between security and visitor experience (depending on the type of facility)
- Audit the activity of individuals within the facility
- Ensure access to further protected systems are monitored

Reception/Security Desk

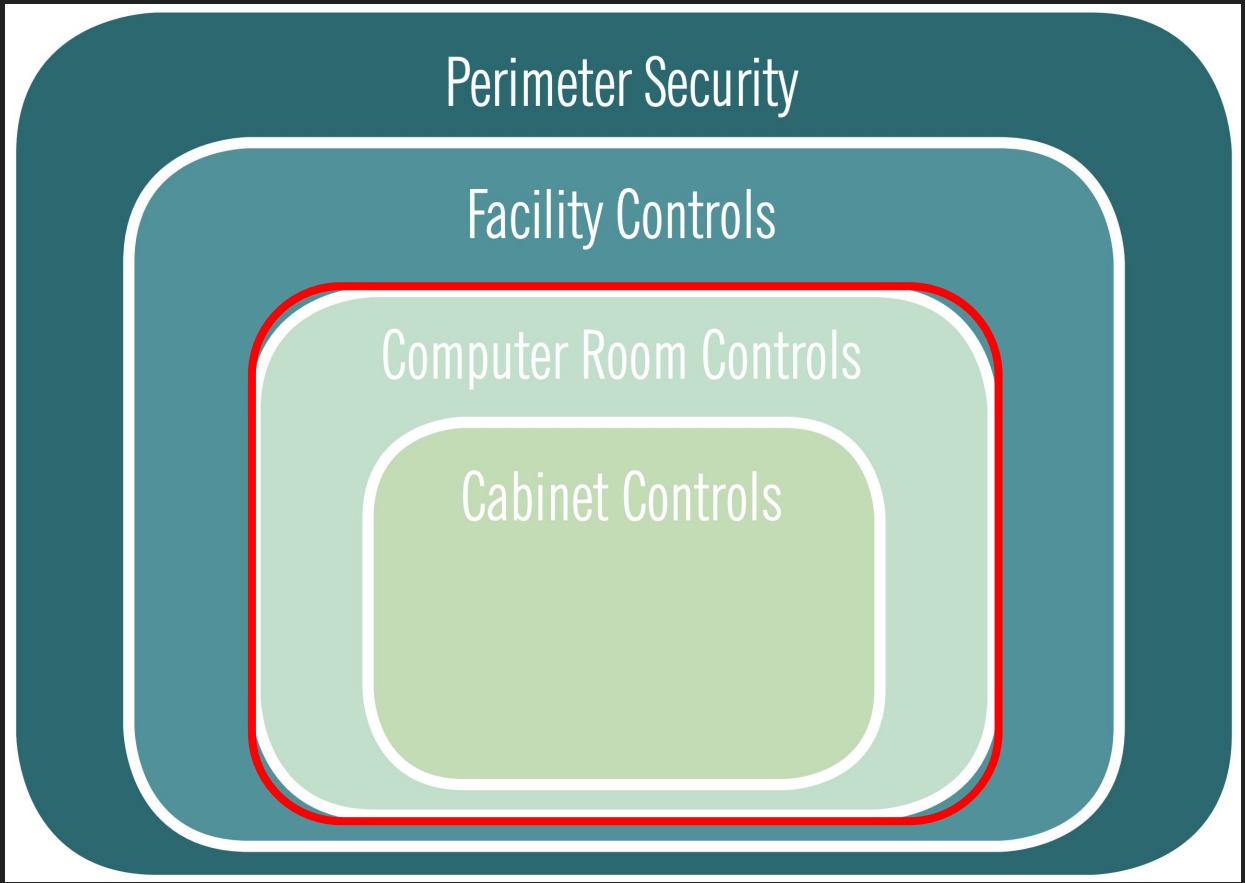
Cameras with Facial Recognition



Multi-factor authentication

Multi-factor authentication

Layers of Physical Security



Computer Room Controls

The main goals of Layer 3 (Computer Room Controls) are:

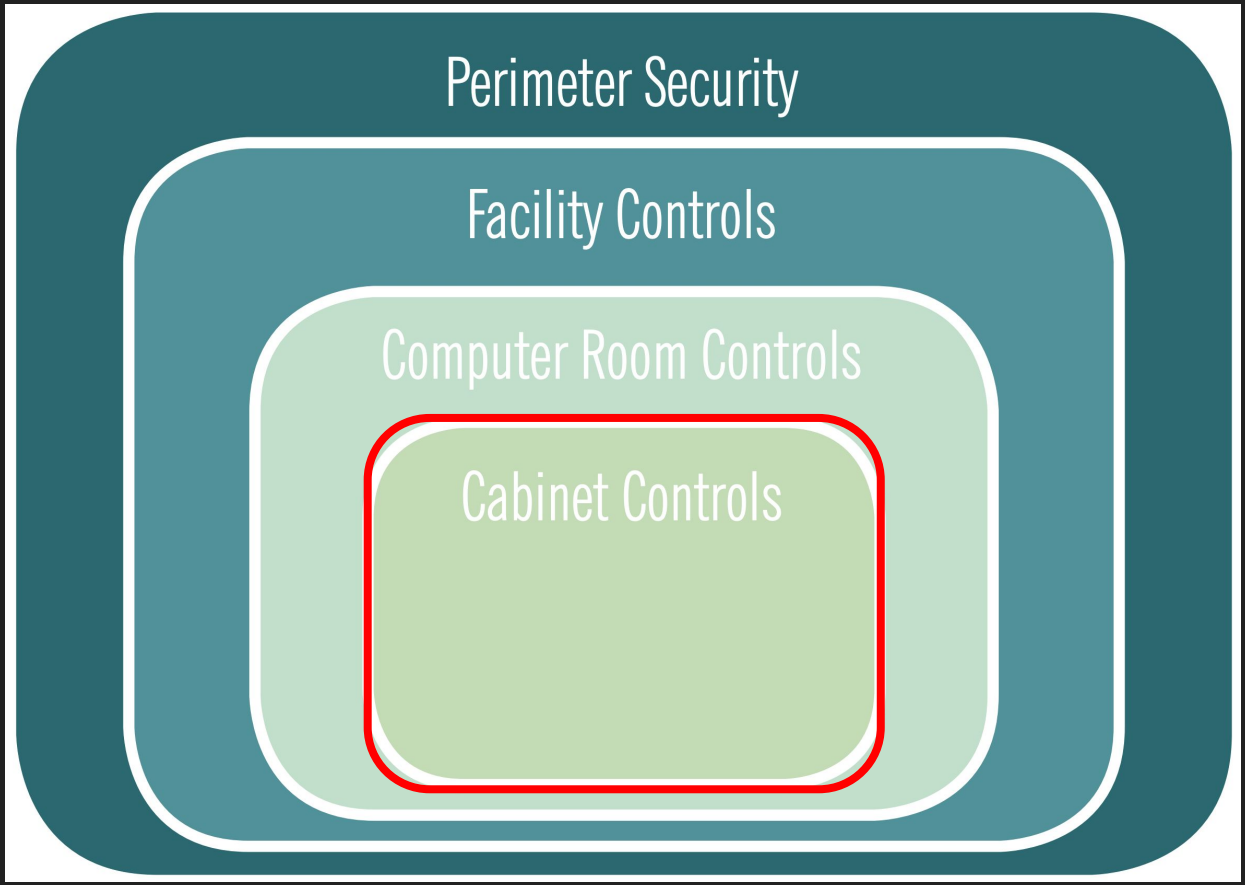
- Further restrict access through multiple forms of verification
- Strictly Monitor all authorized access and actions within the space
- Have redundant power and communications

Biometric Access Control

Biometric Access Control

More Man Traps

Layers of Physical Security



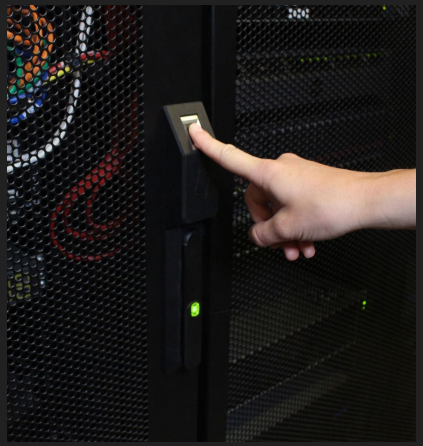
Cabinet Controls

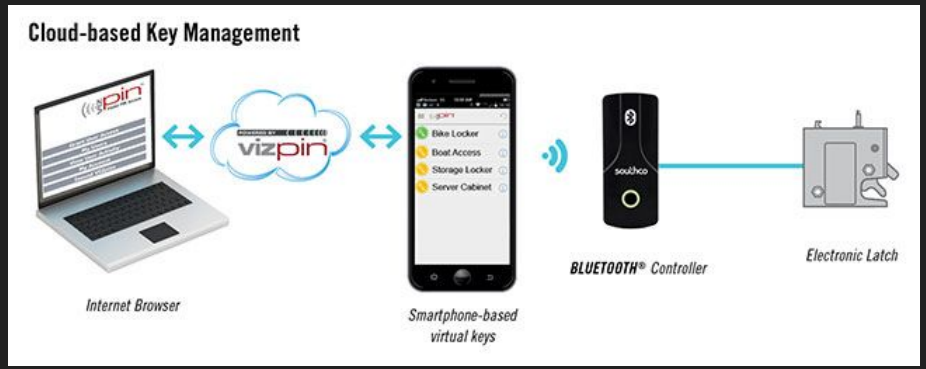
The main goals of Layer 4 (Cabinet Controls) are:

- Further restricting access to an individual cabinet or server
- Particularly important and effective in minimizing the significant and often-ignored “insider threat”
- Prevents innocent and unintended data access
- Provides an audit log as to what devices were touched and by whom
- Essential in a multi-tenant data center (Colocation)

