An Integrated Approach to Physical Security – Best Practices

Best Practices to Implement

Background:

- Bachelors, Civil Engineering; Construction Management
- Masters, Public Health, Epidemiology and Biostatistics
- CPTED Certification
- Industry, military, and government related research and grant experience
- Non-Profit and Education Sector Consulting
- Certificate in Education Financing

Background:

9 Jurisdictions/ 16,000 Students / 50 Schools

Challenges

- Asset rich/cash poor
- Some funding available but not spent in a systematic, coordinated way to impact the system

Needs

- Comprehensive, systems-based strategy for physical security improvements
- Assessment of assets/policies and procedures
- Standards
- Funding strategy
  - Grants
  - Remove barriers to applying

Results

- ~$4 Million in 3 years
- Security improvements that also addressed capital improvements

Learning Objectives

1. **Understand the security landscape and the threats to Houses of Worship**

2. **Understand the basic premise of planning for security**

   – Understand the challenges to be solved for the end user and ensure the best solution.

3. **Identify hardware applications appropriate to the opening**

   – Understand After-Action Reports, the Federal Commission on School Safety, and CPTED best practices.

3. **Understand the importance of building relationships with vendors**

   – Educate Owners on planning for security and implementing best practices.

Security Landscape at a Glance

Catholic Church:

- 289 attacks between May 2020 and Feb 2023
- 130 incidents post Dobbs v. Jackson’s Health Organization

Source: https://catholicvote.org/tracker-church-attacks/

Family Research Council:

- 2023 – 436 incidents
  - Double the number from 2022
  - 8x the number in 2018
- Hostility against US Churches is accelerating

Source: https://www.frc.org/issueanalysis/hostility-against-churches-is-on-the-rise-in-the-united-states

Jewish Community:

- Anti-Defamation League reported anti-Semitic incidents reached all time high in 2021 – 2717 incidents
- Since Oct 7, attacks on the Jewish community have been increasing in every category
- On avg 61% year over year increase

Muslim Community:

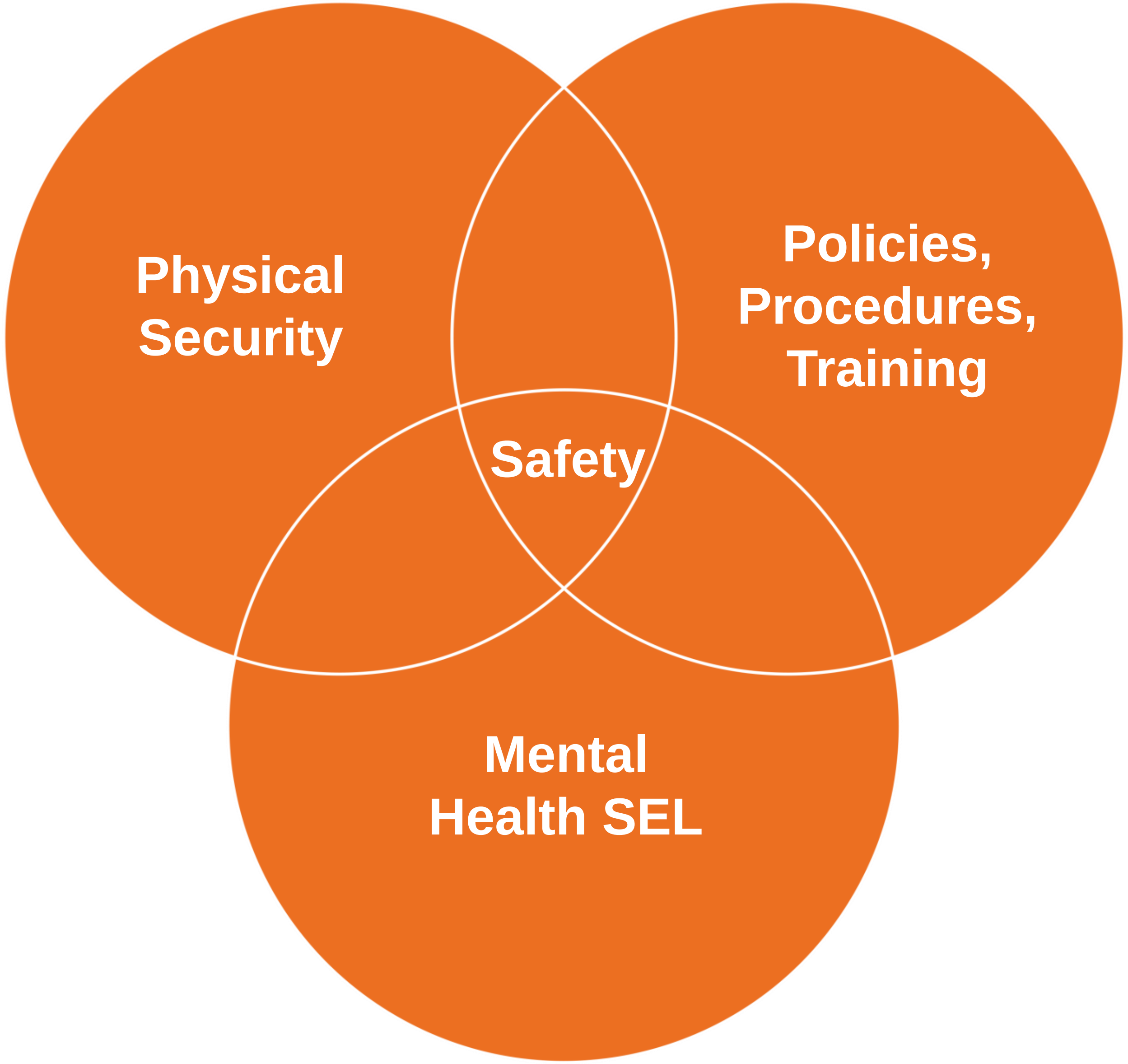
- Attacks on the Islamic community continue to increase in the United States with arson and vandalism at mosques, cemeteries, and schools.
- Buildings have been damaged by bullets, bombs, graffiti, eggs, and animal remains.

Source: https://www.asisonline.org/security-management-magazine/articles/2023/03/extremism-and-houses-of-worship/extremism-against-places-of-worship/

Understanding Safety vs Security – Does it Matter?

Words Matter

- How we define terms influences how we plan and address issues
- **Security** is **external** to the individual
  - Security is protective physical, emotional, and environmental measures in conjunction with training, policies and procedures
- **Safety** is **internal**
  - Safety relates to an individual's perception of feeling free from harm or danger



Creating a Systems Based Approach

Prevention

Reduce number of threats/increase probability of detection

- Threat Assessment/Reporting
- Mental Health
- Vulnerability Assessments
- School Climate Initiatives

Protection and Mitigation

Detect/Delay/Deny incidents and limit consequences

- Physical Security Improvements
- Security Policies and Procedures
- Training/Exercises
- Drills
- Tiplines/Anonymous Reporting

Response/Recovery

Remedy consequences and resumption of normal operations

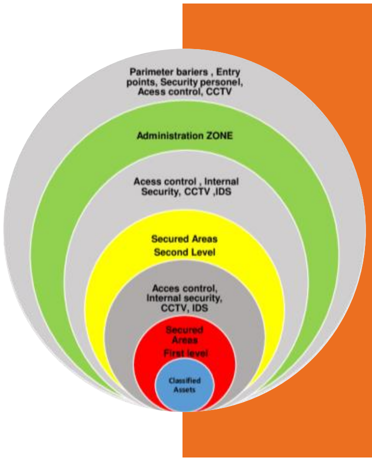
- Training and Exercises
- Continuity of Operations Plan
- Resumption of Normal Operations

Understanding the Elements of Physical Security

Integrated "system" that works together to maximize return

Physical security **begins** at the **perimeter** and **works inward**

Physical improvements provide the most benefit when integrated with other parts of the system


Parimeter bariers , Entry points, Security personel, Acess control, CCTV
Administration ZONE
Acess control , Internal Security, CCTV ,IDS
Secured Areas Second Level
Acces control, Internal security, CCTV, IDS
Secured Areas First level
Classified Assets

Multiple layers of safety and security measures before reaching the interior of the school or building

