

# A New Layer Of Security Inside The White Space

Melissa Campbell & Brian Franz

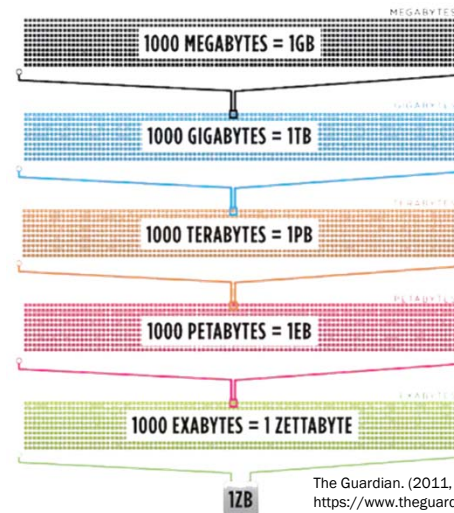
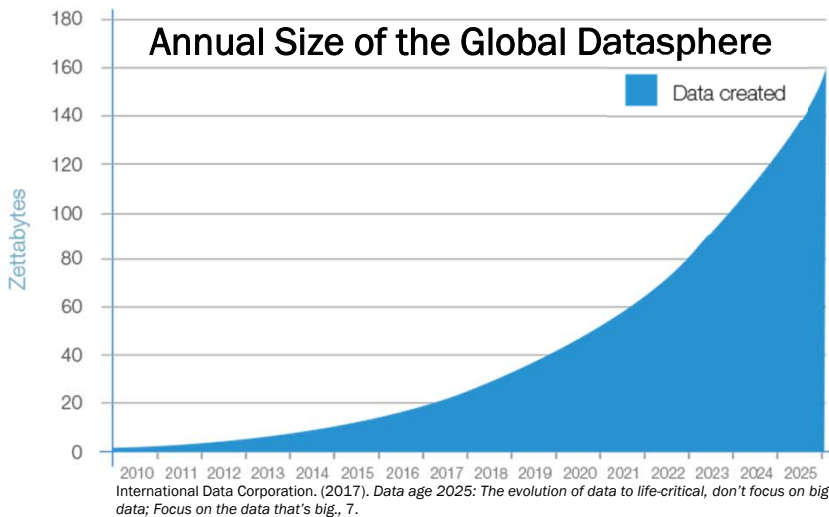
Great Lakes Case & Cabinet Co., Inc.



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# Increased Data, Increased Value

- In the last 2 years, 90% of data has been created.
- With the increased amount of data being produced, the data center is growing exponentially; not only in data but also in equipment.
- With data center growth, there is a combined increase in the value inside the data center and an increase in the number of people with access to that data center.



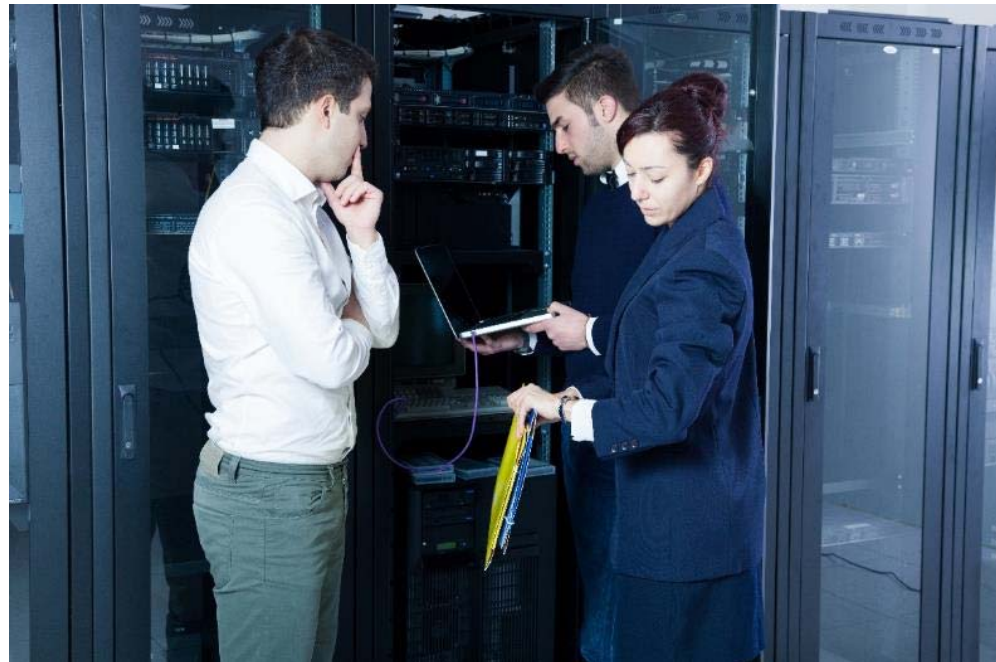
The Guardian. (2011, June 29). Adapted from <https://www.theguardian.com/technology/blog/2011/jun/29/zettabyte-data-internet-cisco>