Cabinet Controls

Cabinet Controls



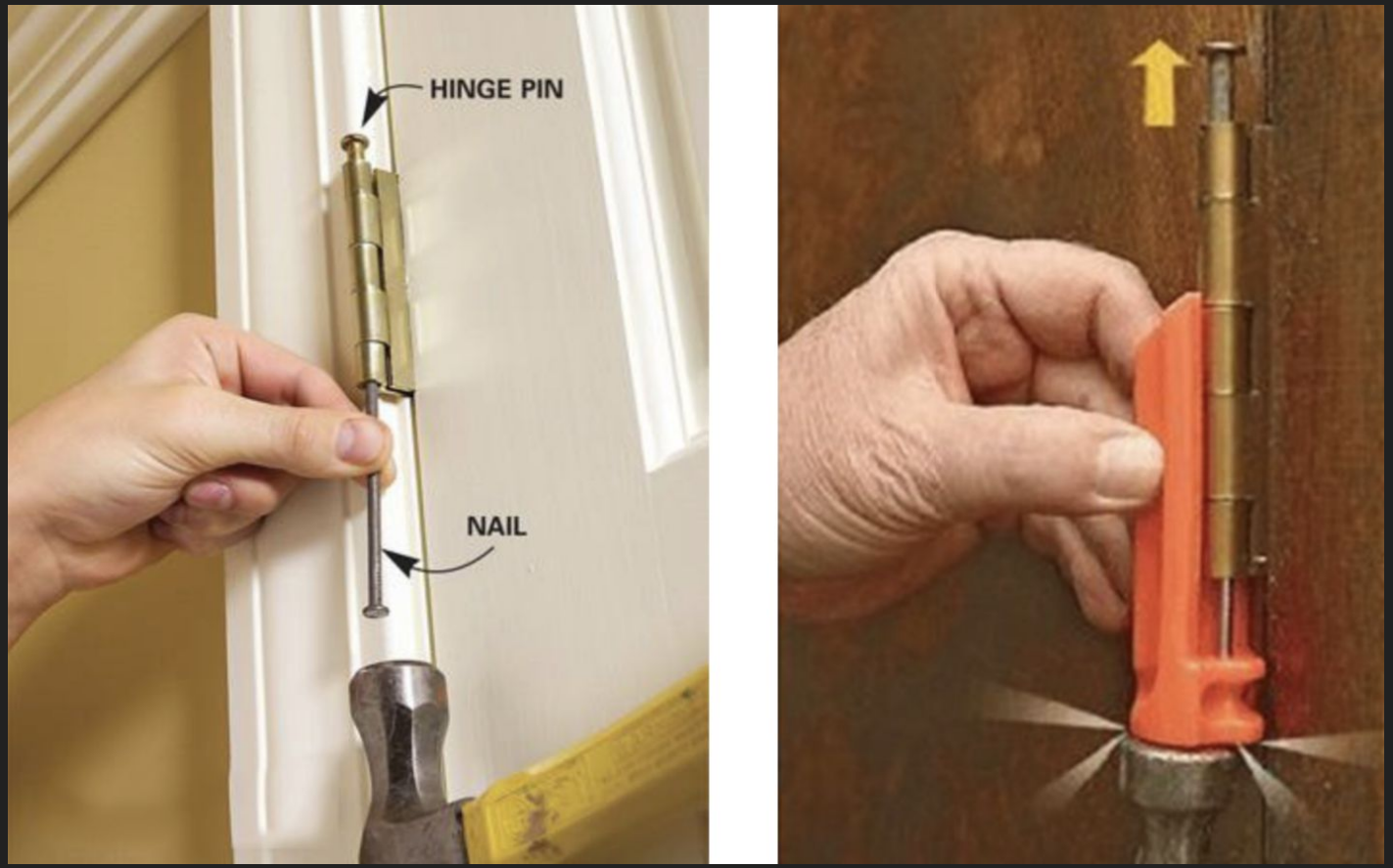


Cabinet Controls

Cabinet Controls

Common Security Oversights

Hinge Removal



Security Hinges

Jam Pins

Jam Pins

Jam Pins

Jam Pins

Lock Picking?