4 D's of Physical Security

Deter

Detect

Delay

Deny

Deter

Measures that prevent an attack or threat from happening

Visual deterrents that communicate legitimate use and users

- Public
- Semi-Public
- Private

EXAMPLES

– Fencing

– **Lighting**

– **Landscaping**

- Signs

- Locked Facilities

– Presence of Security Measures

– **Cameras**

– **Sensors**

Detect

Measures that detect the presence of a threat

Systems that detect and alert in the presence of a threat

- Physical Security
- Human Capital
- Situational Awareness

EXAMPLES

– **Video Surveillance** (with monitoring)

– **Intrusion Detection Systems**

– Staff Training

– Presence of Security

Delay

Measures that slow down an attack or increase the level of effort needed to allow the incident to occur

Systems that detect and alert in the presence of a threat

- Physical Security
- Policies and Procedures
- Communications

EXAMPLES

– **Secured Openings**
– Laminate Glass
– Barriers, Bollards, Fencing, Gates
– **Ability to Lockdown – Compliance and Training**
– **Mass Notification Software**

Deny

Measures that prevent or restrict access to valued assets

Systems that deny access to valuable resources

- Physical Security
- Policies and Procedures
- Technology

EXAMPLES

– **Locks/access control with ability to lockdown remotely**

– Key/credential control / Policy on Use

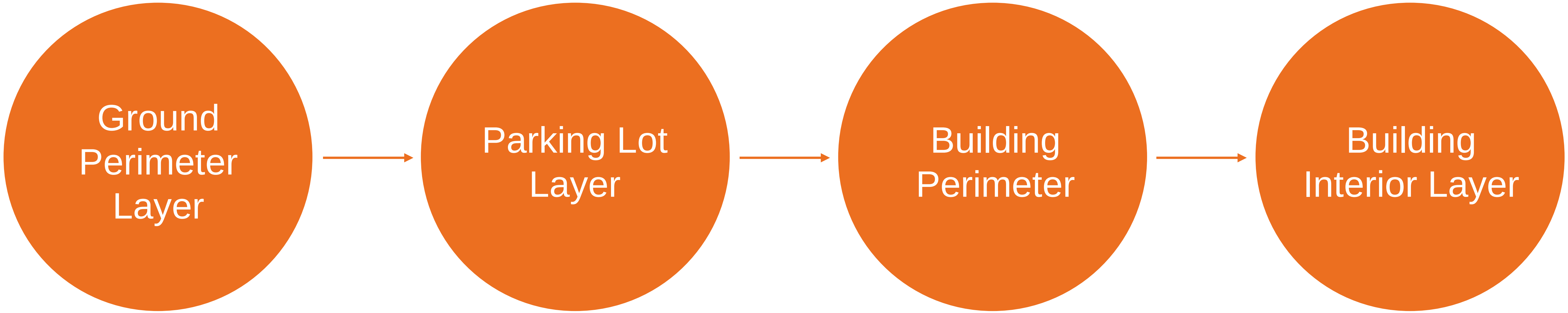
– Restricted use of facility

– **Partitioned Networks**

– **Secured Networks and Edge Devices**

– Policies on email/passwords

Work From The Outside In – NOT The Inside Out



Ground Perimeter Layer

Parking Lot Layer

Building Perimeter

Building Interior Layer

Demarcation of Public/Private Space:

Deterrence is the primary objective

Identification of Legitimate Vs Illegitimate Users:

Detection is the primary objective

Prevention of Illicit Users Intent on Harm from Gaining Access:

Delay/Deny are the primary objectives.

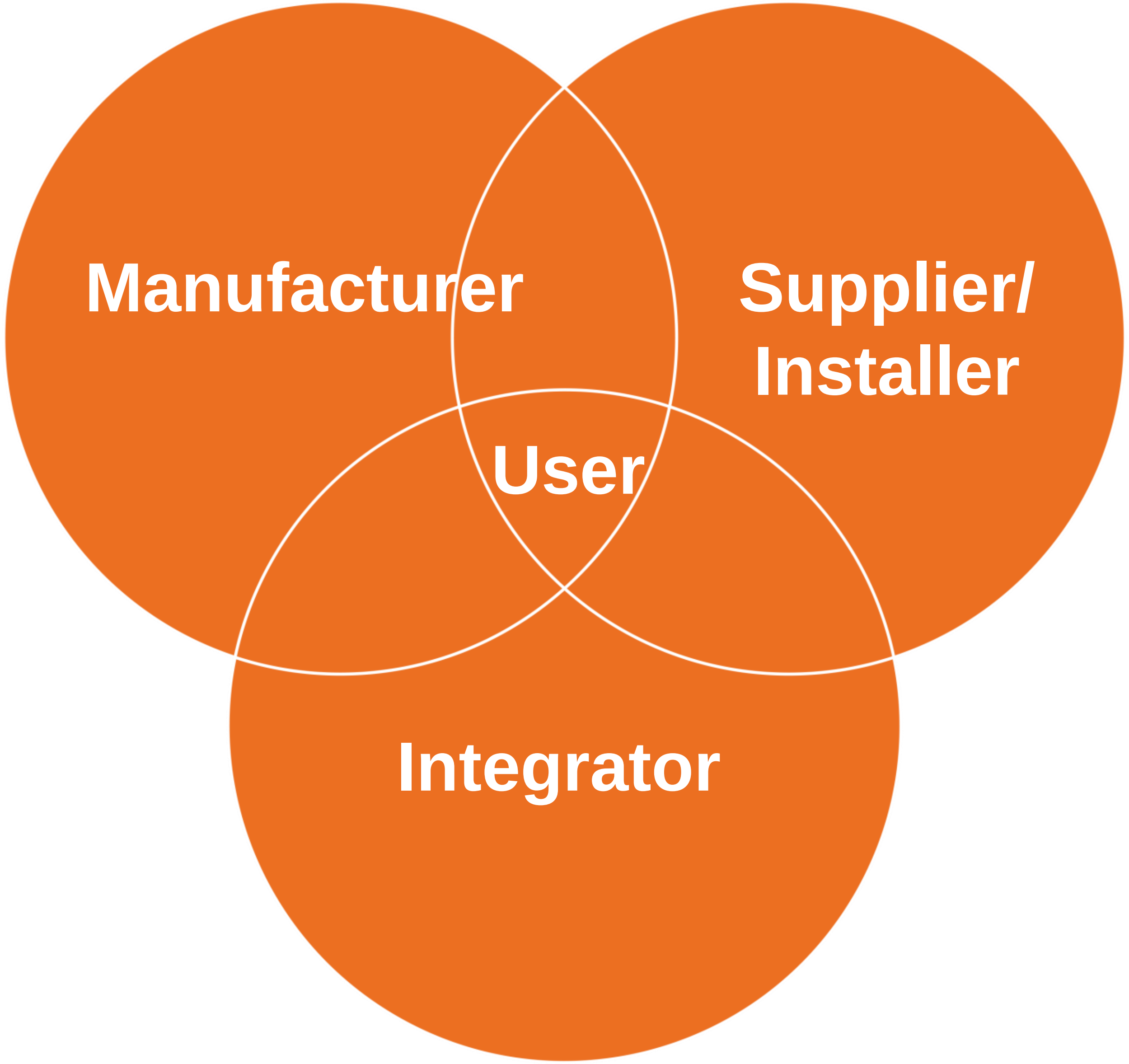
Protection of most valuable assets – people/property/data