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

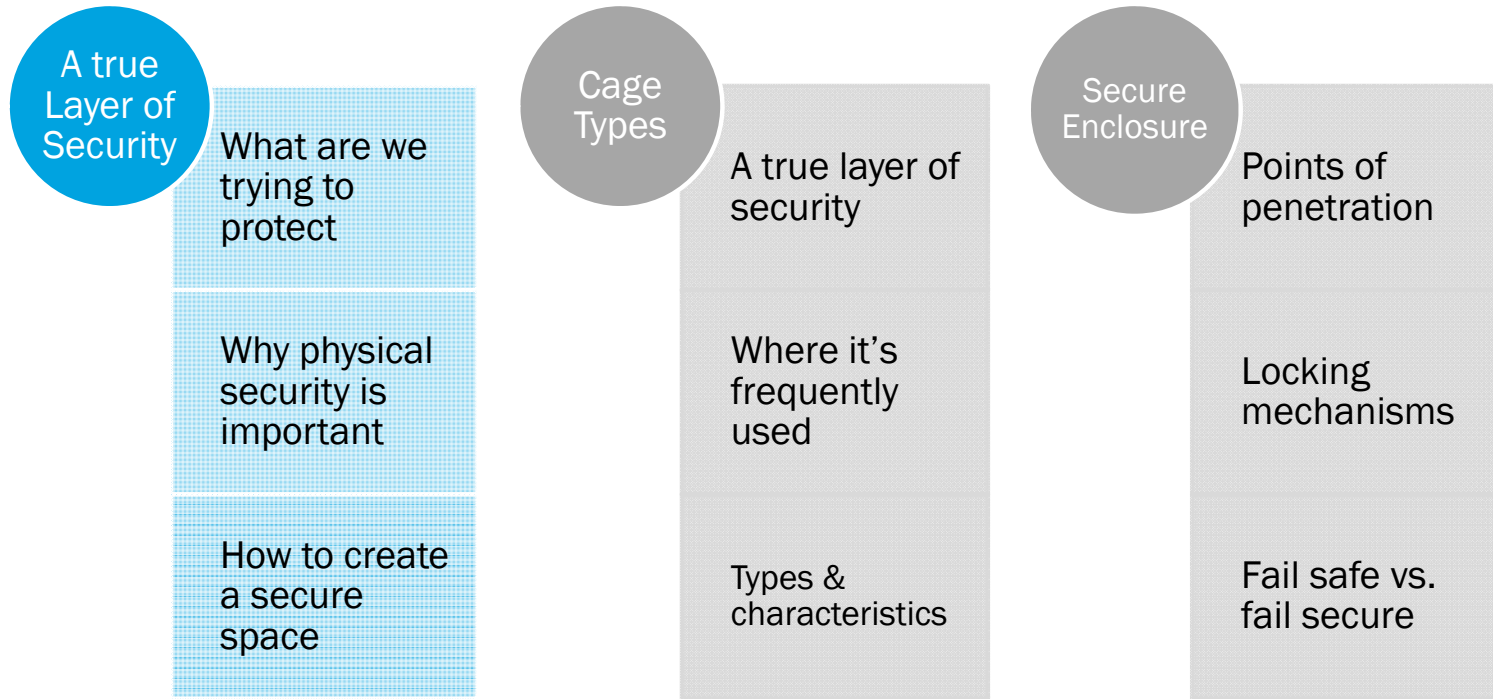
# Increased Data, Increased Value

- A data center today regularly has hundreds of people who have access to the traditional five layers of the facility.
- Beyond the fifth layer, the white space, exists the data center enclosures.
- Each of the people in the facility can pose a threat to the enclosure, the equipment, and the data. A layer of security around the enclosure is now required.



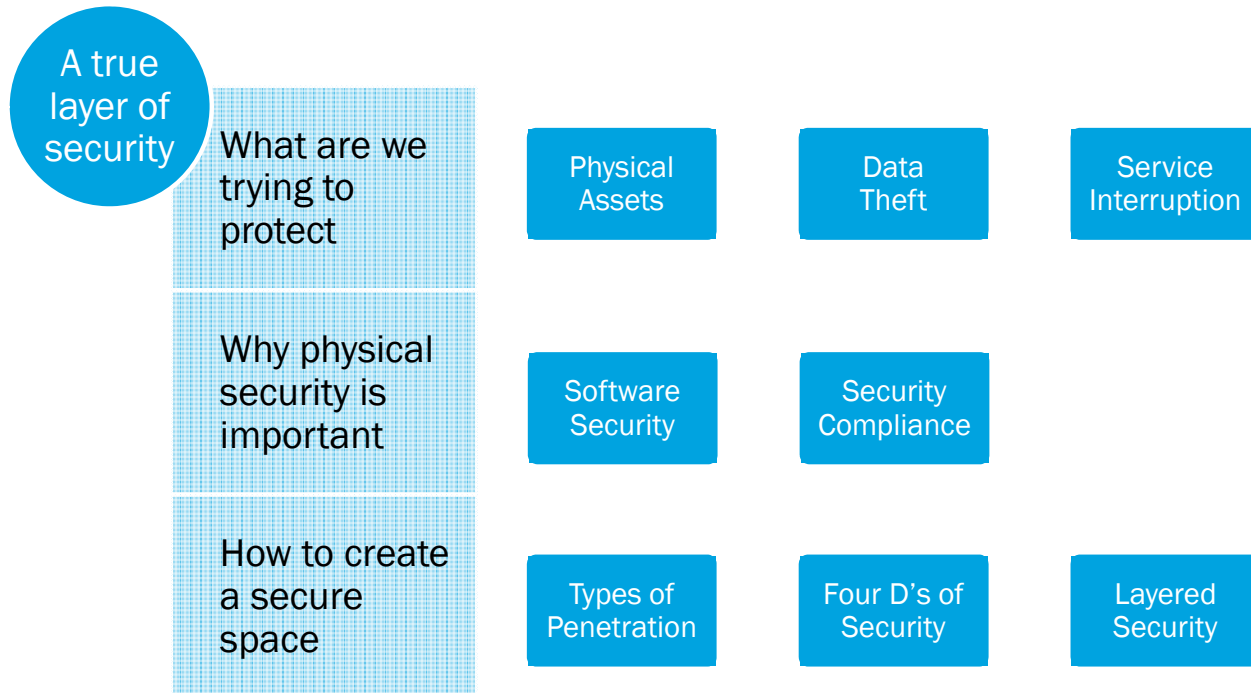
**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# What Will Be Covered



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# A True Layer of Security



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

**Anybody Know Who This Is?**



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

## Damage to Physical Assets

- A contractor for the FAA, Brian Howard took down a critical piece of infrastructure in our nations air space because he was a disgruntled employee.
- How did he do it? He walked through the door on a Friday around 5:06 am, opened the networking enclosures and lit them on fire.
- The fire caused 2000 flights to be grounded on Friday, with more than 5,000 flights canceled at O'Hare and Midway airports in the following week.