Bypassing Locks Altogether

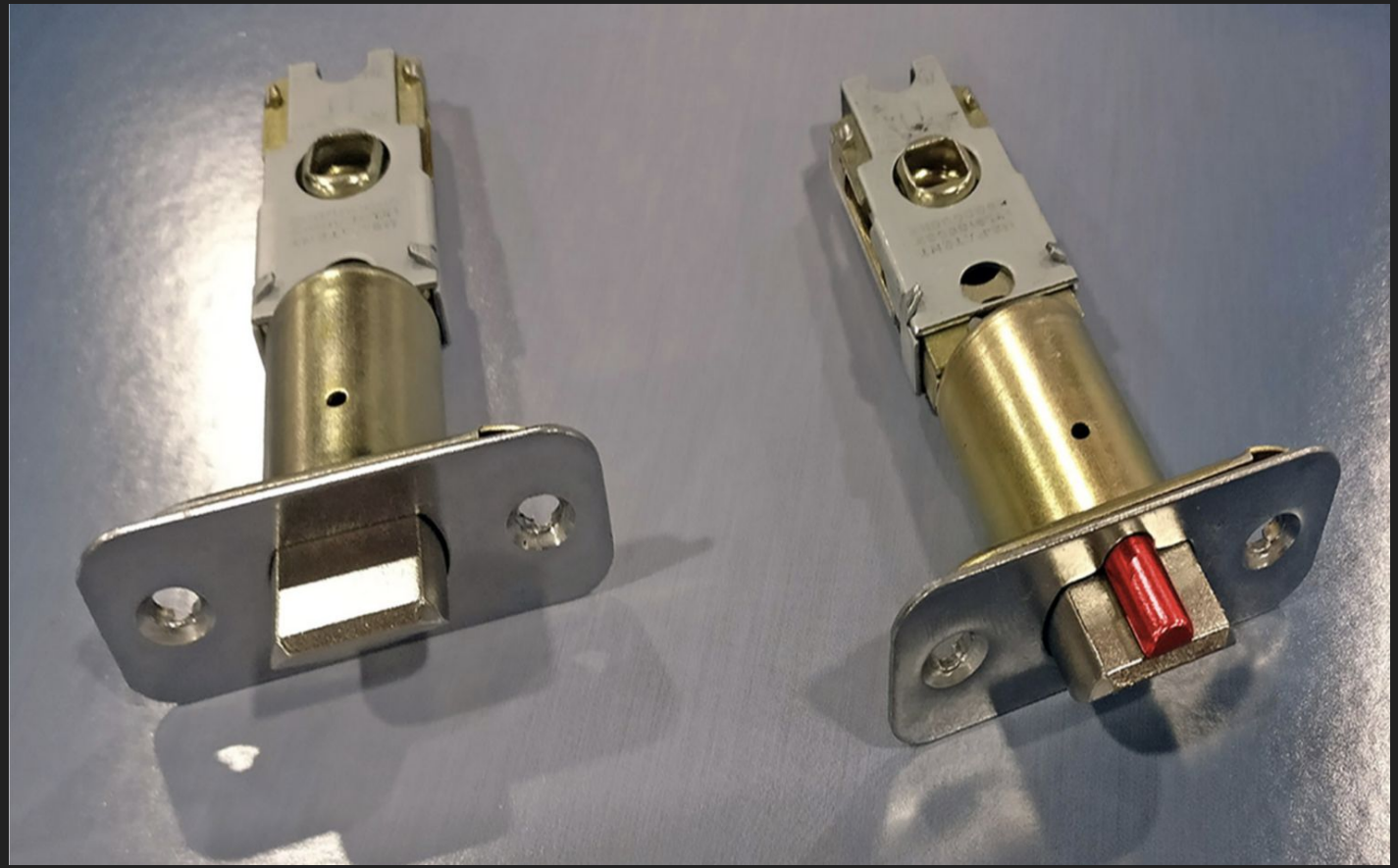
Bypassing Locks Altogether

Bypassing Locks Altogether

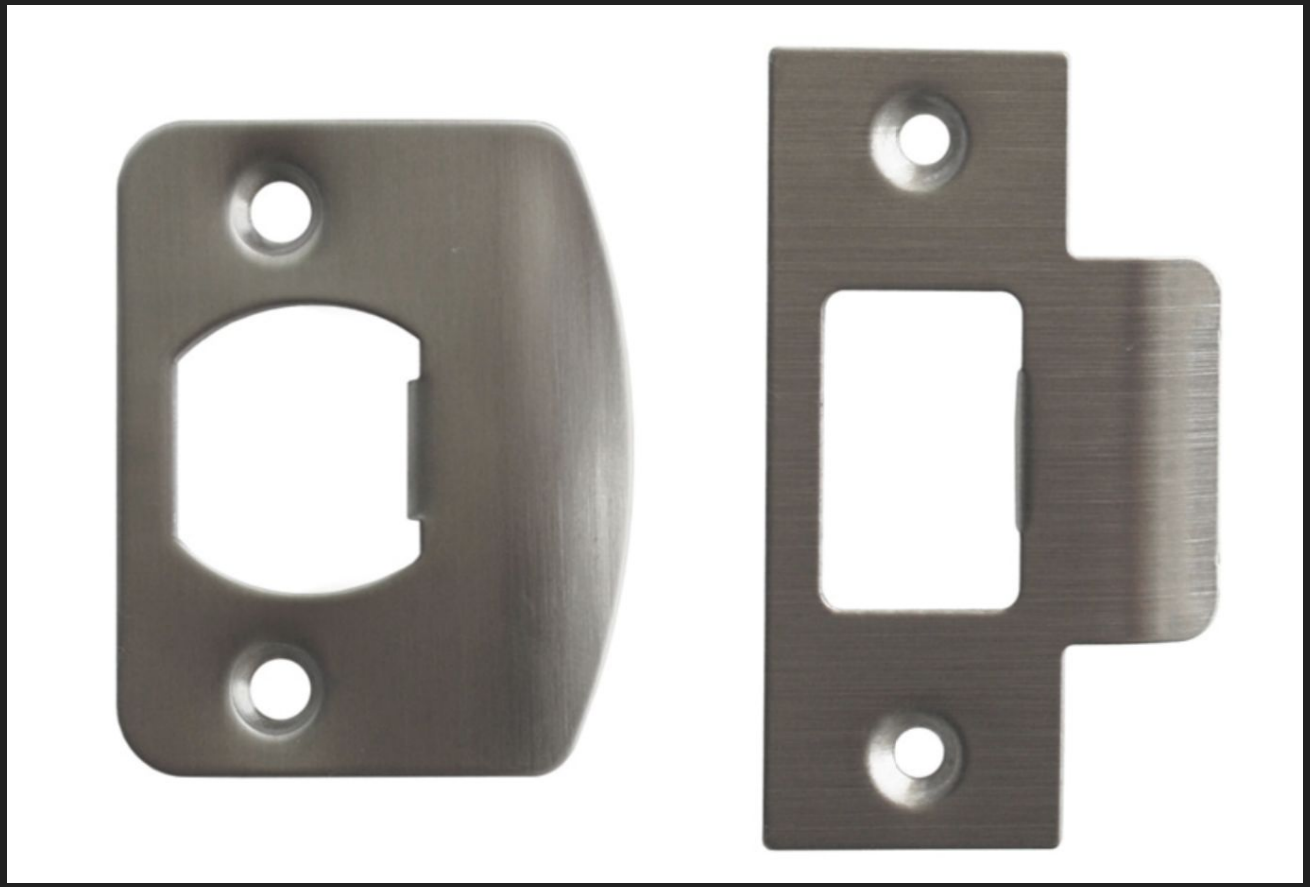
Bypassing Locks Altogether

Dead Latches

Dead Latches

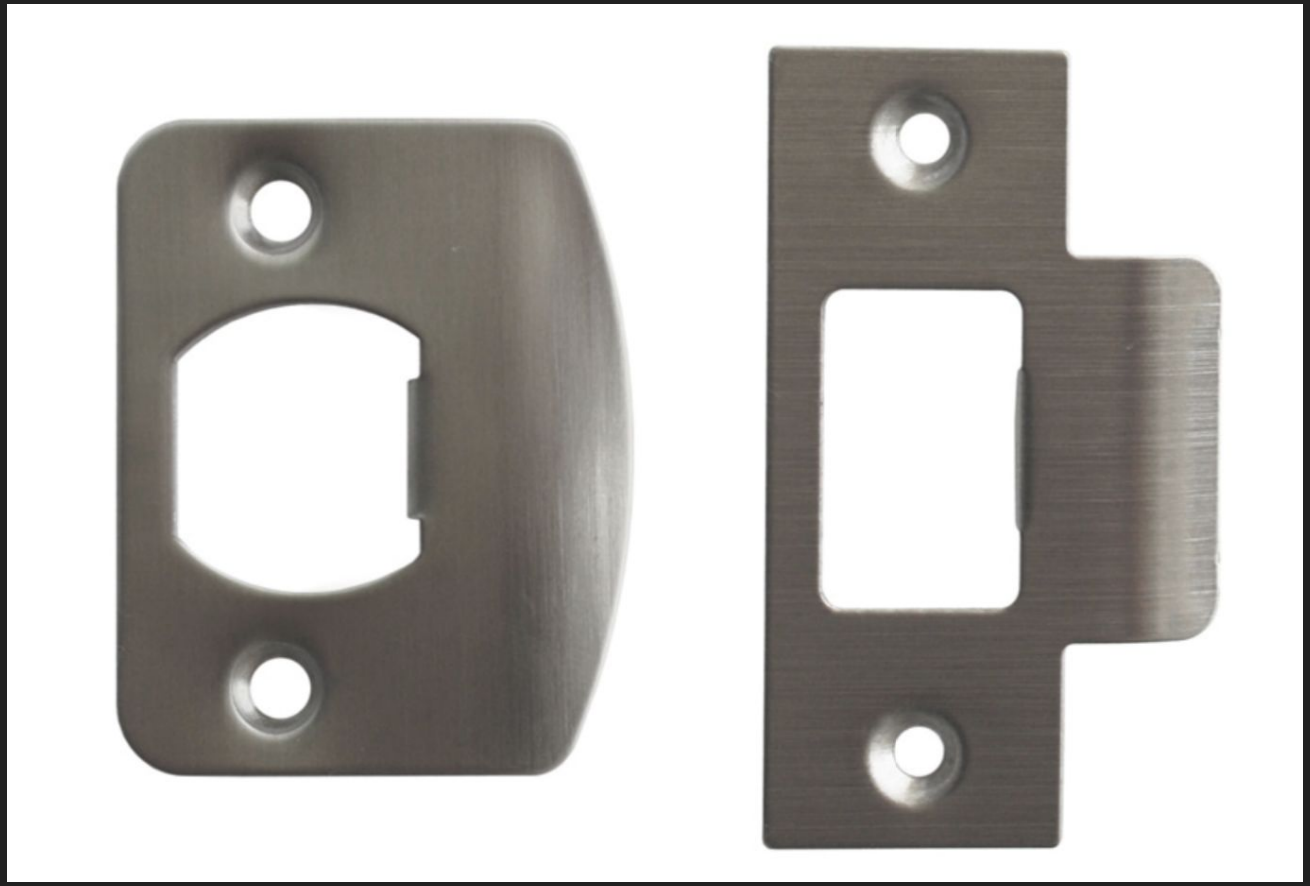


Dead Latches Require Proper Fitment



Dead Latches

Dead Latches



Crash Bars

Crash Bars

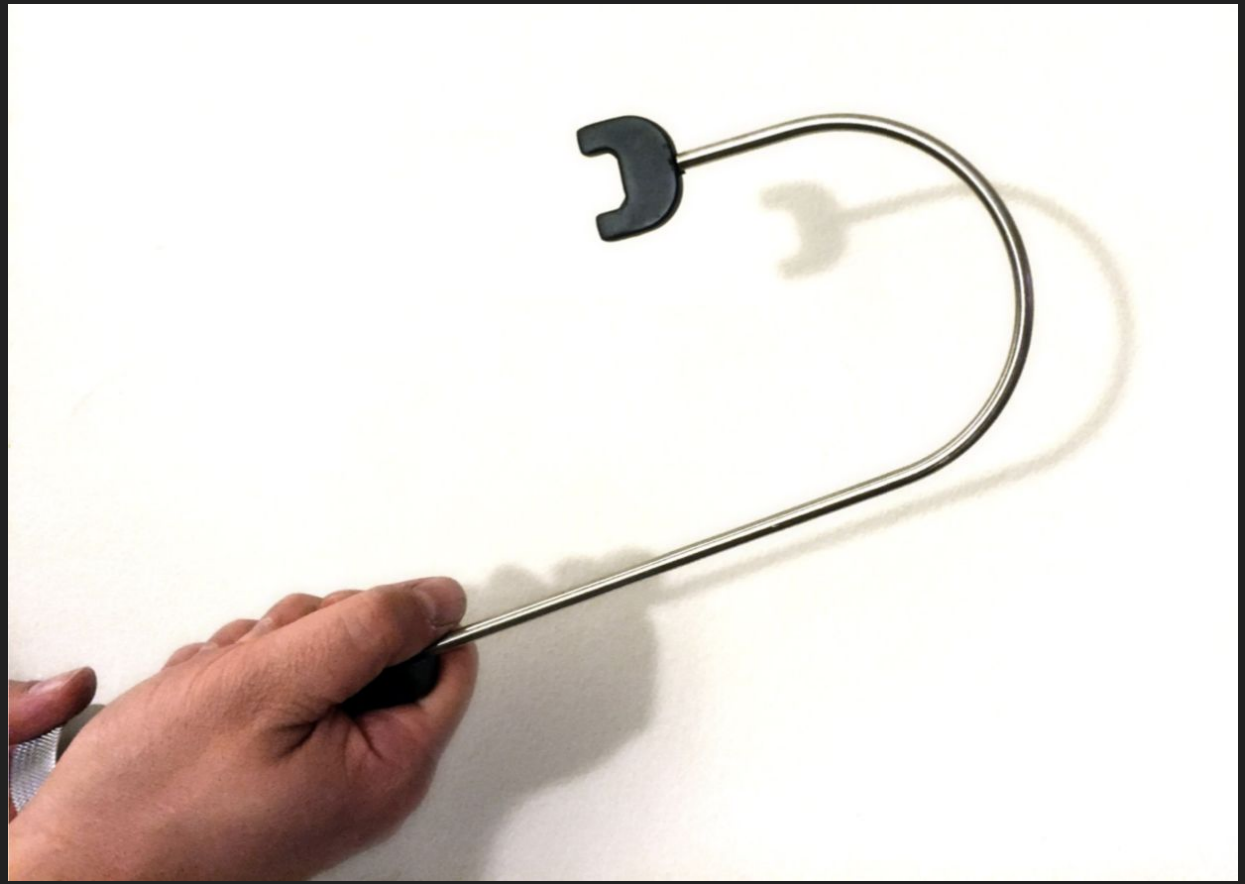
Crash Bars

Crash Bars

Crash Bars

DeadBolts

Dead Bolts



REX Sensors

REX Sensors

REX Sensors

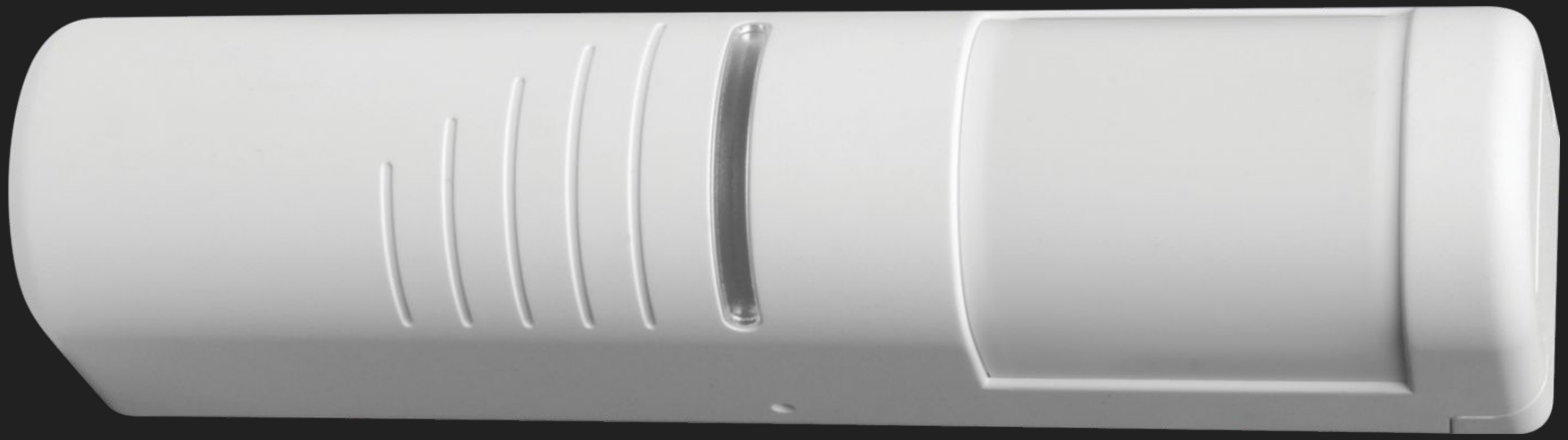
REX Sensors

REX Sensors

REX Sensors

REX Sensors

REX Sensors - The Fix



Door Handle Attacks

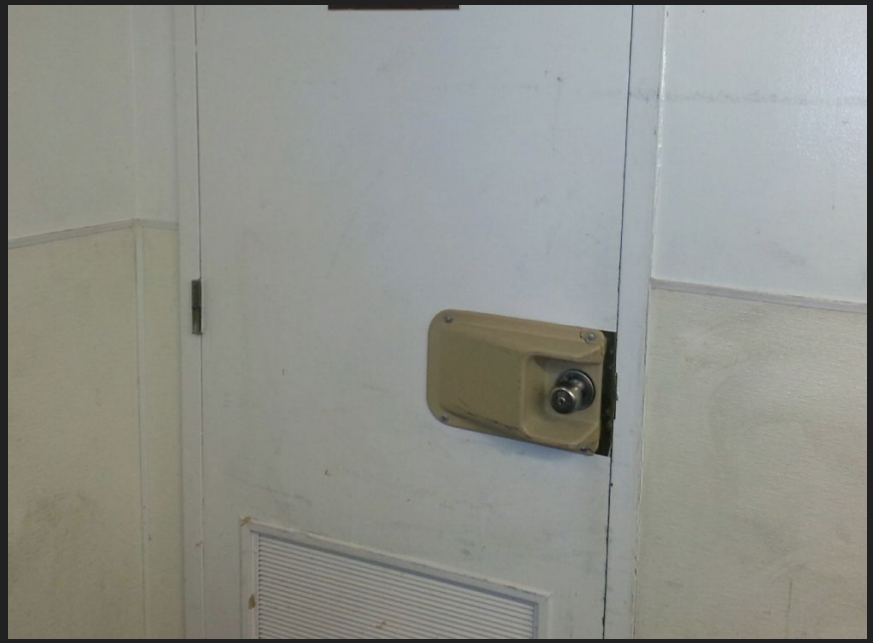
Under Door Tool

Under Door Tool

Under Door Tool - The fix?