DENYING access is primary objective

Understanding the Interplay of Roles

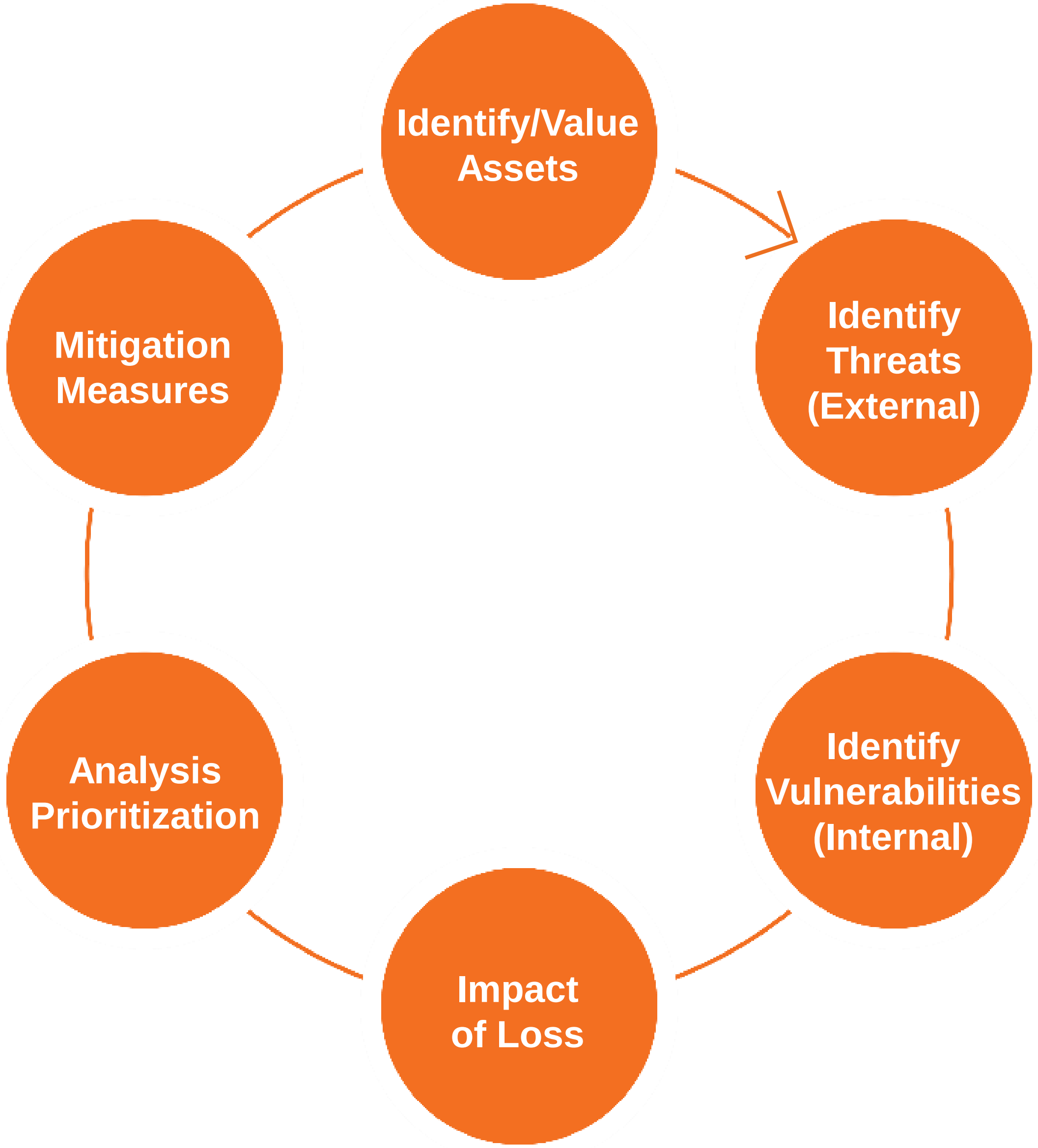
It takes a supplier/installer, manufacturer, and integrator working together to provide an end user the best solution and experience

- Managing these relationships with end users creates robust solutions
- Structuring/streamlining process is essential
- Process is systematic and efficient if done correctly
- **End User trusts the end result and team**



Integrating Best Practices with an Evidence Based Approach

Where To Start... At The Beginning



Assess before you address

- Poor decisions
- Solutions that do not work
- Solutions that are in conflict

Need to understand risk

- Risk is the intersection of vulnerability and threat

Prioritize needs based upon analysis

Identify all mitigation measures

An interdisciplinary approach is critical to avoid

- Silos
- Duplication of efforts
- Impact on the parts - not the system

Asset Identification And Valuation

Step 1

- Define and understand primary business functions and processes

Step 2

- Identify site and building infrastructure and systems
  - Life Safety Systems
  - Mechanical Systems
  - IT Network
  - Secure or Restricted Areas

Step 3

- Identify tangible and intangible assets
  - People
  - Data
  - One-of-a-Kind Assets
  - Reputation

Valuation:

- Injuries/deaths related to infrastructure damage
- Replacement costs of assets
- Revenue loss
- Backup/redundancy capability
- Financial losses
- Insurance impact
- Lost business from loss event
- Management time (time directed away from mission)
- Reputational damage / PR costs

Threats (External):

Criminal Threat:

- A person or entity intent on doing harm in retribution for something done or not done

Natural or Man-Made Threats:

- Hurricanes
- Tornadoes
- Earthquakes
- Power failure of the electrical grid

Geography:

- Proximate to Critical Infrastructure
- Geographic Features – Flood plain or earthquake zone

Vulnerabilities (Internal):

Systems:

- Aging infrastructure
- Lack of redundancy or backup
- Ease of access to critical infrastructure or facility
- Hazardous materials

Physical Security:

- Inadequate physical security measures
- Outdated or non-functional equipment
- Lack of understanding of physical security capacity

People, Policies, Procedures:

- No training or inadequate training
- Lack of compliance
- No policies and procedures/inadequate policies

Quantifying Loss And Assessing Risk:

PROBABILITY

IMPACT

	RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
CATASTROPHIC	MODERATE	MODERATE	HIGH	CRITICAL	CRITICAL
SIGNIFICANT	LOW	MODERATE	MODERATE	HIGH	CRITICAL
MODERATE	LOW	MODERATE	MODERATE	MODERATE	HIGH
LOW	VERY LOW	LOW	MODERATE	MODERATE	MODERATE
NEGLIGIBLE	VERY LOW	VERY LOW	LOW	LOW	MODERATE

