A New Layer Of Security Inside The White Space

Jason Hallenbeck, DCDC, DCP
Data Center Design
Great Lakes Case & Cabinet

2017 BICSI Winter Conference & Exhibition
January 22-26 • Tampa, FL

What Will Be Covered

Intro To Security

- How to accomplish a secure space
- Why physical security is important
- What are we trying to protect

Cage

- A true layer of security
- Types
- Where it's frequently used

Secured Enclosure

- Fail safe versus secure
- Points of penetration
- Locking Mechanisms

An Introduction To Security

How to accomplish a secure space

- 4 D's of security
- Types of Penetration
- Layered Security

Why physical security is important

- Brian Howard and software security
- Security Compliances

What are we trying to protect

- Data
- Physical assets
- Service interruption

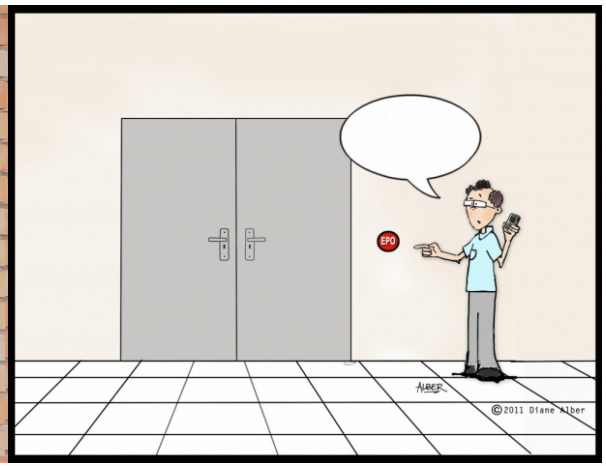
The 4 D's of Security

Types of Penetration

Penetration By Deception

Penetration By Force

Penetration By Accident



Why Does Software Security Receive So Much Attention?


The Washington Post

Man who leaked NSA secrets steps forward

To leaker, personal risks were clear

in • ter • es • ting (ĭn'trĭ-stĭng) adj. **1.** capable of holding one's attention. **2.** arousing a feeling of interest. **3.** oh God, oh God, we're all going to die.

Anybody Know Who This Is?

Brian Howard

A contractor for the FAA, Brian Howard took down a critical piece of infrastructure in our nations air space because he felt he needed to lash out at an employer he thought was wasteful.

How did he do it? He walked through the door, opened the networking enclosures, and lit them on fire.

Data Theft

HIPAA Physical Breaches In 2014

- Multilingual Psychotherapy Centers 12/13/2014 3,500 Medical Record
- Visionworks 11/28/2014 47,683 Medical Records
- Visionworks 11/10/2014 75,000 Medical Records (along with credit info)
- Health Dimensions 11/2/2014 5,370 Medical Records

Totaling 131,553 Peoples PII Physically Walking Out Of The Data Center

Physical Equipment Theft

Chicago Colocation Data Center With A Single Layer Breach

The Chicago colocation facility was broken into four times within two years. Thieves cut a hole through a wall and got away with approximately $15,000 worth of servers every time.

Service Interruption

Massive DC Downtime

Vodafone- Hundreds of thousands of UK customers lost service over an extended period of time

Knocked down a single door and had access to the whole data center

Verizon- Oceans 11 style attack

Dressed as police gaining access by telling employees there were reports of people on the roof.

Even with armed guards service was interrupted

Standards Compliance

FISMA
Federal Information

(3) Identifier Management
The organization requires multiple forms of certification of individual identification be presented to the registration authority

(2) Physical Access Authorizations
The organization requires two forms of identification… for visitor access to the facility where the information system resides… Orgs may use PIV cards, key cards, PINs, and biometrics

PCI
Financial Information

9.1.1 Use access control mechanisms or video cameras to monitor individual physical access to sensitive areas

9.1 Testing procedures: Verify the existence of physical security control for each computer room, data center, and other physical areas with systems in the cardholder data environment

HIPAA
Health Information

164.301(a)(1) implement policies and procedures to limit physical access to its electronic information systems… while ensuring that properly authorized access is allowed

164.310(a)(2)(ii) Implement policies and procedures to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft

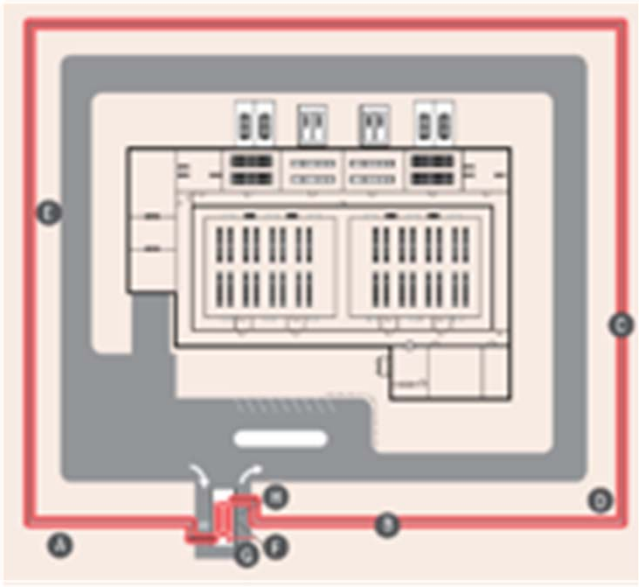
Standards Compliance

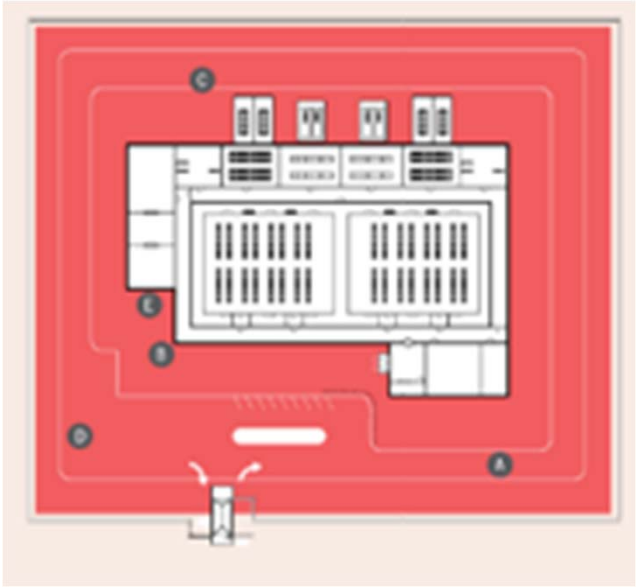
FIPS
Cryptographic Data

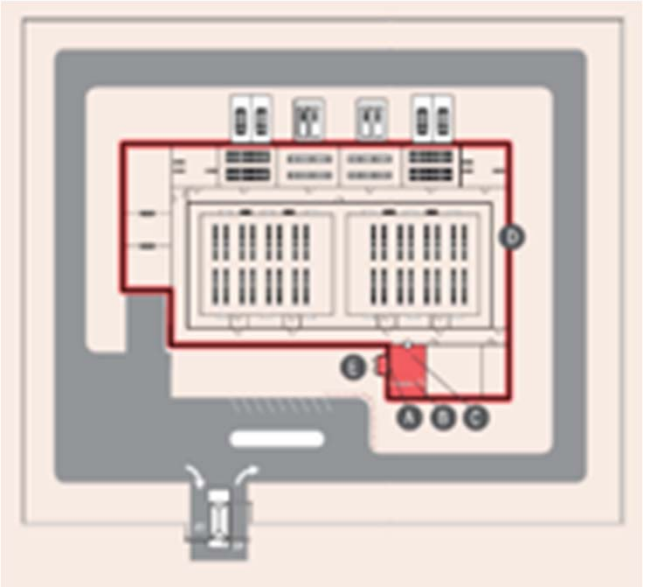
140-2 Section 4 Level 4 Security:
The physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