Under Door Tool

Under Door Tool - Prevention



Under Door Tool - Prevention

The default creds of physical security

Stealing Keys!

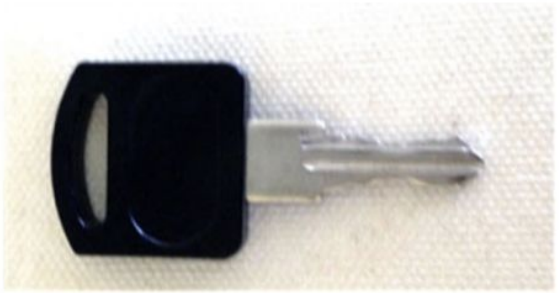
Key Boxes

Telephone Access Boxes

Keyed Alike Systems

Keyed Alike Systems

Home > Select Products > **Gate Operators & Accessories** > Keypads , Card Readers and Fire Boxes >



A126

A126 Linear Key

Availability:: in stock
Product Code: KEY LINEAR

Product Price: **$5.24**

Qty: 1 ADD TO CART

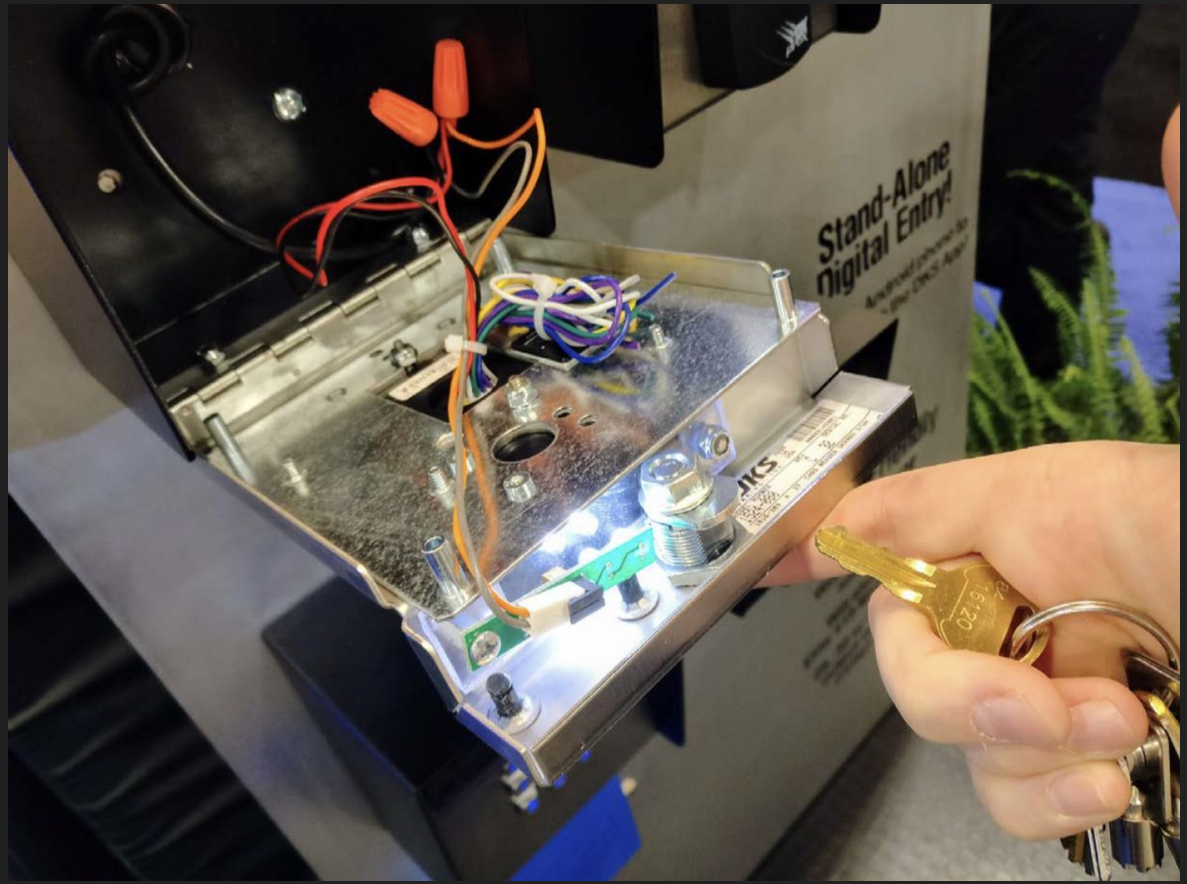
G+1 Like 0 Share

View Quantity Discounts