Ellis, R., Hanna, J., Patterson, T. (2014, Sept. 27). FBI: Suspect sent Facebook message: 'I am about to take out' FAA facility. *CNN*. Retrieved from <http://www.cnn.com/2014/09/26/travel/chicago-ohare-midway-flights-stopped/index.html>

Airlines estimate fire cost  
**\$350**  
MILLION

Jansen, B. (2015, Sept. 11). FAA arsonist gets 12 ½ years in prison term, \$4.5M restitution. *USA Today*. Retrieved from <https://www.usatoday.com/story/news/2015/09/11/faa-fire-air-traffic-control-chicago-aurora-brian-howard/72055046/>



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Data Theft

- The US Department of Health and Human Services (2017) maintains a list of breaches of unsecured health information; the following breaches were caused by unauthorized access/theft to physical equipment.
- The 2017 Cost of Data Breach Study, conducted by Ponemom Institute and sponsored by IBM, averages a healthcare breach costs a company \$380 per individual affected.
- **Cases that are still under investigation as of July 2017, the number of individuals affected, and possible total cost of each breach:**

Walgreen Co. (IL):	8,345	\$3,171,100
Franciscan Health (WA):	18,399	\$6,991,620
Ohio Department of Mental Health (OH):	59,000	\$22,420,000
Empi Inc and DJO, LLC (MN):	160000	\$60,800,000
Commonwealth Health Corporation (KY):	697,800	\$265,164,000

Ponemom Institute. (2017). *2017 Cost of data breach study*, 10.  
US Department of Health and Human Services. (2017). *Breach portal: Notice to the secretary of HHS breach of unsecured protected health information*. Retrieved from [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**



# Service Interruption

- On May 27, 2017, a British based airline canceled more than 400 flights which stranded 75,000 passengers in one day.
- An engineer disconnected a power supply near Heathrow airport and when reconnected, caused a power surge that resulted in immediate loss of power.
- It is estimated to have cost the airline \$112 million (Patrizio, 2017).



Credit: British Airways

Patrizio, A. (2017, June 8). British airways' outage, like most data center outages, was caused by humans. *NETWORKWORLD*. Retrieved from <http://www.networkworld.com/article/3200105/data-center/british-airways-outage-like-most-data-center-outages-was-caused-by-humans.html>



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Software Security

- “Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.” (US Department of Homeland Security, 2017)
- The US government has deemed it as high priority:
  - Divisions of federal agencies are completely devoted to software security and cybercrime/safety
  - U.S. Secret Service maintains the Electronic Crimes Task Force
  - Department of Homeland Security maintains the National Cybersecurity Protection System.
- Cybercrime requires a great deal of intelligence and is interesting; pop culture has launched it into our daily lives with television shows and movies
  - Since this is what consumers are interested in, news is dominated with cybercrime.



US Department of Homeland Security. (2017). *Cybersecurity*. Retrieved from <https://www.dhs.gov/topic/cybersecurity>  
Grubb, T. (2010, April 26). The five A's that make cybercrime so attractive. *Security Week*. Retrieved from <http://www.securityweek.com/five-a%E2%80%99s-make-cybercrime-so-attractive>



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Software Security

- Companies across the globe have implemented measures to protect software and try to eliminate cybercrime.
- Despite this, the Data Center Journal states the five simplest ways to hack into a data center and tamper with software/hardware include:
  - Crawling through void spaces in the wall
  - Lock-picking the door
  - “Tailgating” into the building (tailing other employees)
  - Posing as contractors or service repairman
  - Forcing open improperly installed doors or windows.
- The standards that address the safety of software can also be applied to the physical equipment that stores data.



Kleperis, T. (2016, July 14). Protecting your assets: Addressing cybersecurity. *The Data Center Journal*. Retrieved from [http://www.datacenterjournal.com/protecting-assets-addressing-cybersecurity/#\\_ftn5](http://www.datacenterjournal.com/protecting-assets-addressing-cybersecurity/#_ftn5)



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Standards Compliance

FISMA Federal Information	PCI Financial Information	HIPAA Health Information
(3) Identifier Management The organization requires multiple forms of certification of individual identification presented to the registration authority	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 controls for each computer room, data center, and other physical areas with systems in the cardholder data environment	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)(i) Implement policies and procedures to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft
(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		

There are many standards but FIPS sums it up!



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Standards Compliance

When there are no existing voluntary industry standards to address federal requirements for security and interoperability, the US National Institute of Standards Technology (NIST) issues such standards, referred to as Federal Information Processing Standards (FIPS).

NIST specifies that when federal organizations use cryptographic-based security systems to provide protection for sensitive but unclassified information in computer and telecommunication systems, the organization is mandated to adhere to FIPS.

One of the best standards that apply to physical assets is **FIPS 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.