PROBABILITY

Likelihood an event will occur
– value 1-5

IMPACT

Consequence of event occurring
– value 1-5

RISK

Probability x Impact
– value 1-25

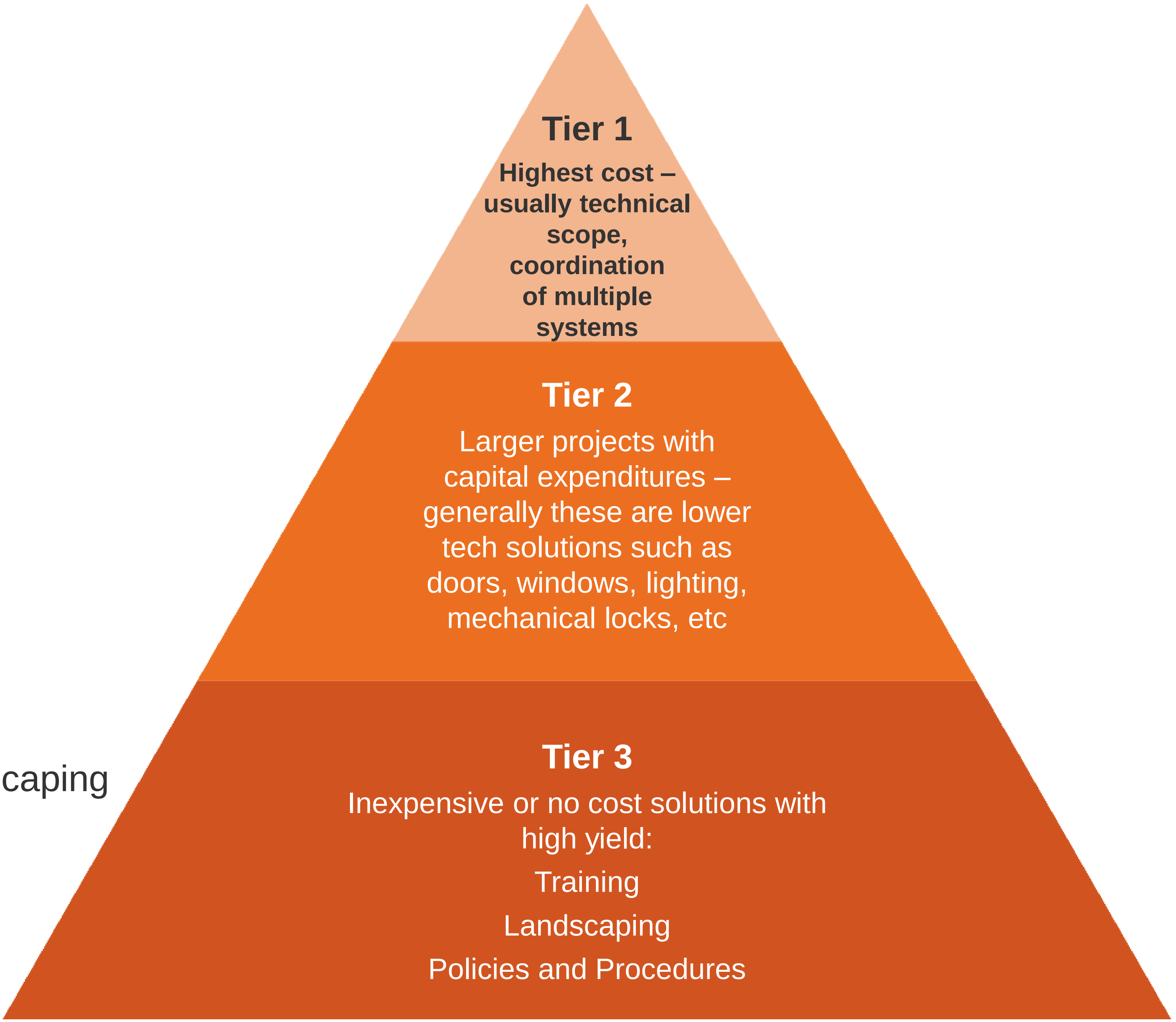
Creating The Plan

ACTION	WHO	OUTCOME
Identification of Assets	Operations, facilities, IT, Finance, Risk, SROs	List of Targets to Address
Vulnerability Assessment	Facilities, Architect/AHJ, LE/EMS, DHS PSA	Identification of Vulnerabilities to Address
Prioritization of Improvements	CFO, Operations, Risk, Facilities, IT, SRO/School Security	Hierarchy of “Security Needs”
Consultations with industry Professionals/Trusted Partners	Manufacturer’s Reps Trusted Partners Security Consultant	Options for Solutions Scope of Work to Be Done Estimates of Probable Costs
Establishment of Budget/ Identification of Funding Sources	Facilities, IT, CFO, Operations, School Board	Identification of Funding, Including Competitive/Non-Competitive Grants
RFPs for Security Improvements	Procurement, Facilities, IT, Operations, Risk, School Board	Contract/Implementation

Analysis Prioritization

Using the data obtained in the risk analysis

1. **Group projects by cost and complexity**
2. **Analyze the risk - determine solution**:
   - Policies and procedures
   - Training
   - Behavioral modification
3. **Evaluate resources available at little or no cost**
   - Volunteers with special skills
   - Community Members with businesses
   - Work that can be done by volunteers such as landscaping
4. **Examine funding strategies:**
   - Grants – Private and Public
   - Capital Improvement Budgeting
   - Donors



Tier 1

Highest cost – usually technical scope, coordination of multiple systems

Tier 2

Larger projects with capital expenditures – generally these are lower tech solutions such as doors, windows, lighting, mechanical locks, etc

Tier 3

Inexpensive or no cost solutions with high yield:

Training

Landscaping

Policies and Procedures

Best Practices for Openings

Best Practices to Implement

What do the evidence and data reflect?

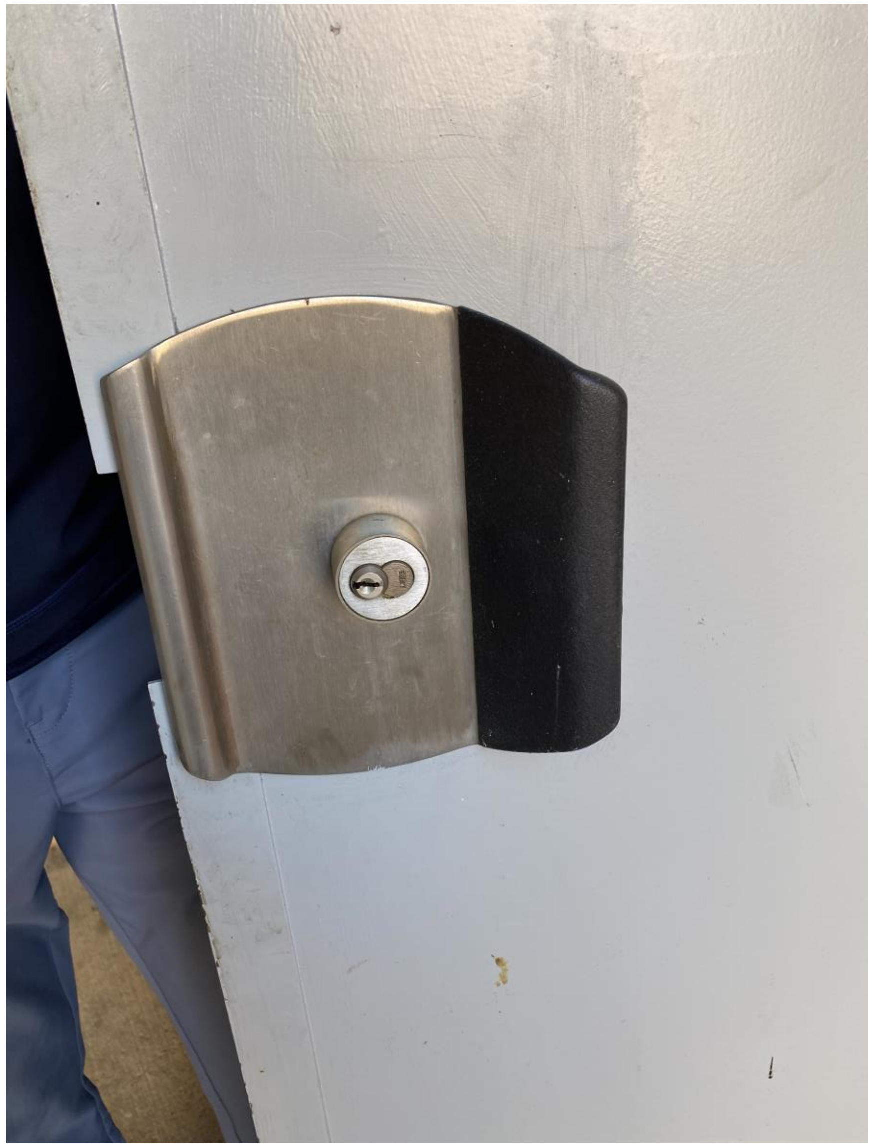
Studies and after-action reports have shown that one particular measure is highly effective and predictive of saving lives….