Layered Security Model

Outside Layers



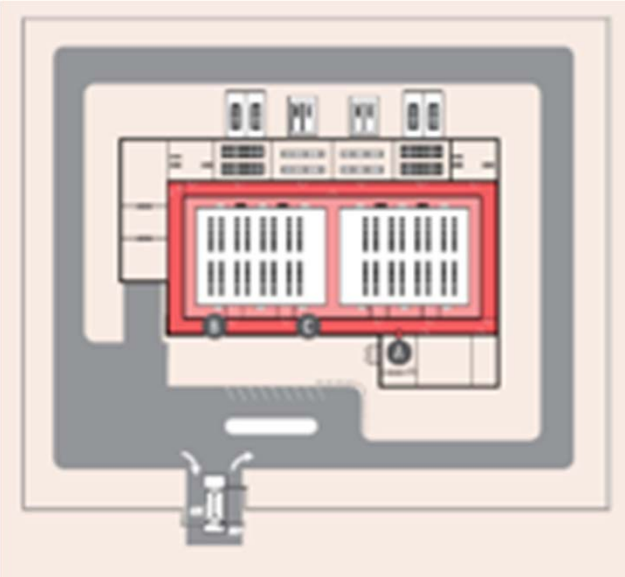


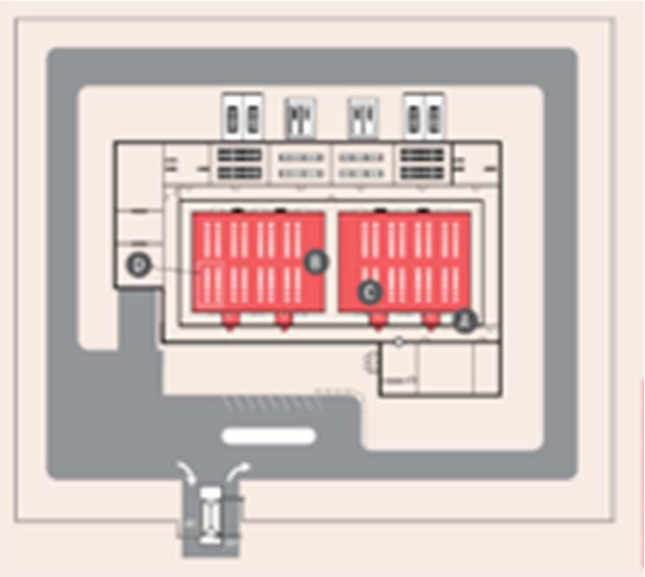


BICSI 002 12.2.2.2 12.10.1 12.10.2
BICSI 005 B.4.2 B.5

Layered Security Model

Inside Layers





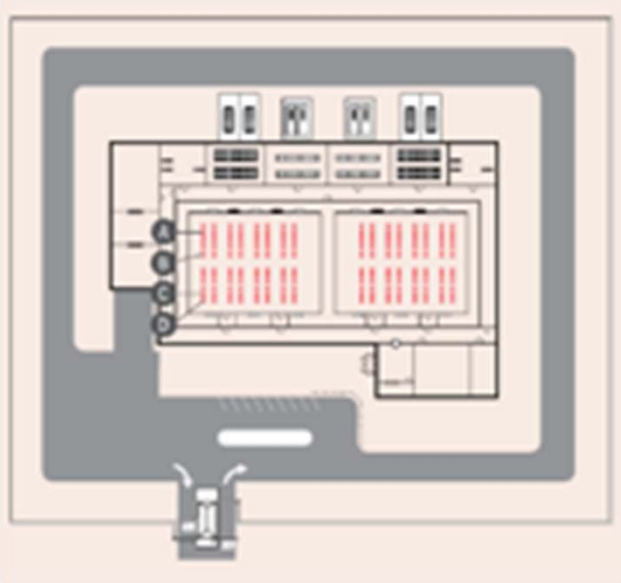
BICSI 002 12.2.2.2 12.10.1 12.10.2
BICSI 005 B.4.2 B.5

Layered Security Model

A New Layer

90 percent of the worlds data has been created over the last two years and that data has become increasingly more valuable. With increased data, the amount of equipment to support this data is growing exponentially and the number of people needed to support this equipment is also growing

Consequently a new layer of security at the enclosure level has become necessary to appropriately manage the increasing staff and valuable data stored within the enclosures.