US National Institute of Standards Technology. (2017). FIPS general information. *NIST Information Technology Laboratory*. Retrieved from <https://www.nist.gov/information-technology-laboratory/fips-general-information>  
US Department of Commerce. (2001, May 25). FIPS PUB 140-2: Security requirements for cryptographic modules. Retrieved from <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>

BICSI 002 12.4.2



**2017 BICSI *Fall***  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Types of Penetration

Penetration by Force



Penetration by Accident



Penetration by Deception



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# The 4 D's of Security

The purpose of all security measures are intended to mitigate and eliminate any and all types of penetration:

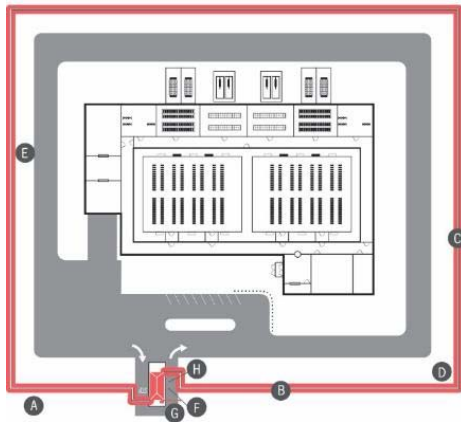
- **Deter** the thought of penetration by making it difficult to penetrate
- **Delay** the entrance to provide more time for authorities to react
- **Detect** the attempt of penetration so that authorities can respond in a timely manner
- **Decide** how to react depending on the alerts received and act on the decision

Security measures are implemented in multiple ways through out the traditional five-layered security model.



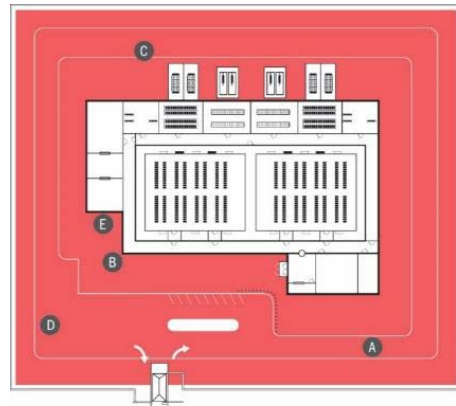
# Layered Security Model

## Outside Layers



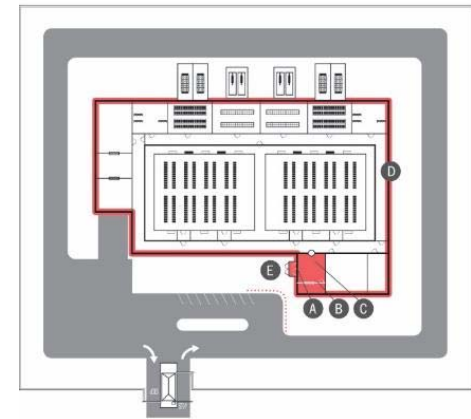
### Perimeter Defense

- Controls authorized and unauthorized access to the data center's property



### Clear Zone

- Critical electrical and mechanical areas (i.e. power plant, generators)
- Equipment loading docks and secondary entry points



### Facility Façade and Reception

- Visitor control

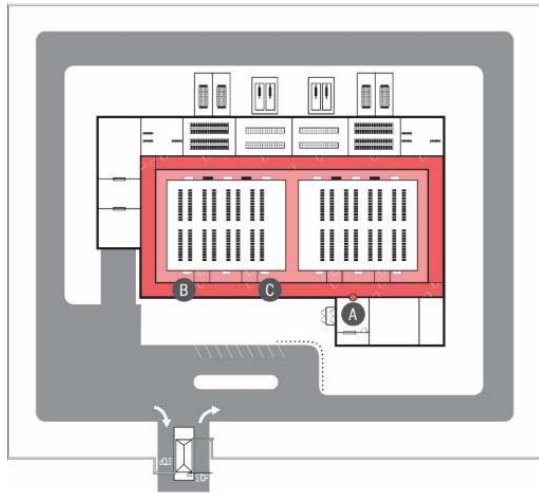


**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV



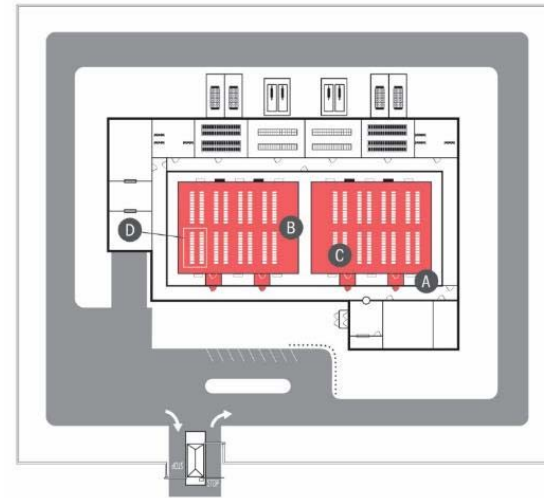
# Layered Security Model

## Inside Layers



### Gray Space

- Hallways and escorted areas that lead to the data center



### Data Center Room and White Space

- Mantrap outside of the data center



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV



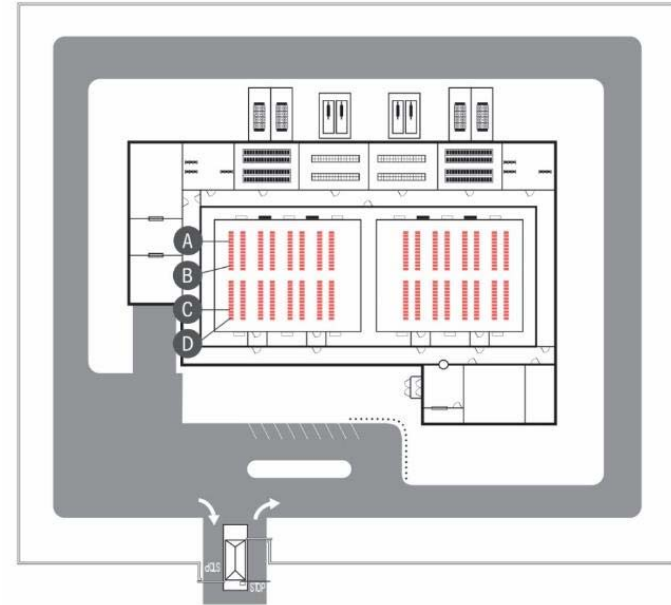
**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# Layered Security Model