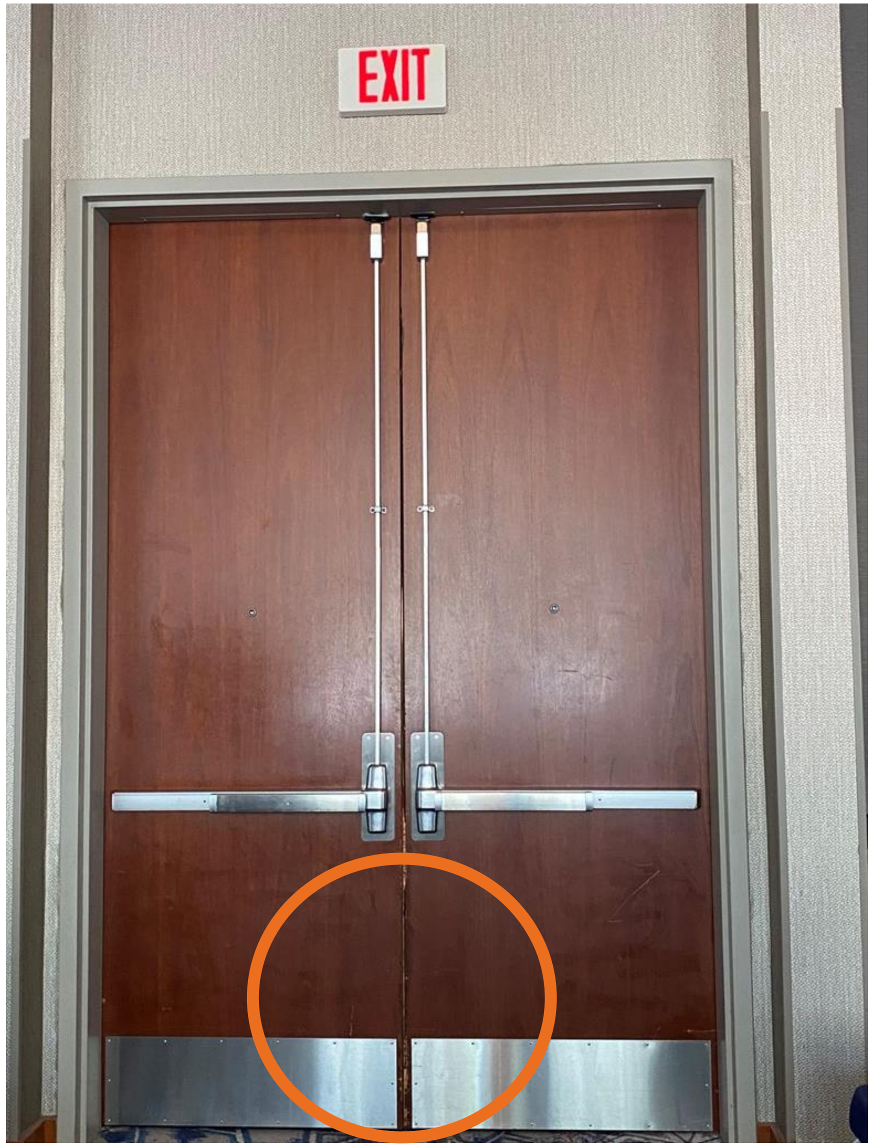
The ability to lockdown a facility and secure classroom doors from the interior of the space.

Sources:

Cybersecurity and Infrastructure Security Agency, 2020), Final Report of the Sandy Hook Advisory Commission, Marjory Stoneman Douglas High School Public Safety Commission, Investigate Committee on the Robb Elementary Shooting: Interim Report 2022

Best Practices – Exterior Openings (Mechanical)

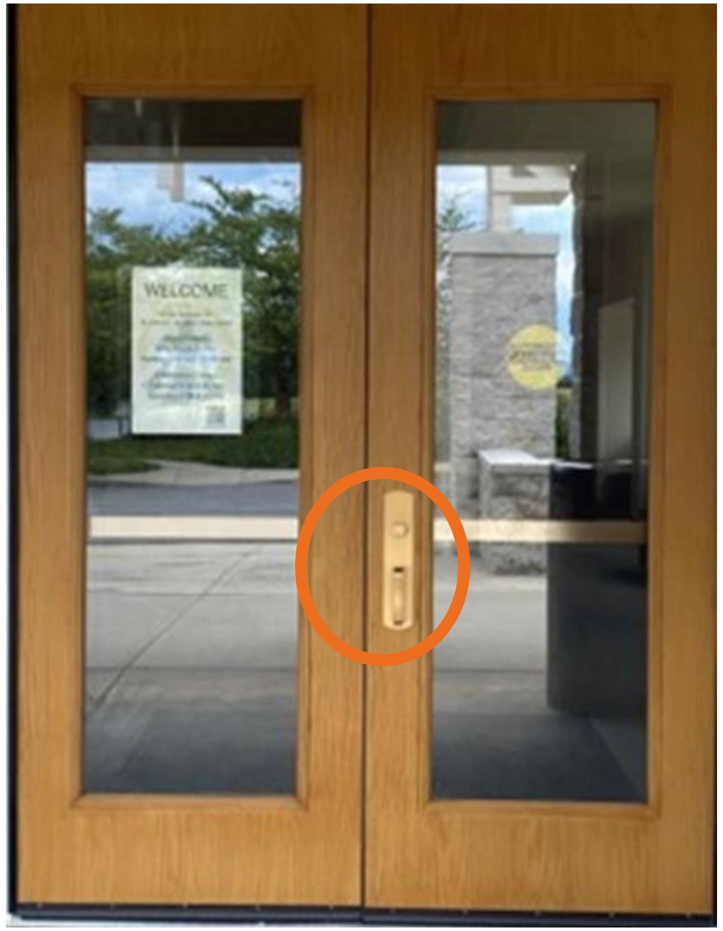


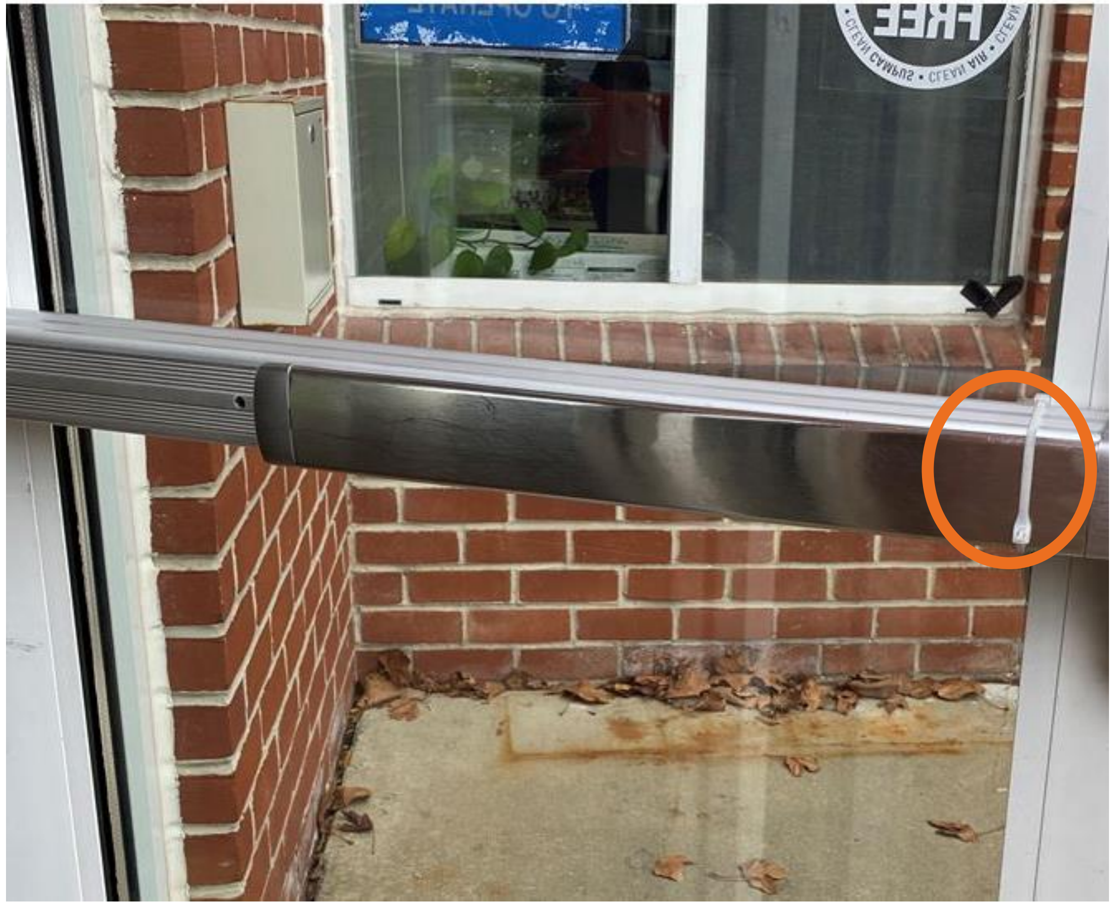


- No lock/unlock from outside locksets
- No Lever Trim or use storeroom function
- Use Rigid Handles/ Pulls
- Convert pairs to rim by mullion if possible
  - No bottom rods – ADA
- Roll-up doors (monitoring/keying)

Best Practices – Exterior Openings (Mechanical)