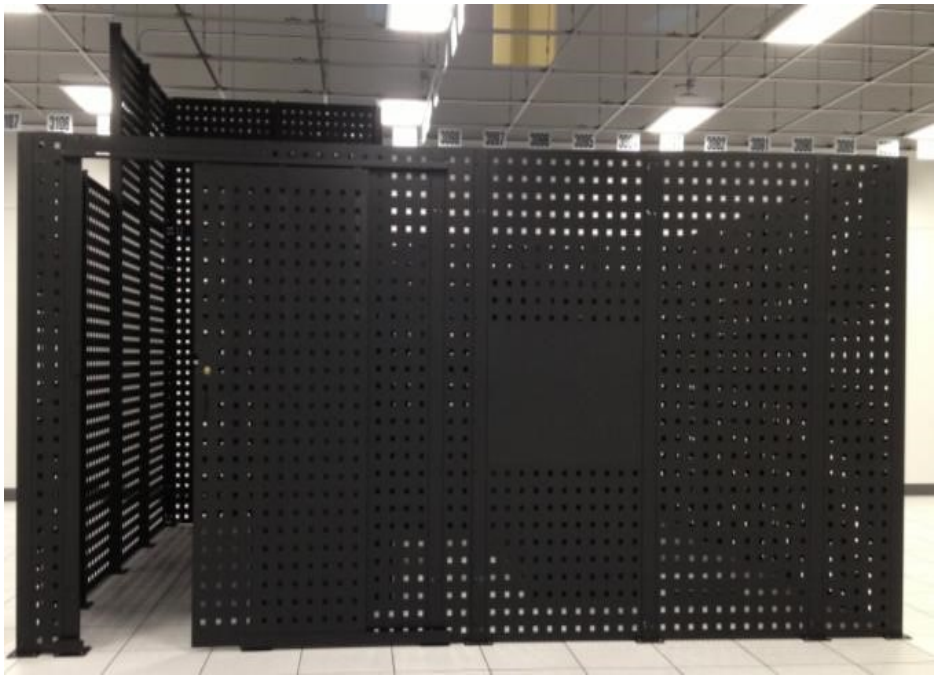
What Will Be Covered

- **A true layer of security**
  - How to accomplish a secure space
  - Complete Envelope of Protection
  - Access Control
- **Cage Types**
  - A true layer of security
  - Types
  - Where it's frequently used
- **Secure Enclosures**
  - Fail safe versus secure
  - Points of penetration
  - Locking Mechanisms

Metal and Welded Wire Barriers

Metal and welded wire barriers in essence create a room within a room, developing the new layer of security inside the white space

These deployments are often modular in size, able to retrofit into existing buildings and altered to a different size or shape after initial installation



IDA/MDA/Mechanical Separation

Sometimes we only need to protect our most critical pieces of infrastructure.

The IDA and HDAs, or the cores and spines of our network are often the most critical parts of the data center. They are often small in size, but touch every part of the data center. This is why it's often prudent to place these critical pieces of infrastructure behind metal or wire barriers.

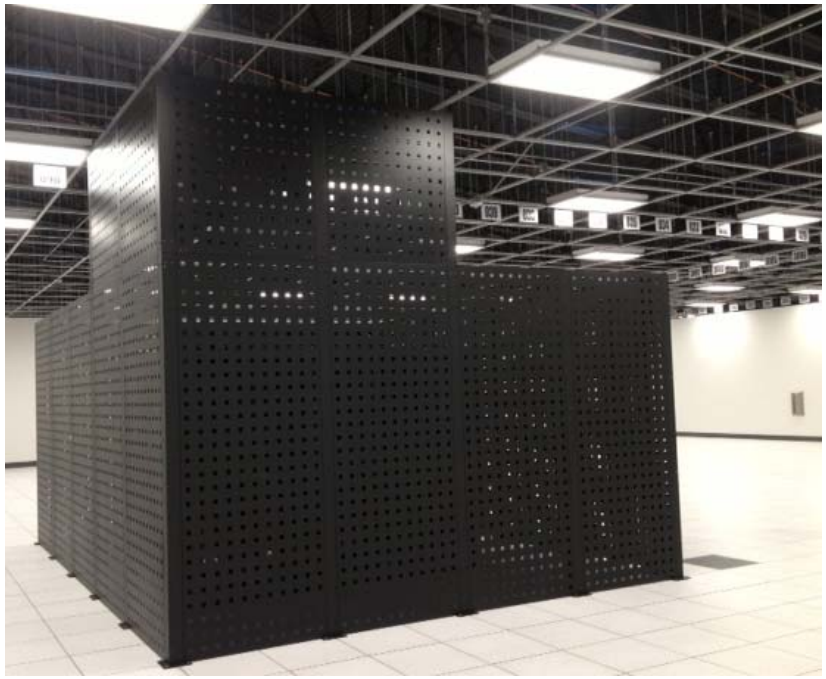
The mechanical equipment, although spread throughout the data center, is often limited to few but large pieces of equipment. Due to their lack of quantity and ease of tampering it's often prudent to place mechanical equipment in a separate room or behind a metal or wire barrier to control access.