## A New Layer

Despite security measures throughout the traditional five-layered security model, penetration at the enclosure has still occurred, resulting in loss of physical equipment, data, and service interruption.

Through the use of well manufactured cages and enclosures, a sixth layer of security can be created to deter, delay, and detect unauthorized entry.



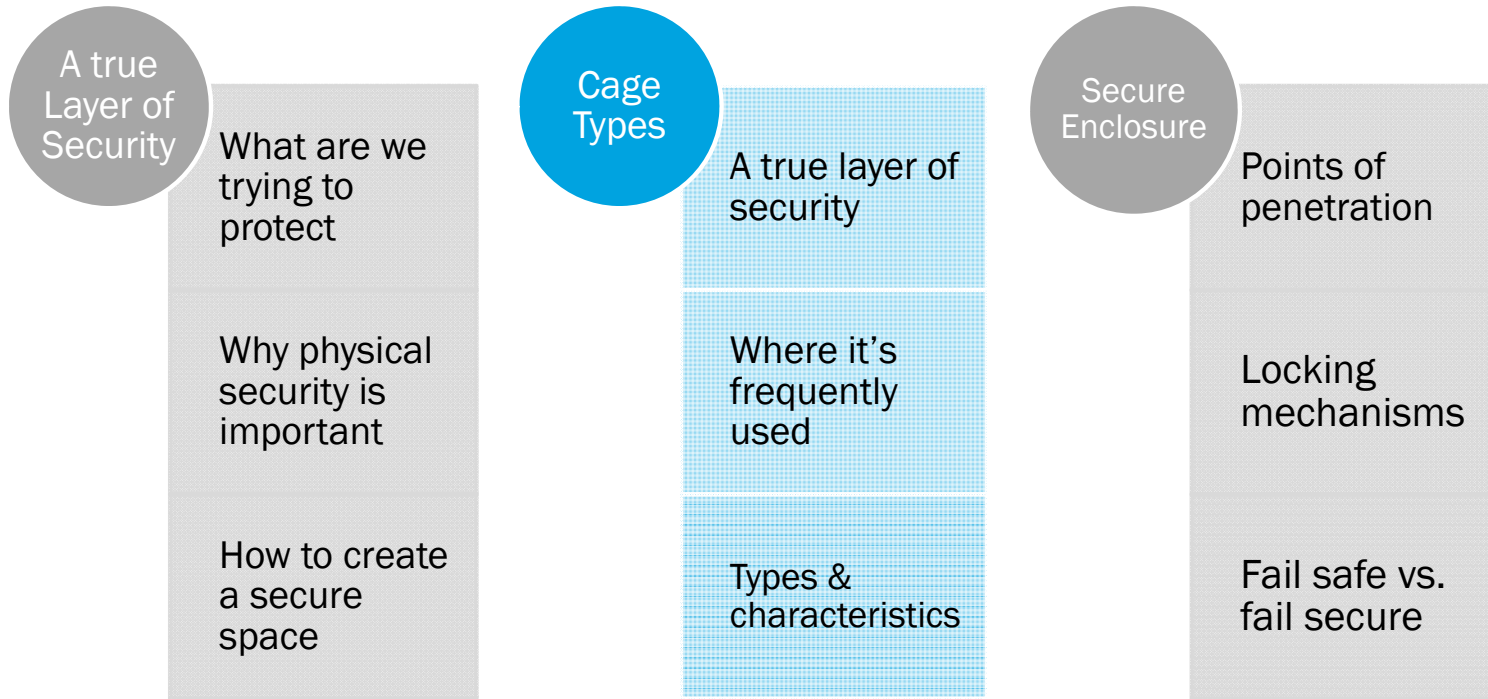
Anixter & Data Center Dynamics. (2017) Global technology briefing: Risk management best practices, 41.

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



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# What Will Be Covered



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# A True Layer of Security

Metal and welded wire barriers in essence create a room within a room, serving as a new layer of security inside of the white space. These metal and welded wire barriers, often referred to as cages or privacy panel systems, provide an additional layer of protection around groups of enclosures.



**Welded wire barrier**



**Metal barrier**



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

## Where it's Frequently Used

Metal and welded wire can be used to:

- Separate customers in a co-location facility
- Segregate enclosures of various security levels
- Separate the telcom/meet-me area from the data center floor, or separate providers from each other
- Main distribution areas as well as storage areas can be protected and layered into their own zone via security panels



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

BICSI 002 12.10.9

## Where it's Frequently Used

Metal and welded wire barriers are also used to protect mechanical equipment and components of cabling system structures:

- Mechanical items (such as HVAC units, UPS, etc.) in a Class 3 or 4 data center that are not located in a physical mechanical room can be segregated from the data center
- Intermediate distribution area (IDA) that provides a second level cable subsystem; may include LAN and SAN switches
- Horizontal distribution area (HDA), equipment includes LAN, SAN, and KVM switches used to provide network connectivity



BICSI 002 14.4.5.2 14.4.6.2 7.4.6.2



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Types of Cages

Metal barriers are described as sheets of metal that have been cut or shaped and somewhat flattened and are:

- Resistant to cutting
- Will not unravel or uncoil
- Is easy to fabricate and install
- Permits environmental condition
- Provides enhanced psychological deterrence

Welded wire barriers, created by a series of wires that intersect each other, should only be used when a less demanding barrier is required: tool rooms, utility rooms, etc.