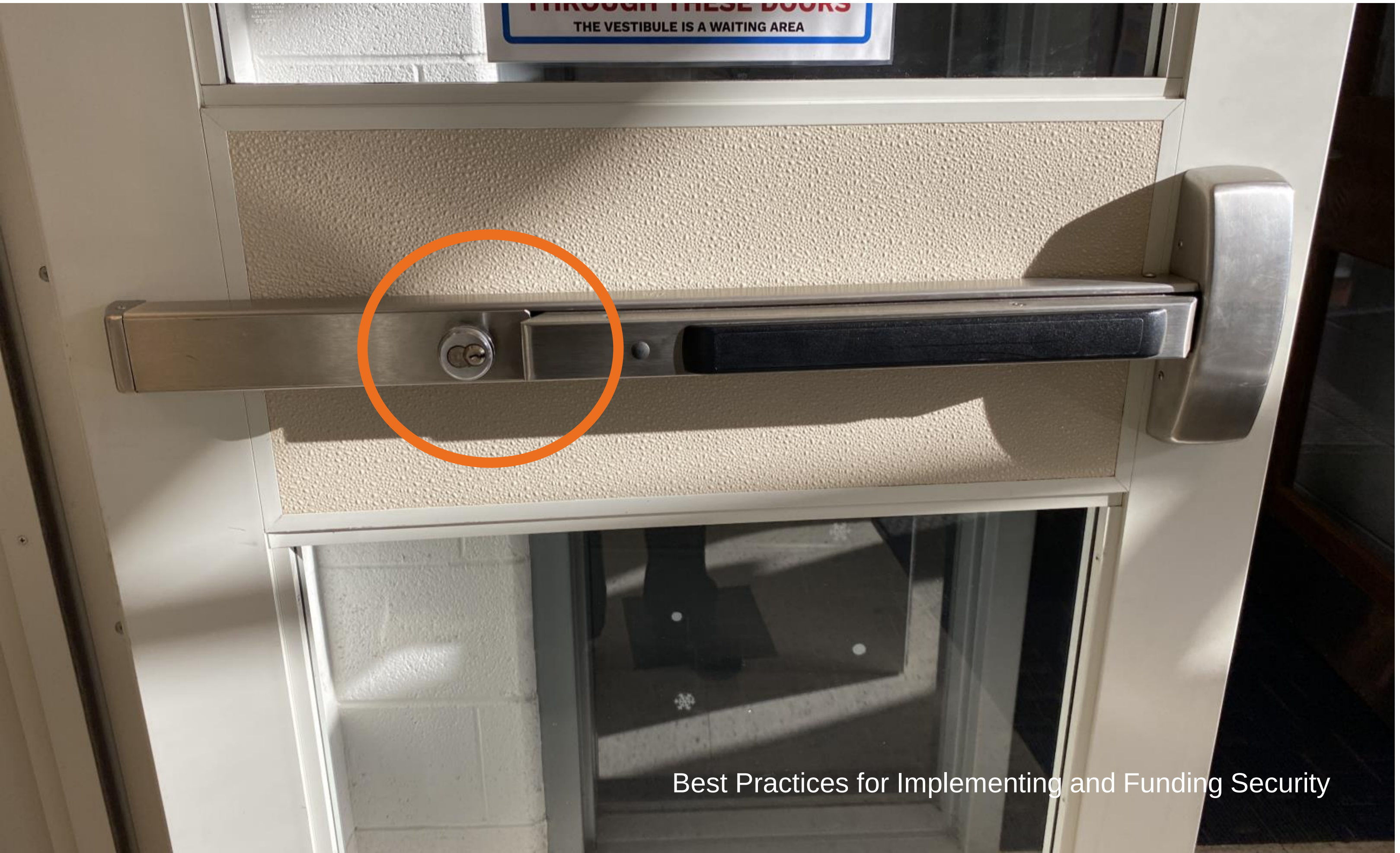
- Doors normally locked at all times
    - Unlocked for specific time zones
- Single pull OR recessed pulls
    - Eliminate “strapping” or chaining
- Glass no more than 50% of door
- Laminate or impact resistant glass





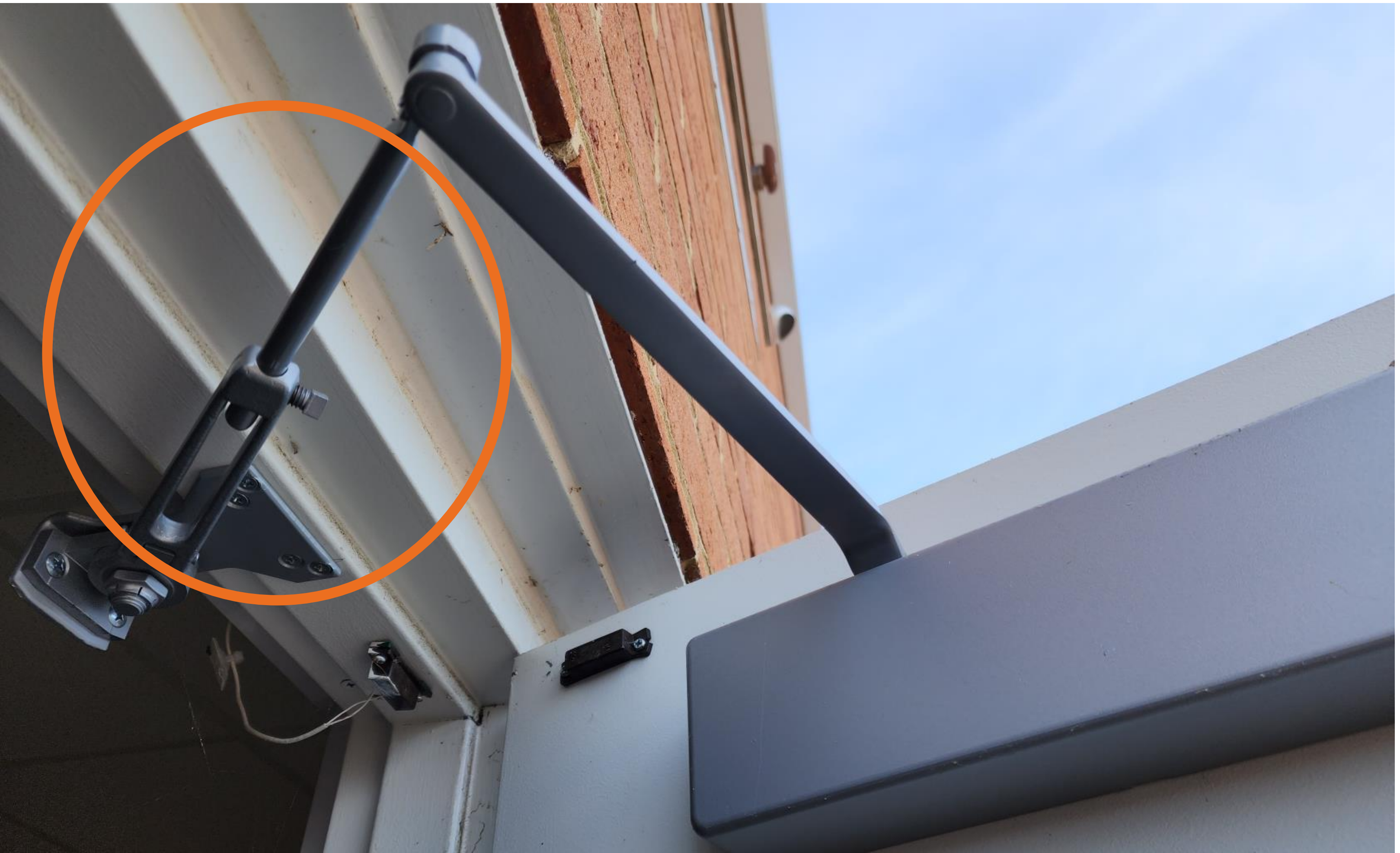
Best Practices – Exterior Openings (Mechanical)