help

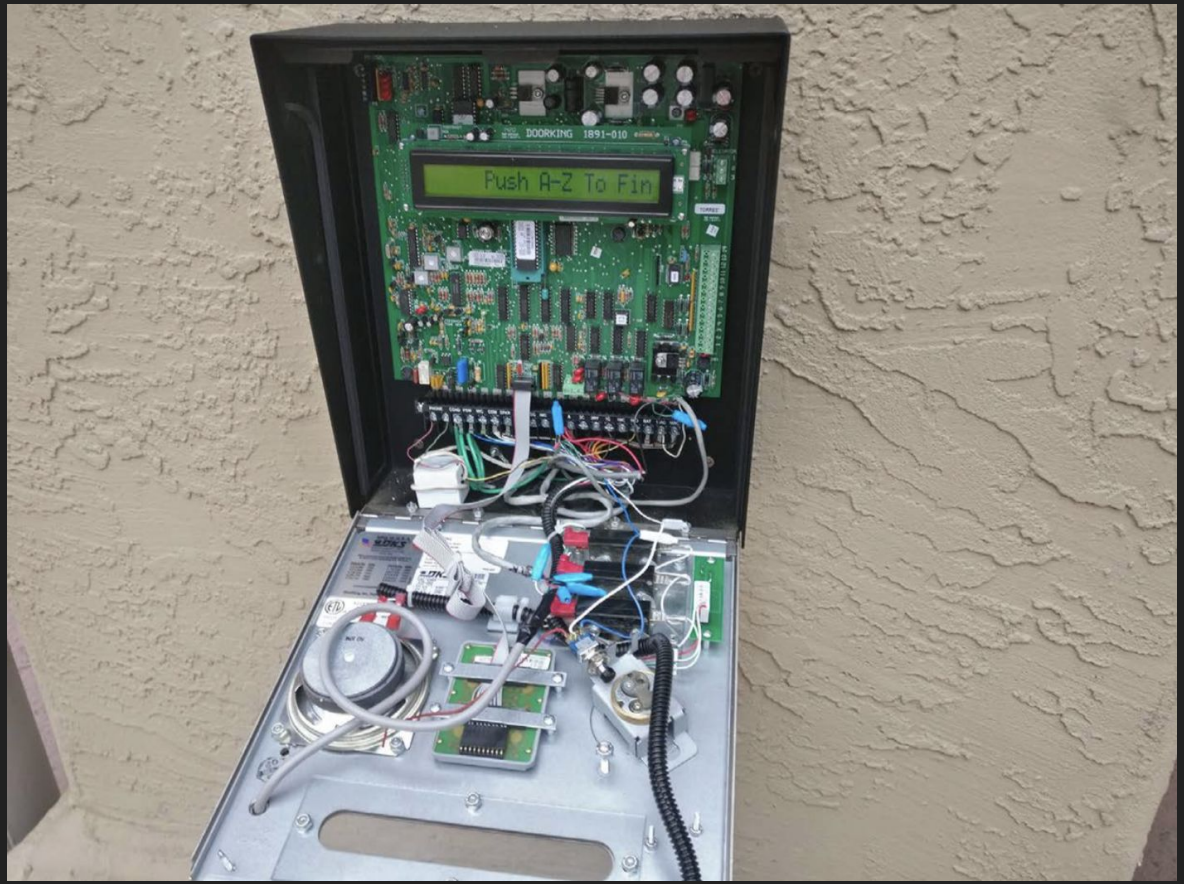
Keyed Alike Systems

Keyed Alike Systems

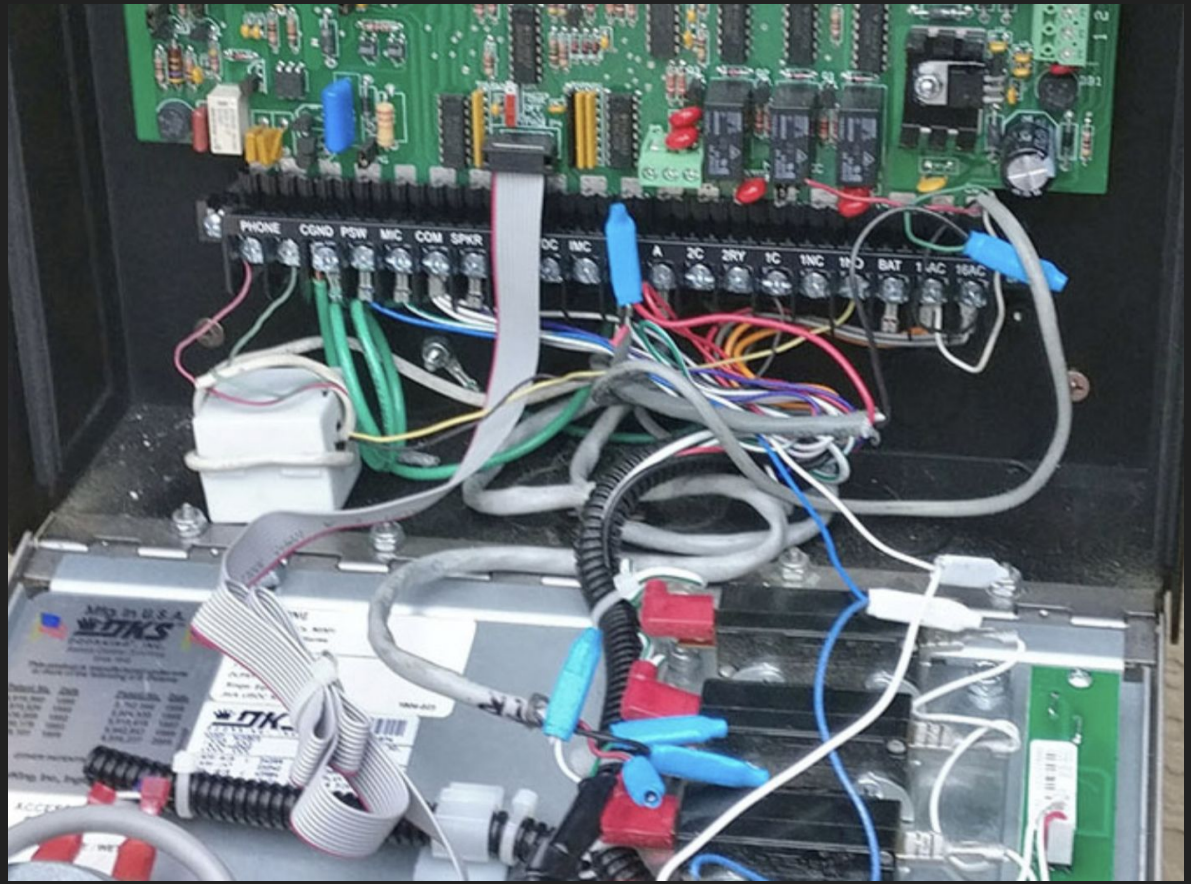


Keyed Alike Systems

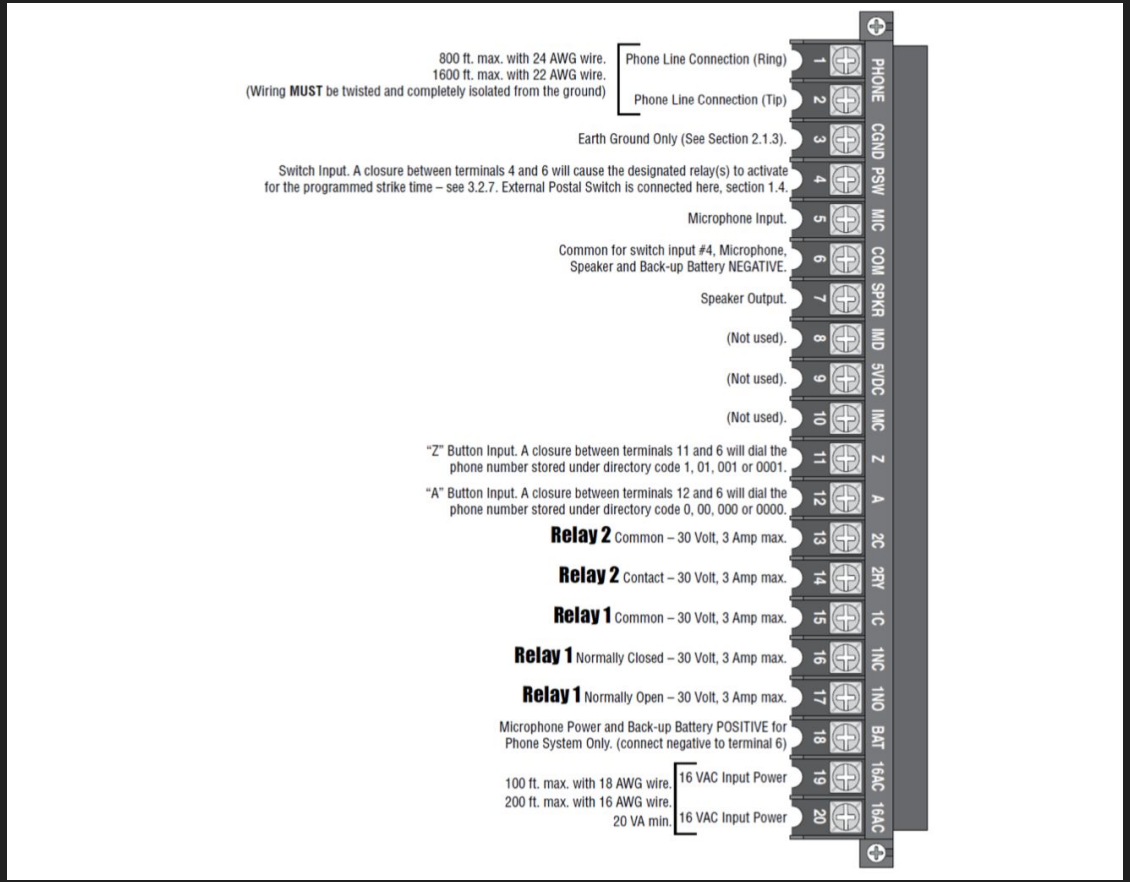
Keyed Alike Systems



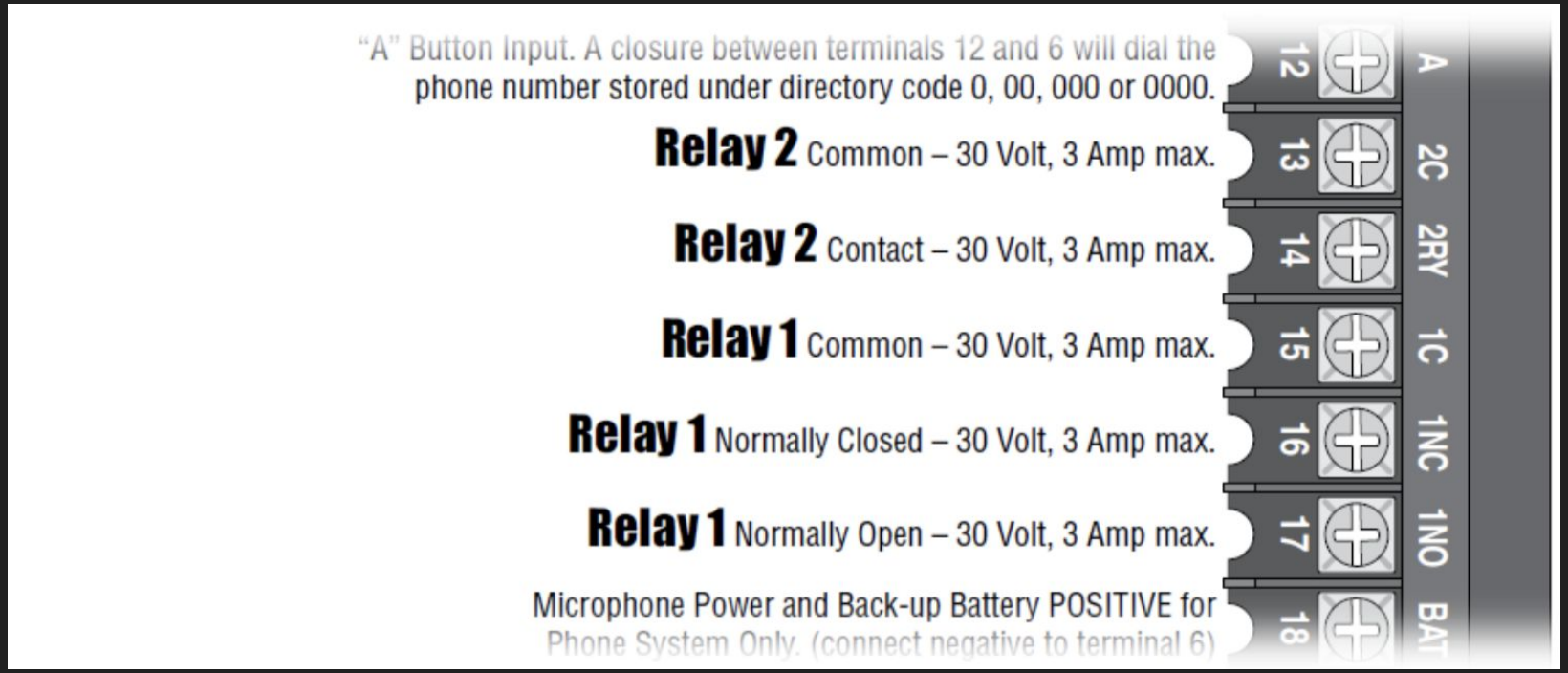
Keyed Alike Systems



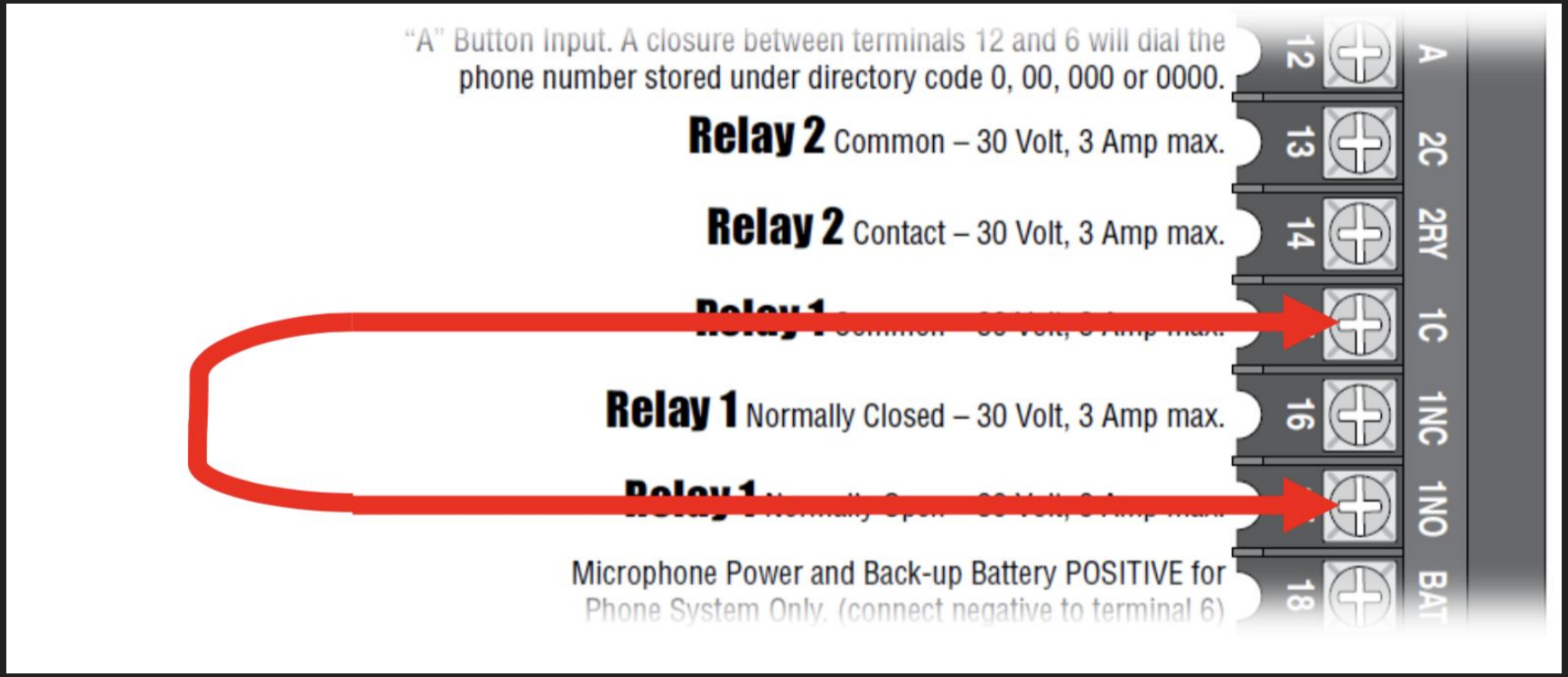
Keyed Alike Systems



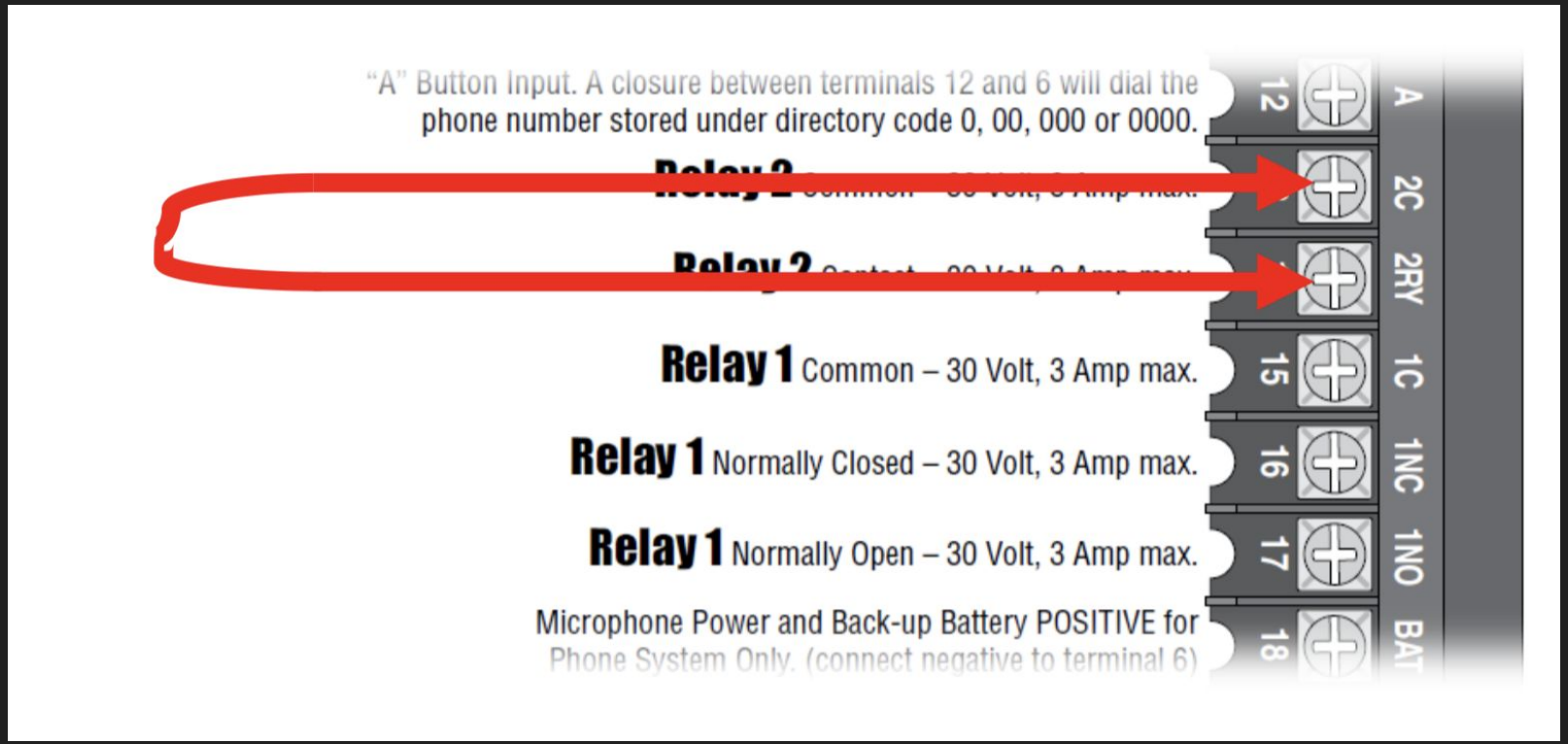
Keyed Alike Systems



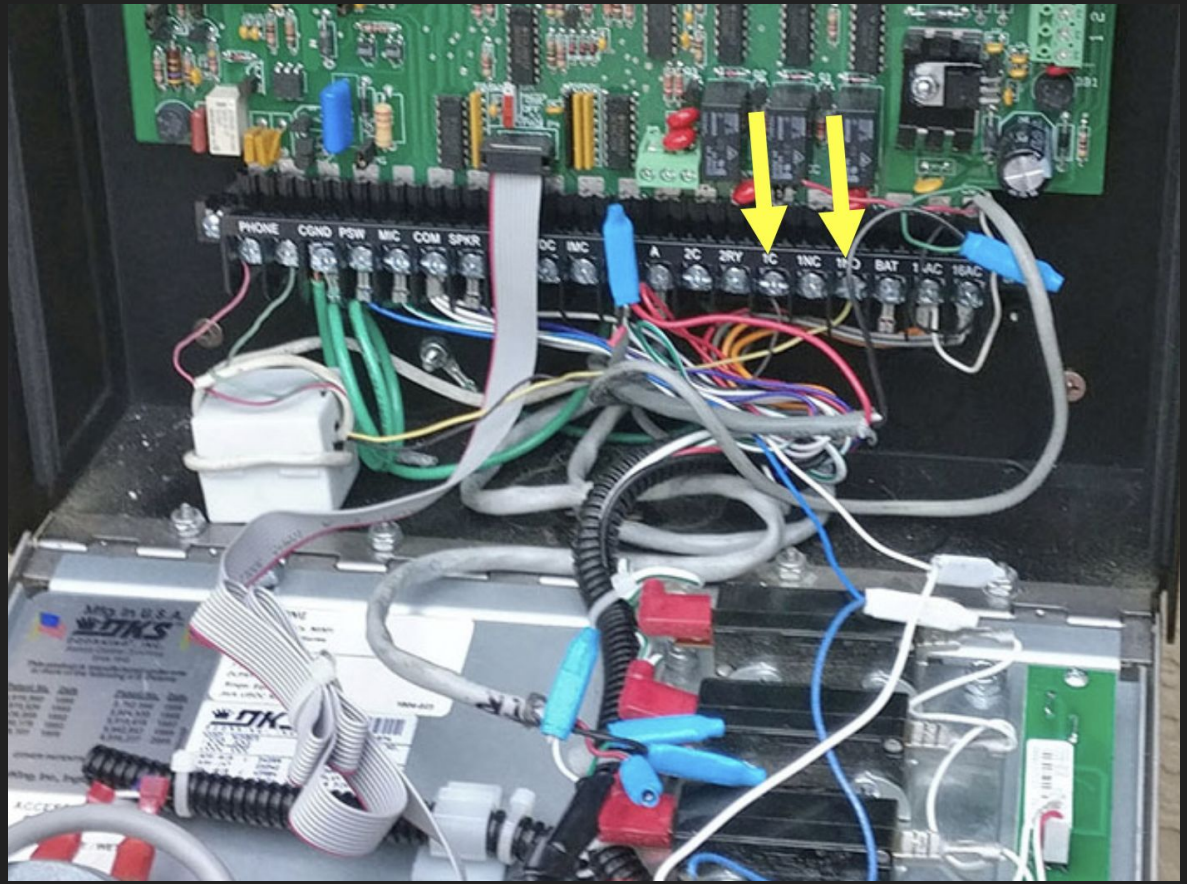
Keyed Alike Systems



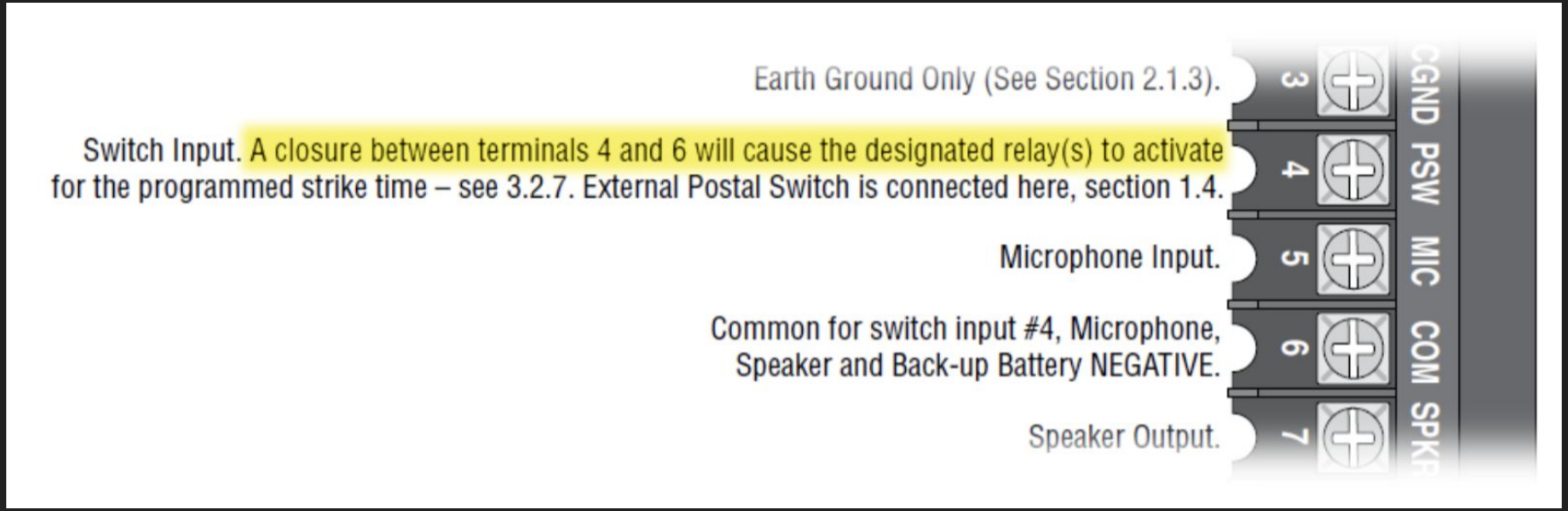
Keyed Alike Systems