Welded wire  
barrier



Metal  
barrier

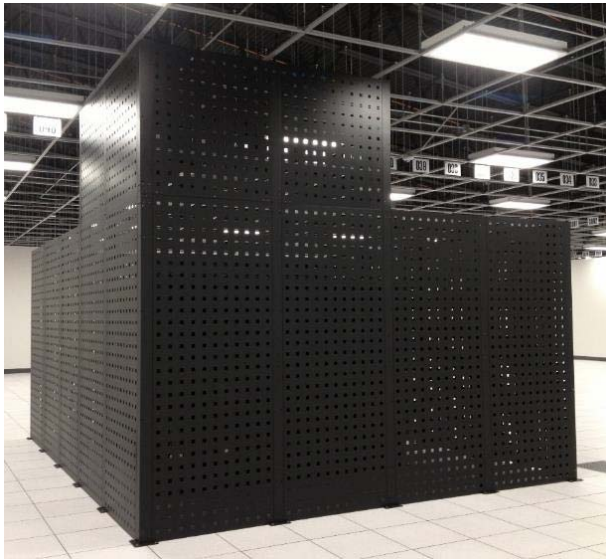


**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV



# Characteristics of Cages

- Modular build out allows flexibility unlike a traditional wall; adaptable to fit into any size facility
- Some companies want minimal site into a space, making perforated panels ideal
- Physical separation and airflow may be desired, making a mesh or wired product ideal
- When zero line of sight is needed, a solid wall is ideal



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

## Characteristics of Cages

- Cages can be their own room, creating a layer inside of the data center
- Doors can have a variety of locking mechanisms, including options that tie into the building's existing access control system
- Posts should be secured from the inside
- Watch all points of entry including ceiling and floors



Biometric access control



Internal door view



Post secured to slab floor



Ceiling panel installed in Gordon Grid system



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

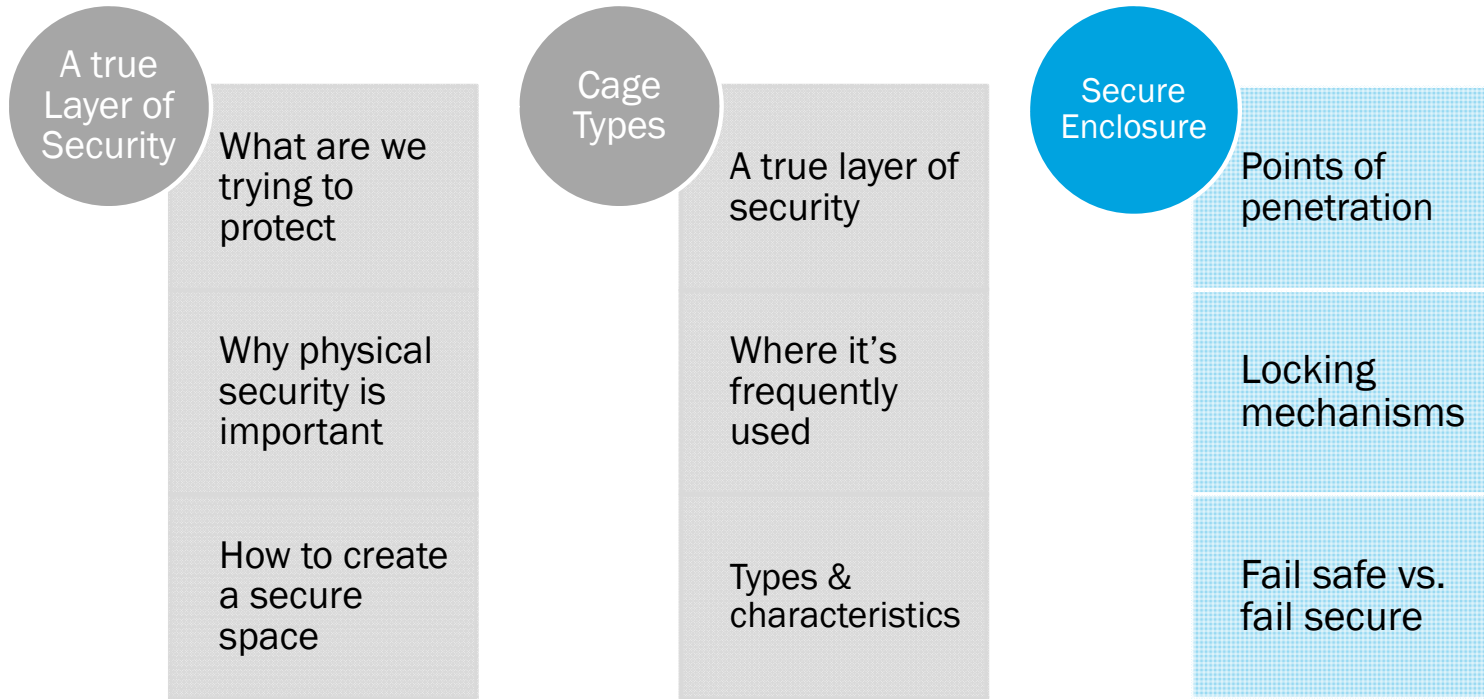
## Characteristics of Cages

Creating the sixth layer of security inside of the data center involves completion of a cage, but also the deployment of secure enclosures.