Colocation Facilities

The place where you will most commonly see a metal barrier or wire fencing is within a colocation facility.

Partitioning off separate users, and often times more importantly house equipment, is often a security requirement.

Access control on each partition of the data center will allow the colocation provider to limit customers to only their own area, but also limit which employees have access to which enclosures.



Levels Of Security & Its Basic Functions

The minimum required components for an ACS include the 4 levels.

Level 1: Central equipment processing, AKA the computer
Level 2: Controllers for field processing
Level 3: Peripheral devices, those that gather information such as card readers
Level 4: Credentials such as cards, fobs, biometrics, pins, & passwords

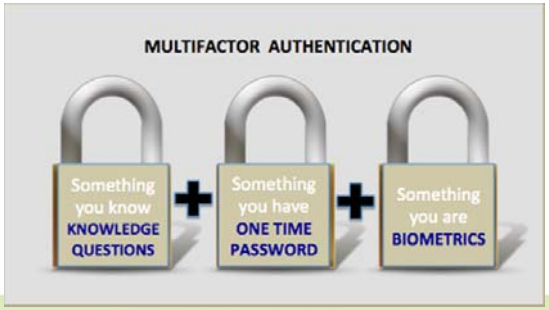
Every Design should support all of the following objectives:
Permit or deny entry
Document activity and could provide automatic notifications
Alter rate of movement within certain areas
Protect occupants, materials, and information against accidental or malicious disclosure

Access Control Tiers

Methods of authentication can be broken down into three types:
Type 1: What a person has (e.g., keys, cards)
Type 2: What a person knows (e.g., passwords, codes, work order numbers)
Type 3: What a person is (e.g., guard recognition, biometric data)

Access control to inner layers of security can be tiered by altering the authentication type, such as having card access to the building, but pin access to the metal barrier.

Access control can be further tiered by multi-factor authentication, where more than one type of authentication occurs at the same time such as using both a card reader and pin number to access the metal barrier.

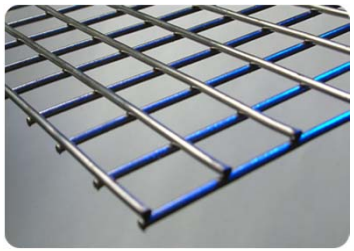


Applying a complete layer of security

When designing a metal barrier system, if the intent is for it to act as a security barrier ensure that it is designed as a true layer of security.

Expanded metal fabric or solid metal is more resistant to cutting, won't unravel, is easy to fabricate and install, can permit environmental condition, and provides and enhanced psychological deterrence

Welded wire fabric should be used when a less demanding barrier is needed than expanded wire.



Woven wire fabric is considered a barrier, but it is used for less demanding applications, and is not generally acceptable as a security countermeasure.

Review Metal Barriers & Welded Wire

Sometimes you just need to protect your most vital equipment

- IDAs
- HDAs
- Mechanical

Colocations often need barriers to separate customers and isolate equipment

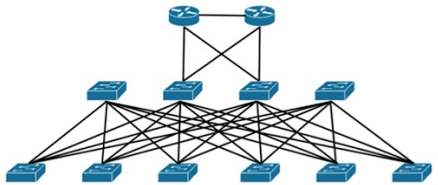
Security systems in their basic function have 4 levels

- Level 1 Central processing
- Level 2 Controllers
- Level 3 Peripheral devices
- Level 4 Credentials

3 Types of authentication creating tiers

- What you have
- What you know
- What you are

Create a complete layer of security



Security Enclosure

Within areas that are designated as “high security” or similar, the following recommendations are applicable for the design and selection of ESS enclosures.