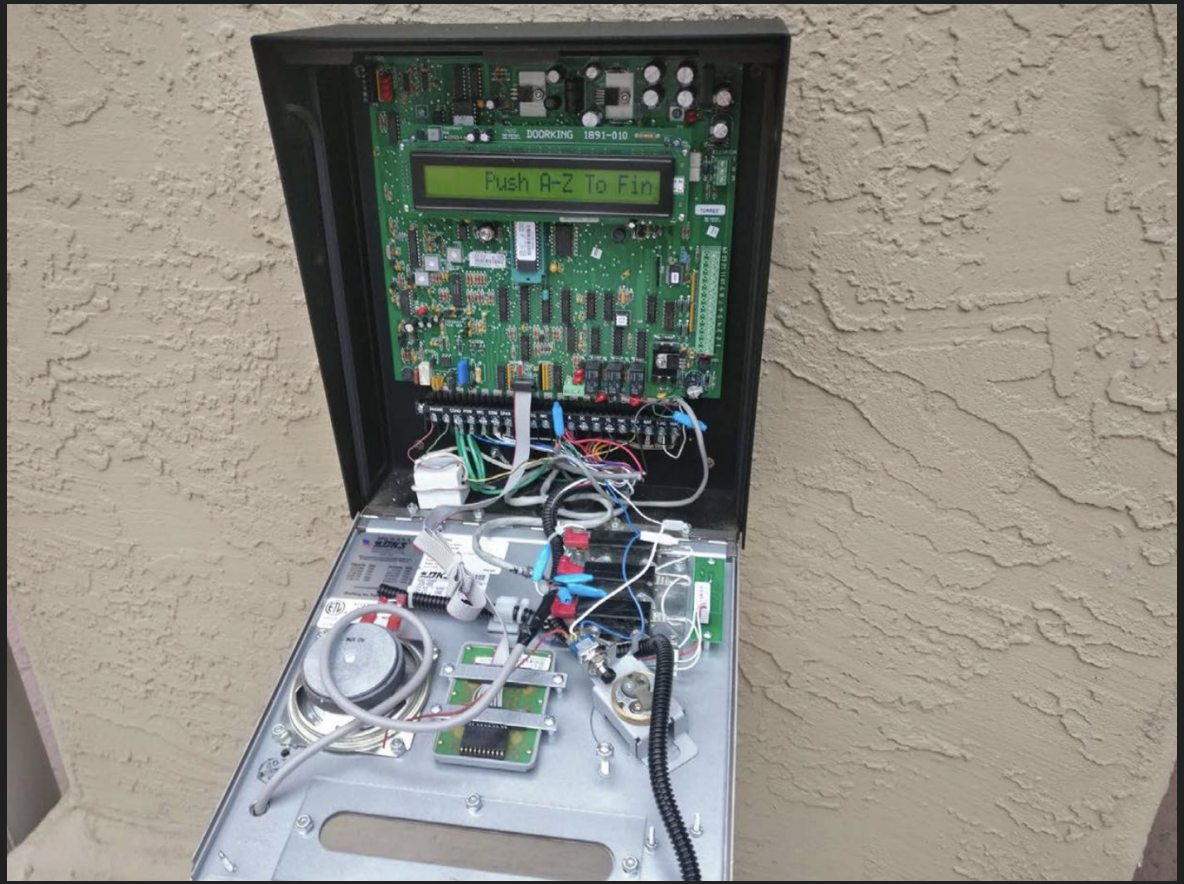
Keyed Alike Systems



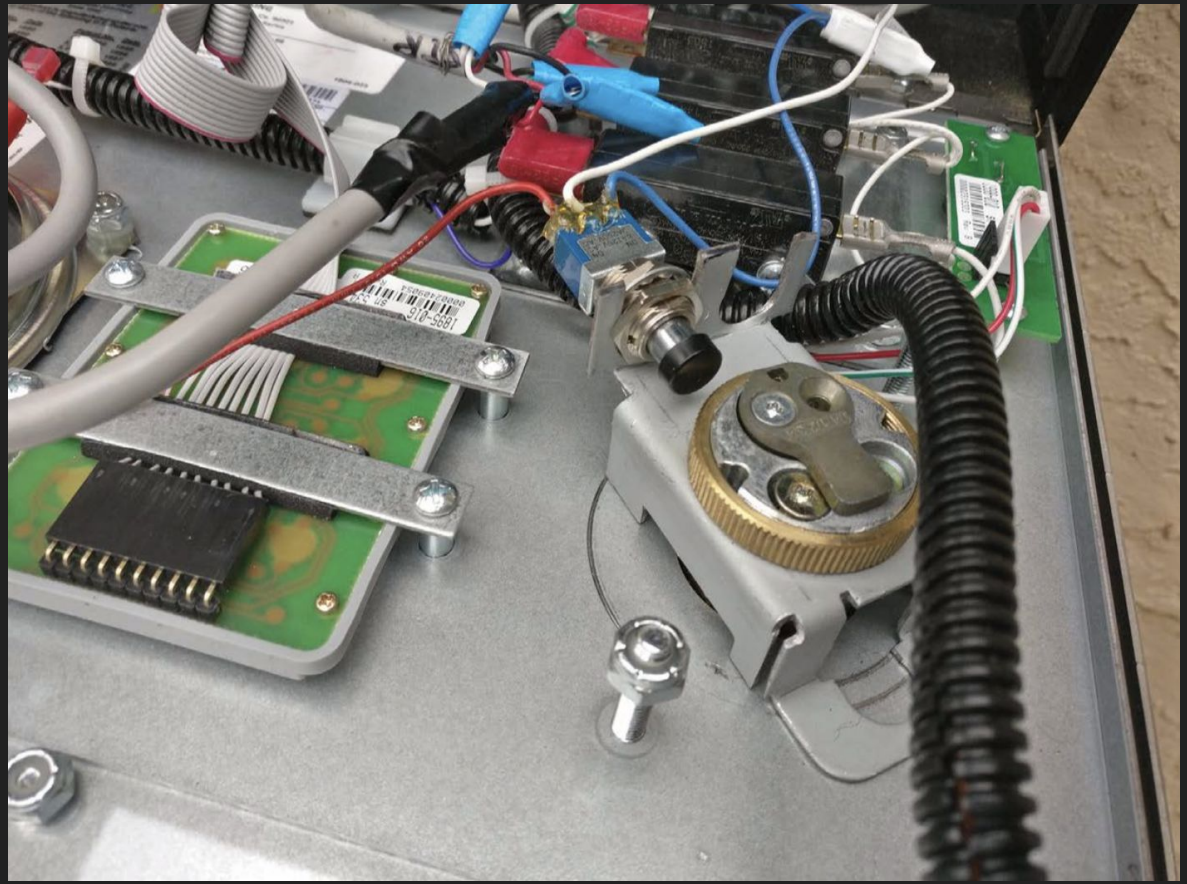
Keyed Alike Systems



Keyed Alike Systems



Keyed Alike Systems



Common Keys to the Kingdom

FEO-K1

C415A

CH751

1284X

Jigglers

Wire Loop

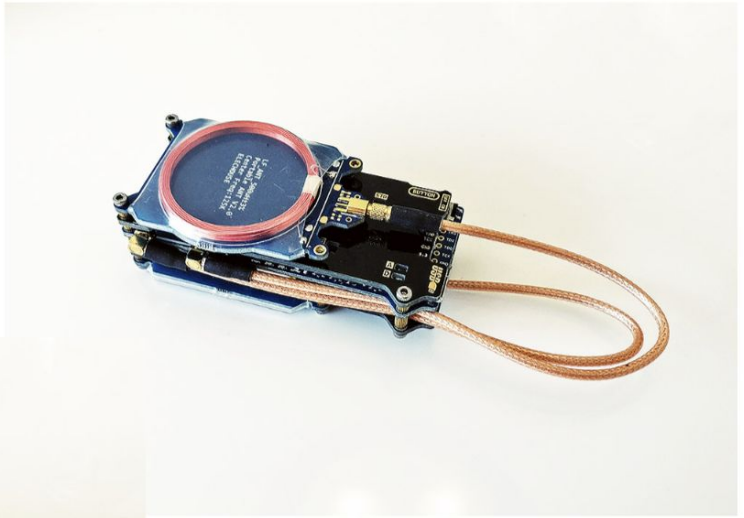
16120

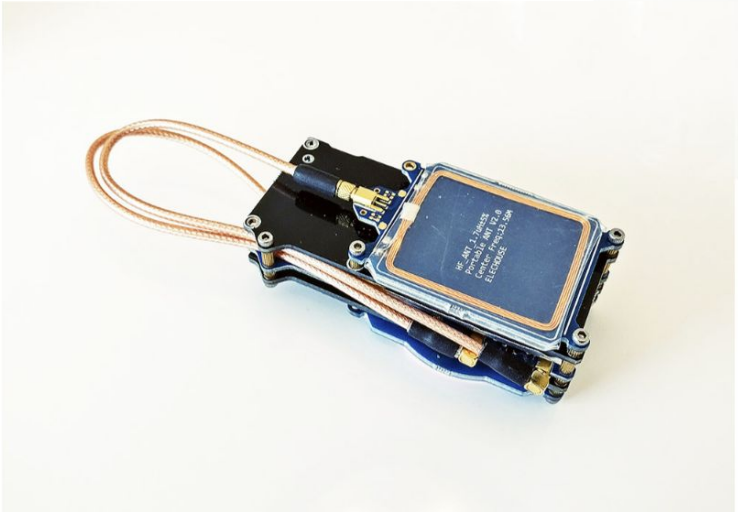
222343

Cuff Key

Attacking Electronic Locks

Attacking Electronic Locks





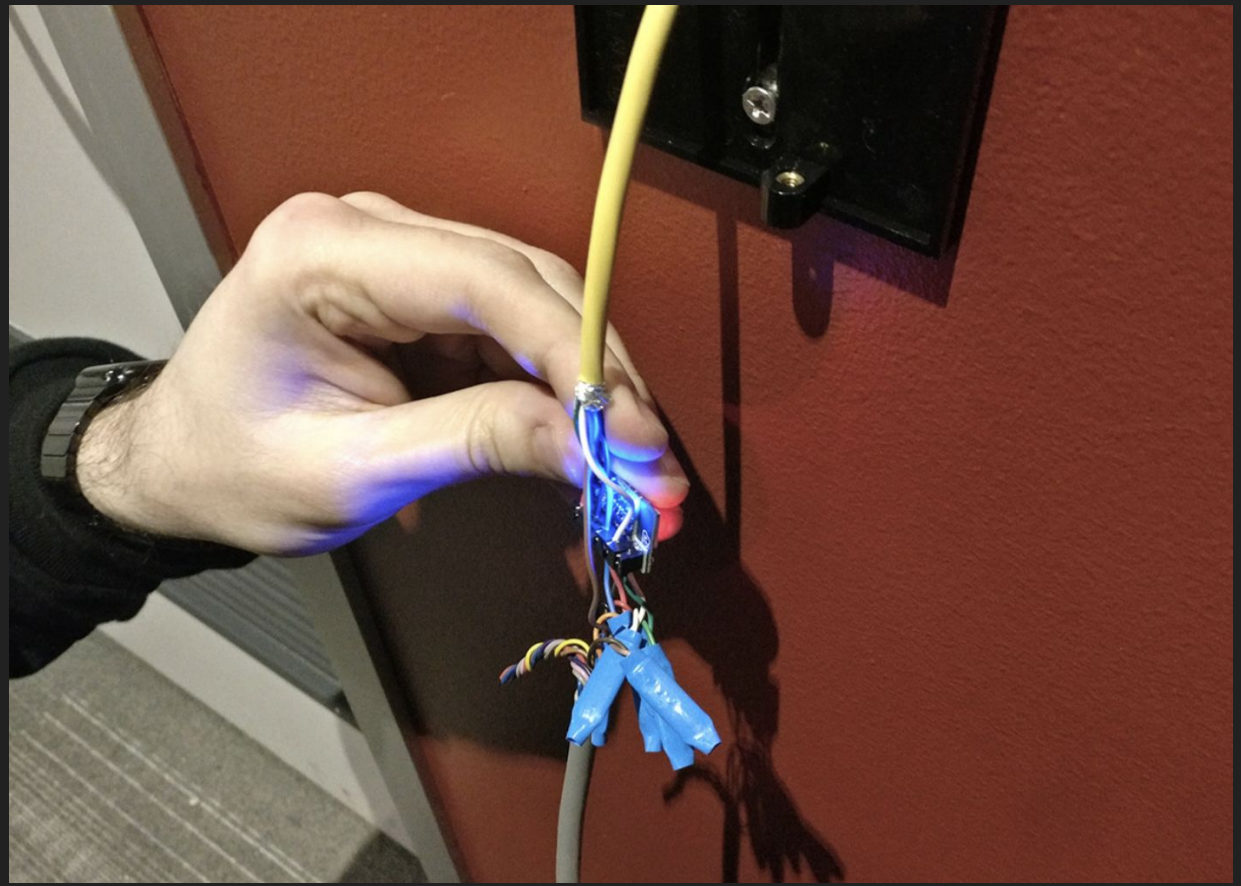
Attacking Electronic Locks

Attacking Electronic Locks

Attacking Electronic Locks

Attacking Electronic Locks

Attacking Electronic Locks



Attacking Electronic Locks

Environmental

The following conditions and utilities must be maintained in server spaces:

- Cooling and humidity conditioning
- Domestic, fresh water
- Drainage
- Chilled, conditioned water
- Temperature change regulation
- Static electricity discharge protection
- Safety Systems such as fire detection
- Sprinklers / Heat and Smoke Detectors
- Steady electric flow (spikes in voltage and current are bad)
- Proper maintenance of mechanical, electrical and life-safety components.