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# What Will Be Covered



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

## Secure Enclosure

Within areas that are designated as “high security” or similar, the following recommendations are applicable for the design of electronic enclosures and boxes:

- 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

A secure enclosure should begin with a fully welded frame that is constructed of certified North American steel (which ensures little to no metal impurities) and manufactured/originated in a facility within the United States.



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

## Points of Penetration: Doors

- Gaps exist between the frame and the door
- The gap allows enough access to fit a pair of needle nose pliers
- Unscrewing the bolt holding in the cam bypasses any locking mechanism on the door
- Hinges can also have gaps along the side



*Recessed doors eliminate gaps and don't allow access to handle or hinge hardware.*



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

## Points of Penetration: Side Panels

- Generic keys can provide access to side panels
- Many enclosures have a total of 4 side panels, resulting in additional points of entry that need monitored



- *Single side panels reduce the points of entry to monitor*
- *Tamper resistant panels are secured from inside the enclosure*



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

## Points of Penetration: Tops & Bottoms

- 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
- Many enclosures come with cable openings that are already knockout or filled with plastic grommet
- The entire bottom of the enclosure is typically an open area that cannot be secured



- *Cable entry remains intact until it is needed*
- *Cable entry that has been removed can be covered/secured with gland plates*



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV



# Locking Mechanisms

## Mechanical

### Pros:

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

### Cons:

- Not centrally managed, so need to be physically touched when employee turnover occurs
- Lack of tamper monitoring
- Lack of tamper resistance



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Locking Mechanisms

## RFID & Pin

### Pros:

- Installation on cages and enclosures
- Stand alone, tie into an existing security system, or integrate with a stand alone software
- Tamper sensors inside the handle
- Capable of real time monitoring if tied into a security system
- 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 shouldered surfed



BICSI 002 12.7.2.2 BICS 005 8.5.1



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Locking Mechanisms

## Biometric

### Pros:

- Installation on cages and enclosures
- Potential three factor authentication
- Can be accomplished with biometric cards
- 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



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Locking Mechanisms

## Popular RFID, PIN, and Biometric Options

													
<b>Authentication Method</b>	Depends on customer's software	Transponder card	Transponder Card + PIN	Transponder Card	Transponder Card + PIN	Depends on customer's software	PIN	Transponder Card	Transponder Card	Transponder Card	Biometrics	Depends on customer's software	Transponder Card
<b>Price</b>	\$\$\$	\$\$\$\$	\$\$\$\$	\$\$\$\$	\$\$\$\$	\$\$\$	\$	\$	\$\$	\$\$	\$\$\$	\$\$	\$\$\$
<b>Typical Lead Time*</b>	1-2 days	1-2 days	1-2 days	1-2 days	1-2 days	1-2 days	4-10 weeks	4-10 weeks	4-10 weeks	4-10 weeks	1-2 days	1-2 days	1-2 days
<b>Other Key Features</b>	-Easily integrates into an existing facility management system	-Well suited for many enclosures located in same location	-Well suited for many enclosures located in same location -Dual factor authentication	-Well suited for enclosures located in different rooms	-Well suited for enclosures located in different rooms -Dual factor authentication	-IP65 rated -Black or white color -Outdoor Applications	-Battery Powered (3 AA) -Up to 20 unique user codes -Manager key w/ 9V electrical override	-Battery Powered (3 AA) -Accepts MIFARE, DES-Fire and HID smart cards -Manager key w/ 9V electrical override	-Accepts HID ICLASS, MIFARE Classic, MIFARE Plus, MIFARE DES-Fire, HID 125 kHz, EM 125kHz -Wiegand Output -Key override	-Accepts MIFARE Classic, MIFARE Plus, MIFARE DES-Fire -Wiegand Output -Key override	-Fingerprint access -Option for EMKA (GER) handle or Southco (USA) Handle -Key override	-Standard electronic lock -Option for EMKA (GER) handle or Southco (USA) Handle -Key override	-Accepts Prox or Mifare -Option for EMKA (GER) handle or Southco (USA) Handle -Key override

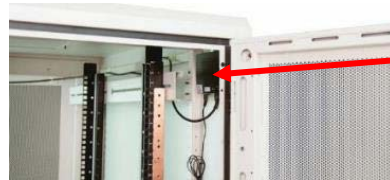


**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
 SEPTEMBER 24-28 | LAS VEGAS, NV

# Locking Mechanisms

## Protecting the Cable

- Cables that communicate with the handle and node are often visible or easily accessible
- Cables can be snipped and or susceptible to a gecko device
- There should be a secure cable pathway from the handle to the node



Visible node & cable



Concealed node & cable



Visible cable from handle to node



Concealed cable from handle to node

Cable pulled through a closed door



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# Fail Safe vs Fail Secure

- Locking mechanisms within a data center facility must typically be characterized as fail safe; locking mechanisms on enclosure doors do not need to adhere to this standard.
- **Fail safe products are unlocked when power is removed:**
  - Traditional layers of security such as doors need to be fail safe, which allow emergency services to access individuals in need of assistance
  - The ability to shutdown a security system by imitating an emergency situation is a potential vulnerability
- **Fail secure products are locked when power is removed:**
  - Enclosures are an unoccupied space, consequently emergency services do not require access in the event of an emergency
  - This means that **when an emergency situation is imitated, the enclosure door will remain closed and locked**



<http://kipandgary.com/blog/comics/#>

BICSI 002 12.7.2.2.3 BICSI 005 8.4.8



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

## Fail Safe vs Fail Secure

- In the event of a power failure and the enclosure must be opened, handles are equipped with various methods to carry out secure emergency openings.
- In this example, through the use of a battery pack, the handle can be opened while it continues to log/report information.