- Enclosures made from metal or similar materials of strength, durability and tamper resistance
- Welded enclosures and fitting covers not needed for maintenance access
- Tamper switches for monitoring potential points of penetration

Fail Safe Versus Fail Secure
Potential points of penetration
Locking mechanisms
Secure cabling

Fail Safe vs Fail Secure

The biggest advantage to enclosure security is the comparison of fail safe versus fail secure.

Fail-secure hardware goes into a locked state, typically in a power loss scenario or emergency procedure.

Many life safety professionals won't allow this for any "livable space", but the enclosure, despite housing our most critical infrastructure, is not a livable space

Fail-Safe, and for the purpose of security this includes REX's and Latched, for life safety are more common, and in the event of an emergency are unsecured.

Points of Penetration: Doors

Hinges should be tamper resistant and facing the protected side of the door

The same concept should be applied for the cam, utilizing an enclosure designed around tamper resistance for the cam is important

The vast majority of enclosures have used the infamous 1333 key, millions of these keys exist, and are purchasable online at major retailers like Amazon

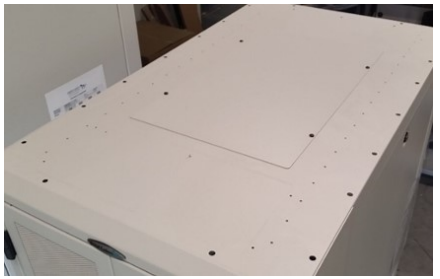
BICSI 002 12.7.2.3 & 12.10.6

Points of Penetration: Sides & Tops & Bottoms

All points of access of fittings like side panels should have mechanical tamper switches to monitor for forced penetration

Limiting the potential points of penetration by limiting the physical number of access points is often prudent

Tops and bottoms, since they're constantly changing for cable access should be maintained to the best of the operators ability to limit open points of access, either by reusing old cable access holes or filling access holes no longer in use



Locking Mechanisms

Mechanical

Pros:

- Simple to install
- Inexpensive
- Can be a simple mechanical combination handle or hasp lock

Cons:

- Not centrally managed, so require to be physically touched when turnover occurs
- Tamper monitoring
- Built in tamper resistance
- Additional monitoring of side panel

BICSI 002 12.7.2.2 BICS 005 8.5.1

Locking Mechanisms

RFID & Pin

Pros:

- Stand alone, tie into an existing security system, or integrate with a stand alone software
- Tamper sensors inside the handle
- Real time monitoring
- Capable of two factor authentication

Cons:

- Existing systems have known vulnerability with wiegand and rs232 communication protocols
- Cards can be copied, and pins can be shoulder surfed

Locking Mechanisms

Biometric

Pros:

- Potential three factor authentication
- Can be accomplished with biometric cards or readers
- Can integrate into existing security systems or stand alone software suites

Cons:

- New biometric databases typically need to be created
- Fingerprints are sometimes damaged or difficult to read
- Fingerprints are left everywhere, and depending on the reader technology they may be easily copied and used

Secure cabling

The communication protocol between the handle and the controller is often the most susceptible to a gecko device. Being sure to have a secure pathway from the handle to the controller to limit the number of places a gecko can be placed is pertinent to preventing MITM attacks.

BICSI 002 5.5.8.2

Recap Enclosures

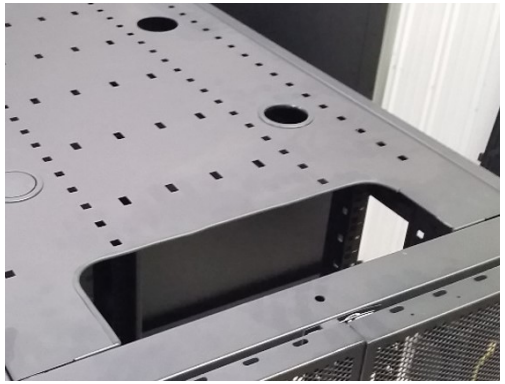
Fail safe v fail secure

Doors as a potential point of penetration

Sides tops and bottoms as a potential point of penetration

Locking mechanism

Secure cabling



Conclusion

Intro To Security

- How to accomplish a secure space
- Why physical security is important
- What are we trying to protect

Cage

- A true layer of security
- Types
- Where it's frequently used

Secured Enclosure

- Fail safe versus secure
- Points of penetration
- Locking Mechanisms

Thank you for your time!

QUESTIONS??