Environmental

Conditions need to be monitored on a 24/7 basis against threats

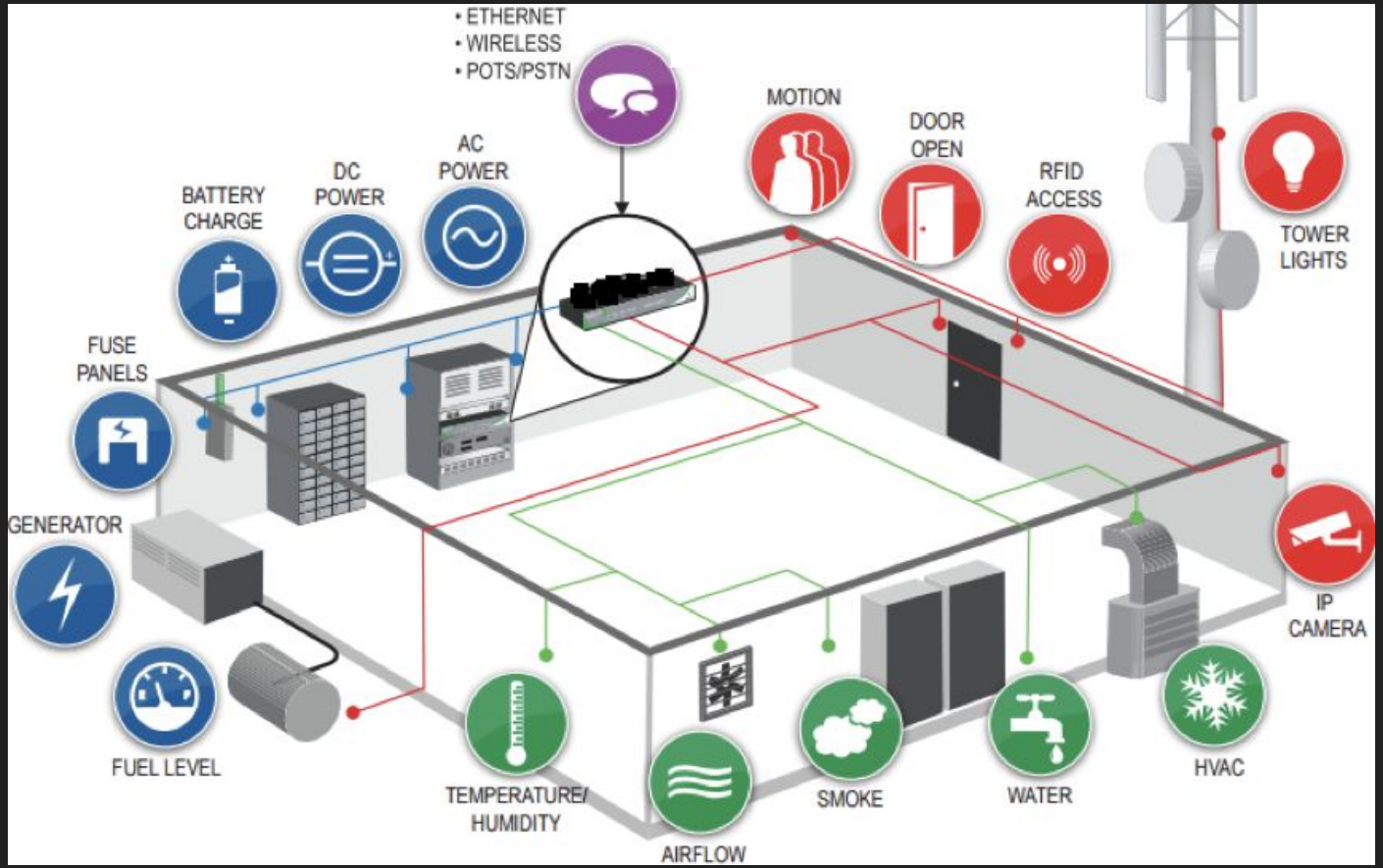
Monitoring sensors and systems need to:

- Be deployed in a variety of locations throughout the server room space
- Automatically notify personnel upon event detection.

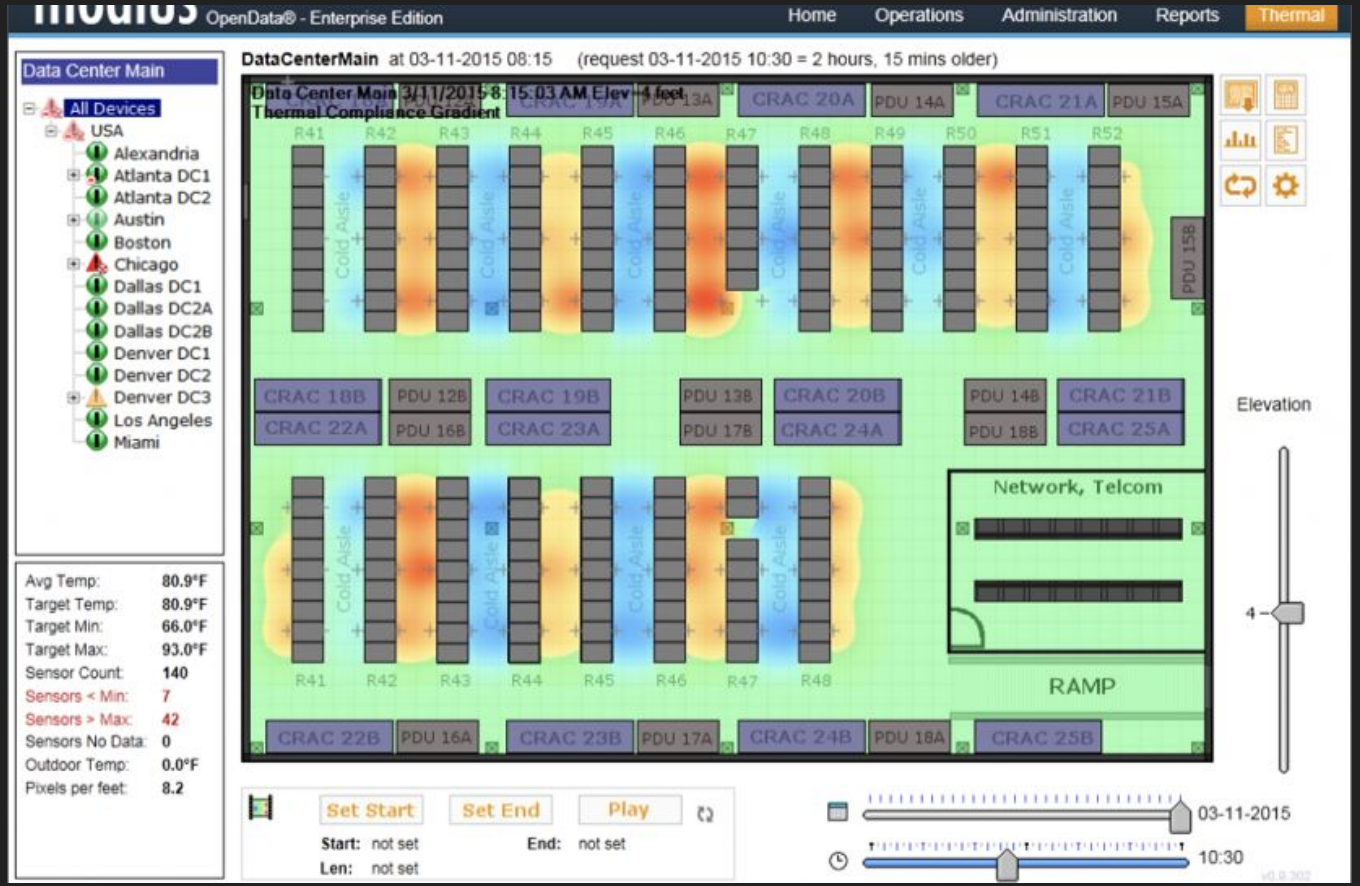
Sensors can include:

- Temperature/humidity
- Fire suppression activation
- Water detection
- Power failure
- UPS/PDU discharge
- Intrusion detection

Environmental



Environmental



Fire Suppression

Fire suppression systems in server spaces are designed to suffocate rather than drown a fire

The suffocation of a fire usually involves pumping an inert, sometimes toxic, gas into the server space, in an effort to starve a fire of oxygen

In the event a fire cannot be controlled using an inert gas, secondary systems kick in using classical water and sprinkler heads

Fire Suppression

The problem of course with this is that if the suppression process can suffocate a fire, it can also suffocate a person

Server rooms must have emergency cut-off switches for both the fire suppression systems and electric flow

Flooding

Floods or pooling can happen for any variety of reasons:

- Burst piping (Sprinklers, Liquid Cooling, etc)
- Cooling runoff
- Condensation on liquid cooling lines
- Fire suppression activation
- Backflow

Raised Floors

Raised floors:

- Are static electricity resistant, reducing the risk of accidental static discharge
- Allow for the efficient flow and circulation of cooled air
- Gives a little bit a wiggle room in the event of a flood or pooled water

Human Security

Social Engineering

Social Engineering

> Any act that influences a person to take an action that may or may not be in their best interest

Examples of Social Engineering

- **Phishing**: The practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information
- **Vishing**: The practice of eliciting information or attempting to influence action via the telephone, may include such tools as “phone spoofing“
- **Impersonation**: The practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system

Social Engineering

Questions?

What questions do you have?

Key Ideas

- Layers of physical security (What is the purpose of each?)
- Common controls that can be implemented depending on budget
- Common oversights that allow bypass of security

References

- Anixter - The Four Layers of Data Center Security - White Paper
- Deviant Ollam - You’re Probably not Red Teaming
- Digitalocean - DC Security White Paper
- Cisco - Securing Enterprise Networks Whitepaper