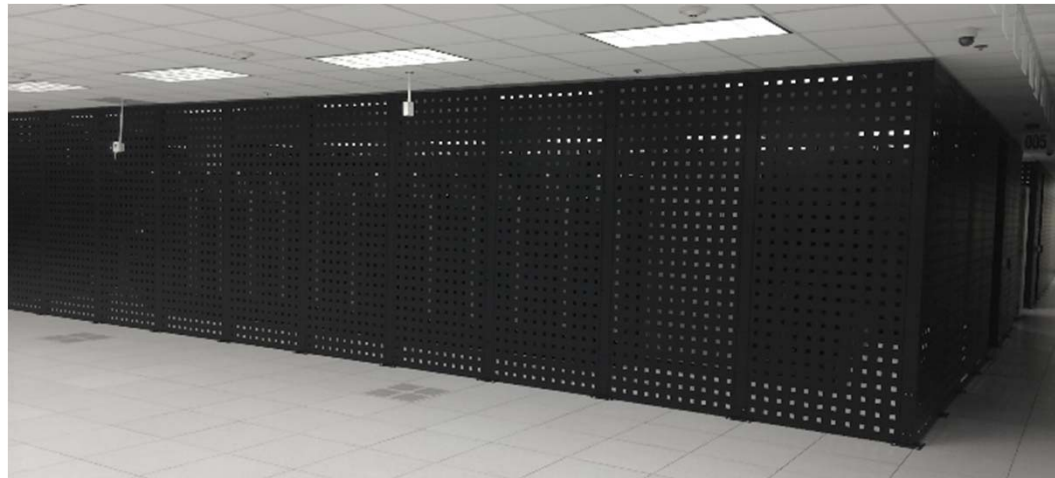


**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
**SEPTEMBER 24-28 | LAS VEGAS, NV**

# Conclusion

In order to prevent forceful, deceptive, or accidental penetration into data center enclosures, products should be deployed that delay, deter, and detect unauthorized entry, while providing real-time alerts to data center managers to decide how to respond to the threat.

A well manufactured cage, enclosure, and superior locking mechanism ultimately creates a sixth layer of security inside of the data center.



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV



# Conclusion

## A true Layer of Security

What are we trying to protect

Why physical security is important

How to create a secure space

## Cage Types

A true layer of security

Where it's frequently used

Types & characteristics

## Secure Enclosure

Points of penetration

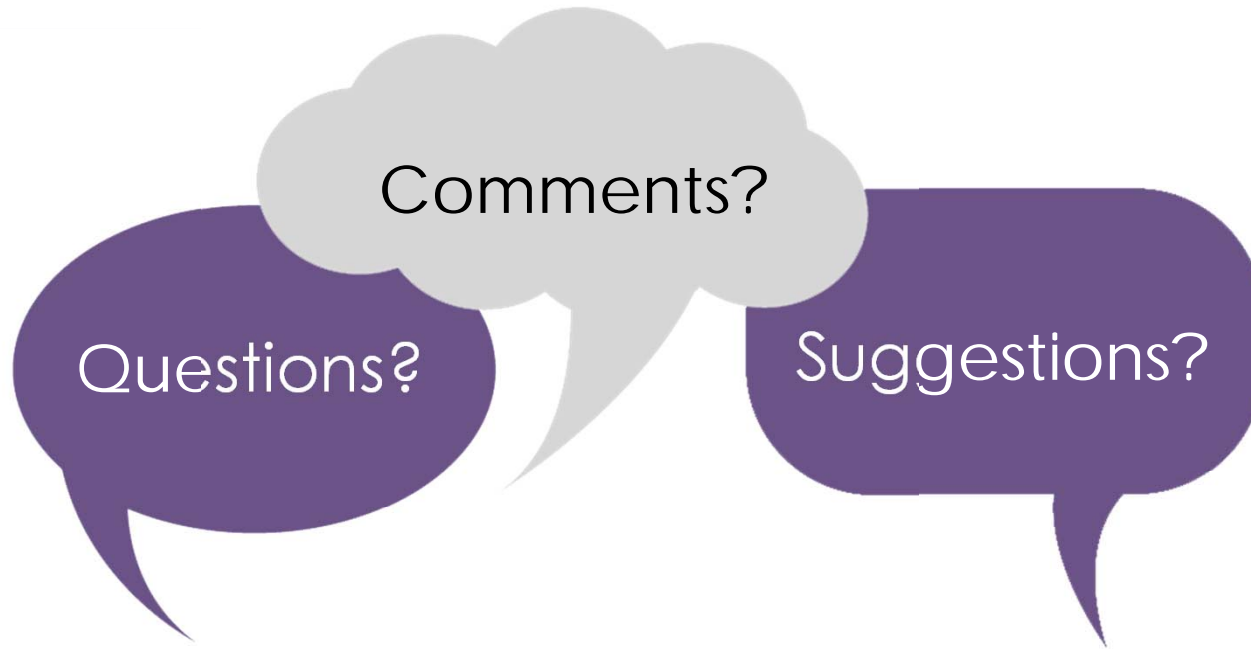
Locking mechanisms

Fail safe vs. fail secure



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV

# Thank You



**2017 BICSI** *Fall*  
**CONFERENCE & EXHIBITION**  
SEPTEMBER 24-28 | LAS VEGAS, NV