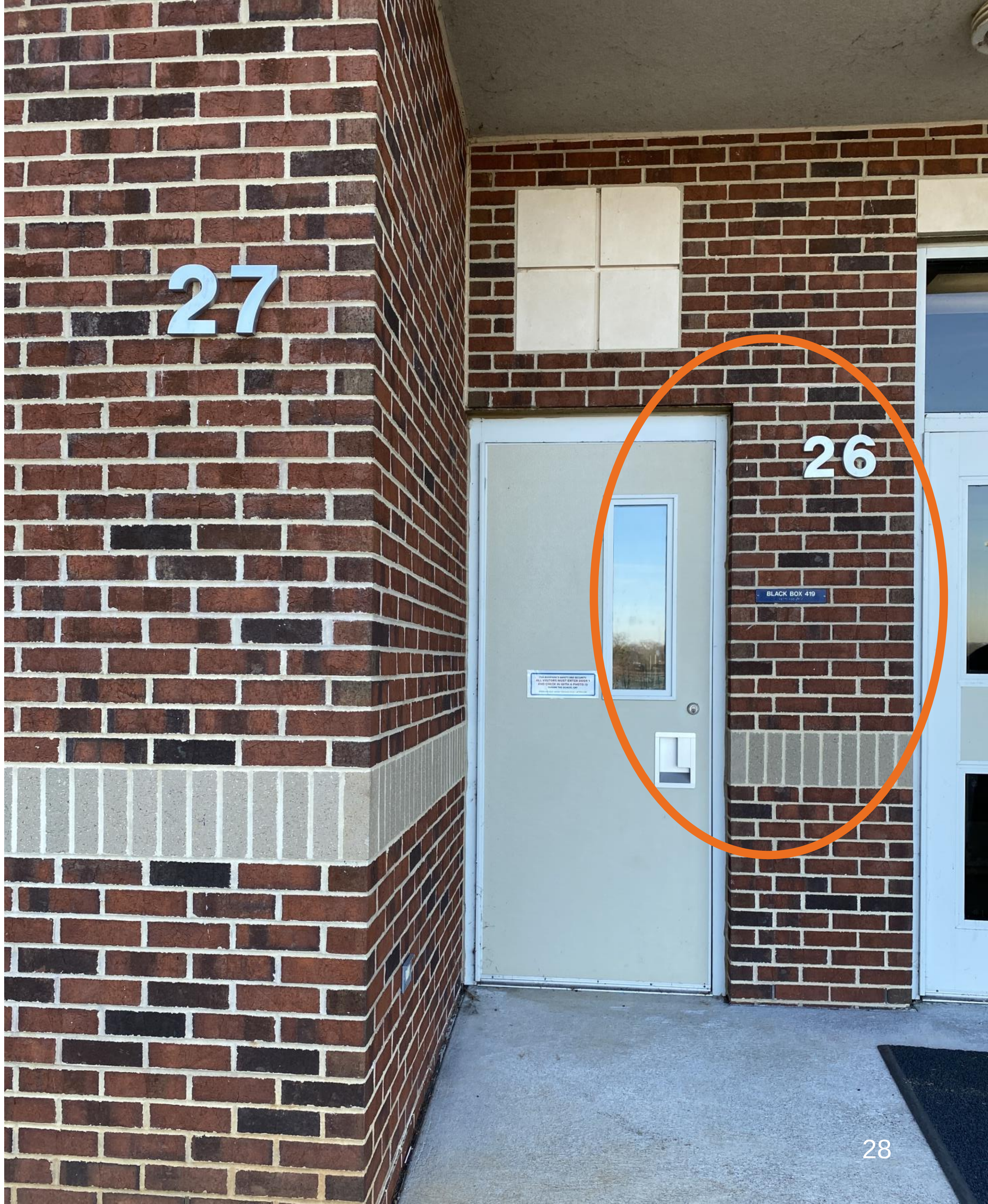
- Push-pad exits rather than cross bar
- Use Mid-Rail / 10” Bottom Rail (ADA)
- No Manual Dogging (Less Dogging)
    - No hex / cylinder dogging
- Reduce number of active entrances / Exit Only



Best Practices – Exterior (Mechanical)

- Eliminate hold opens - hooks, chains, eyelets, rope, rock, cinder block, where possible
- Ensure doors return to a closed, latched position
- Restricted, Patented key system
- Number exterior openings
    - Clockwise starting at main entrance - both sides of door should have numbers





Best Practices – Exterior (Electrical)

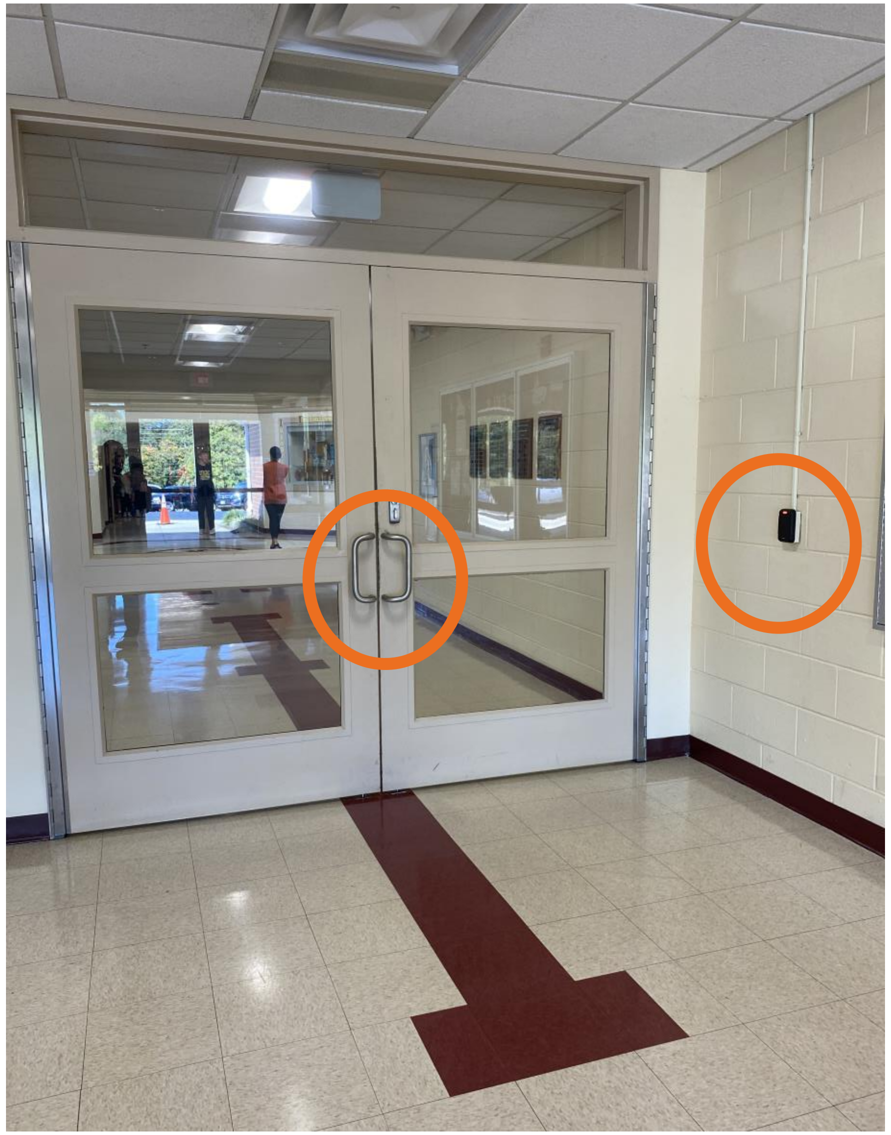
- Motorized latch retraction - most secure
- Single or pair of doors at active exterior locations
- Coordinate w / ADA operator
- Electric strikes no longer recommended – single point of failure
- Provide door monitoring & notification – door position, latch bolt, request to exit switches
- Fail-secure – not fail safe
  - Mag Locks NOT recommended
- Remote release and/or time zone controlled

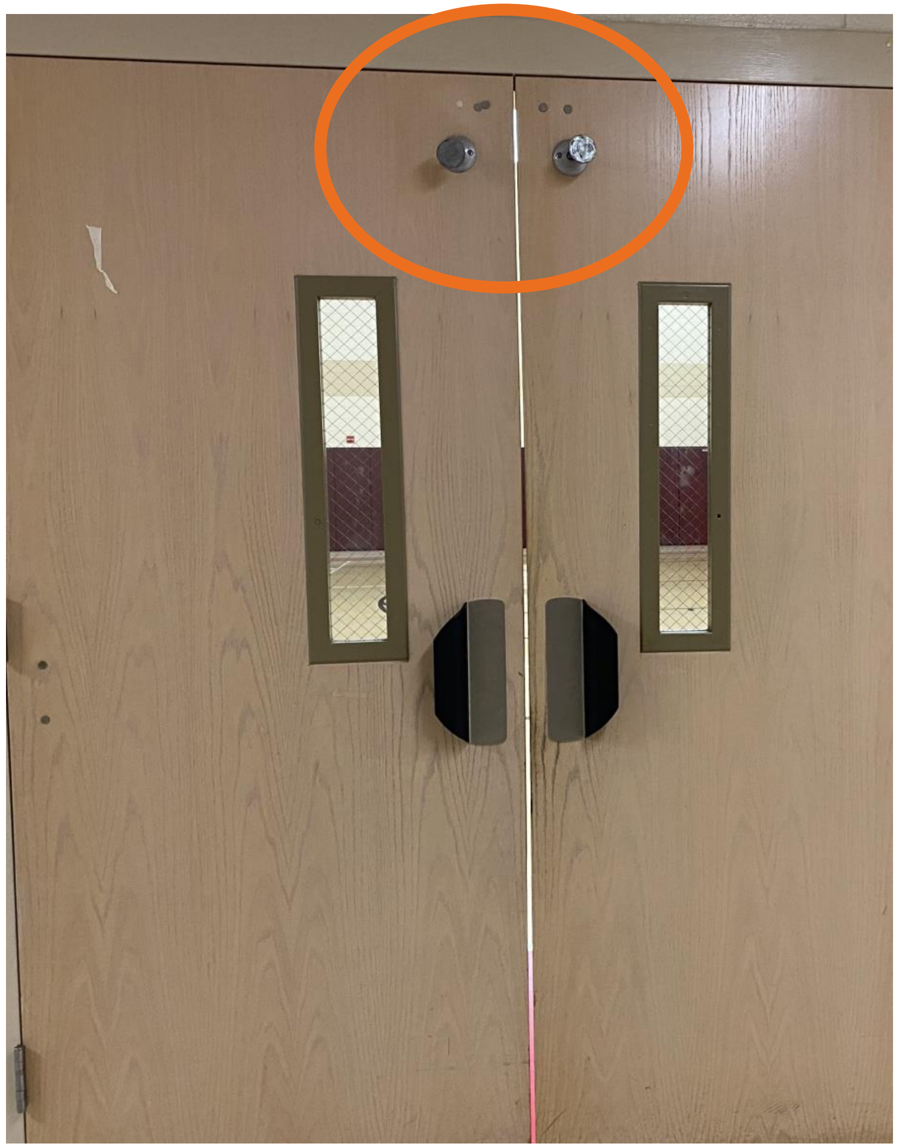
Best Practices – Exterior (Electrical)

- Credentials
  - Standard prox-low frequency / 125kHz = meh...
  - "SMART" 13.56 MHz-high frequency = better
  - Custom Encryption Key = best
- Readers
  - Multi-tech readers allow for transition pathway

Best Practices – Interior Openings

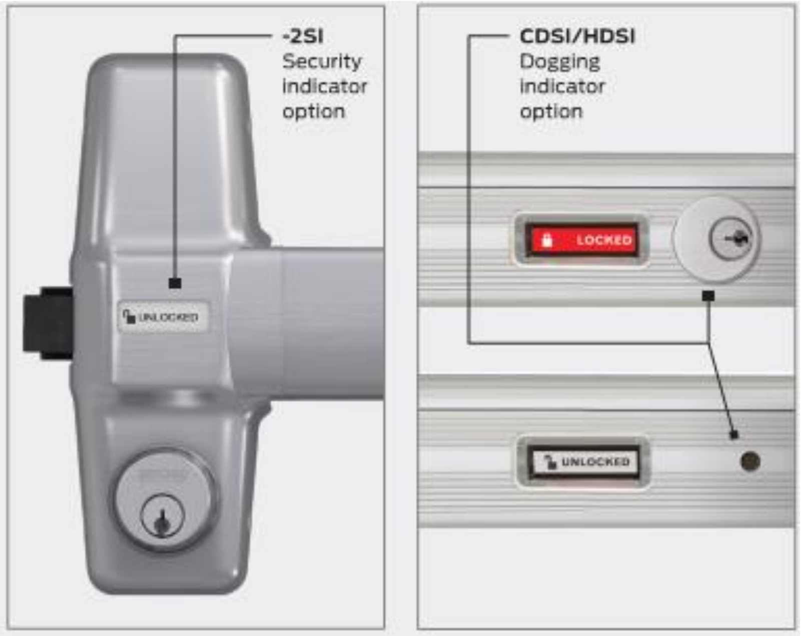
- Segment and compartmentalize building
  - Cross-corridor doors
  - Stairwell doors
  - Ideally secured electronically
- If hold opens are required, use magnetic hold opens tied into fire alarm panel and access control system
- Entrances to office space, common staff areas, etc. secured via PACS or lockable from interior with visual indicator
- Assembly spaces secured from inside (mechanical or electronic)





Best Practices (Mech) – Interior Openings

- Lockable from inside the room without opening the door
- Provide free egress from interior spaces
- Able to open from outside the room with valid key/credential
- Visual lock status indicator



Best Practices (Electronic)– Interior Openings

- Lockable from inside the room without opening the door
- Provide free egress from interior spaces
- Able to open from outside the room with valid key/credential
- Visual lock status indicator
- Interoperability
- Centralized lockdown
- Centralized power

We’ve Identified the Problem:

Now what do we do?

Creating the Team
Tips for Success

- **Inclusion of many stakeholders**
- **Define and understand roles**
- **Understand layers of permission and authority**
- **Who makes the ultimate decision**
- **Input and interrogation by multiple stakeholders ensure robust solutions**
- **Projects cut across disciplines**
- **Nothing exists in a vacuum**
- **Check your ego – Team Work Makes The Dream Work**
- **Identify Blind Spots – Eliminate Gaps, Silos, Disconnects**

Pitfalls to Avoid

- **Starting with complex, expensive systems**
  - Solving problems not fully understood
- **Not addressing the highest needs in order**
- Purchasing systems without understanding the impact on other components of the facility
- **Not including the right decision makers or interrogating the issue from multiple perspectives**
- **Vendors:**
  - Working with a vendor that wants to sell a product, not a solution
  - Working with vendors that do not understand the specific needs or are using outdated solutions

SACRIFICING SECURITY FOR CONVENIENCE OR DESIRE FOR NO CONFLICT

Summary of Best Practices

- Understand your risk
  - Engage outside consultants, county emergency managers, EMS, LE, PSAs
  - Understand localized threats
  - Conduct vulnerability assessments
- Take a layered security approach when securing your campus
- Develop an emergency action plan and TRAIN on it.
  - Identify key members and responsibilities
- Train Ushers and Greeters – The Power of Hello
- Tabletop exercises and other trainings (CPR/AED/First Aid/Stop the Bleed)
- Teach congregation that security is everyone’s responsibility
- Report hate crimes/threats to local LE
- Reach out to local PSA (To locate the PSA in your area, contact central@cisa.dhs.gov or visit cisa.gov/resources-tools/programs/protective-security-advisor-psa-program)

Resources:

- **CISA:**
  - **cisa.gov/topics/physical-security/protecting-houses-worship**
  - **cisa.gov/power-hello**
  - **cisa.gov/resources-tools/resources/de-escalation-series**
  - **https://www.dhs.gov/prevention**

Faith Based Information Sharing and Analysis Organization

- https://faithbased-isao.org

Maryland Active Assailant Interdisciplinary Work Group

- https://aaiwg.maryland.gov/

ASIS Houses of Worship Resources

- https://www.asisonline.org/publications--resources/security-topics/securing-houses-of-worship/

Questions?

Christin Kinman, MPH, CPTED
Christin.Kinman@allegion.com
240.537.8808

ALLEGION™

PIONEERING SAFETY™

About Allegion™

Allegion (NYSE: ALLE) is a global pioneer in seamless access, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion secures people and assets with a range of solutions for homes, businesses, schools and institutions.

For more, visit www.allegion.com.