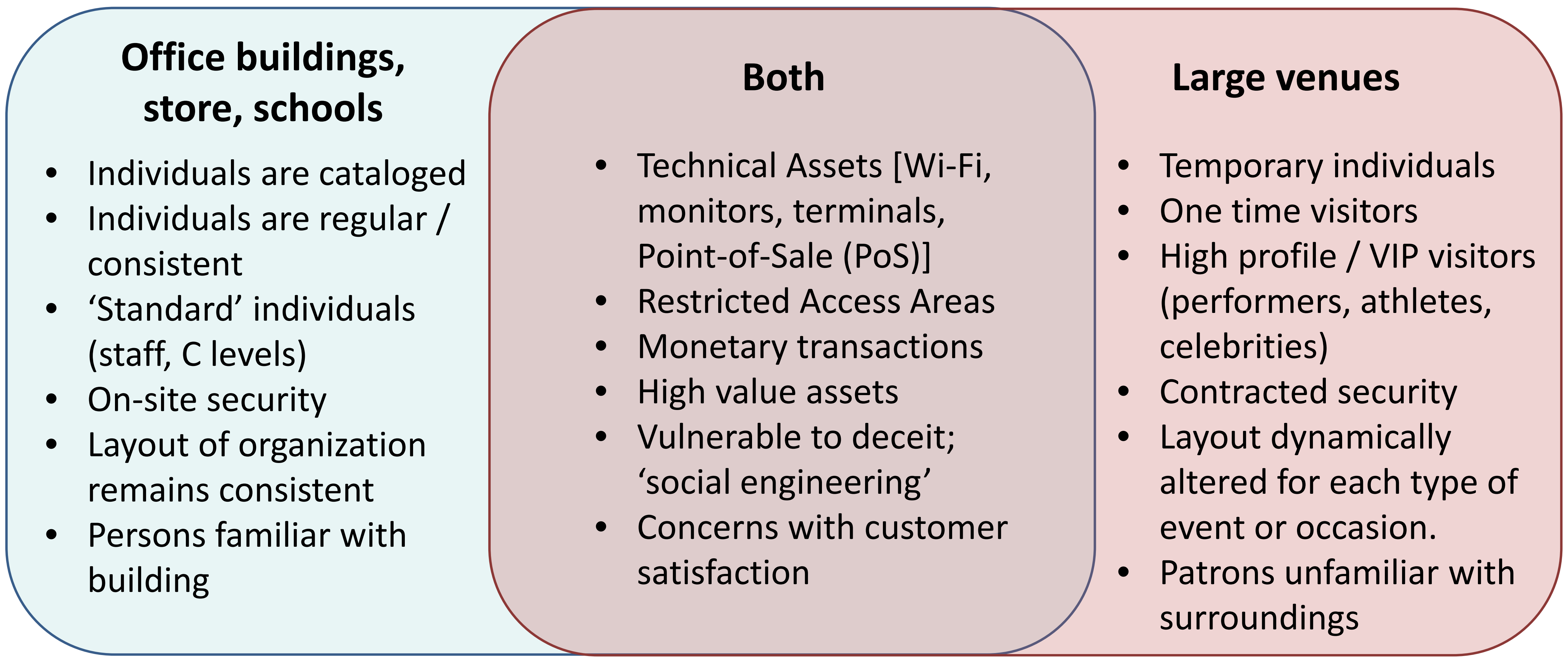
CERIAS
The Center for Education and Research in Information Assurance and Security

PHSI
PURDUE HOMELAND SECURITY INSTITUTE

Security Vulnerabilities for Large Venues

Alissa K Gilbert, J. Eric Dietz

Large venues have different cyberphysical security concerns that require unique attention from standard venues.



Office buildings, store, schools

- Individuals are cataloged
- Individuals are regular / consistent
- 'Standard' individuals (staff, C levels)
- On-site security
- Layout of organization remains consistent
- Persons familiar with building

Both

- Technical Assets [Wi-Fi, monitors, terminals, Point-of-Sale (PoS)]
- Restricted Access Areas
- Monetary transactions
- High value assets
- Vulnerable to deceit; 'social engineering'
- Concerns with customer satisfaction

Large venues

- Temporary individuals
- One time visitors
- High profile / VIP visitors (performers, athletes, celebrities)
- Contracted security
- Layout dynamically altered for each type of event or occasion.
- Patrons unfamiliar with surroundings

- Large venues are categorized as building or locations that can accommodate temporary persons for specific occasions on a large scale (thousands of people).
- Temporary individuals may include contracted employees, temporary workers, volunteers, performers, media personnel, sponsored and representative companies, public safety personnel, fans, patrons, and other individuals.
- On-site security may include digital cameras to hired dedicated security guards; on-site refers to the organization owning these assets instead of a third party.
- Some large venues do have dedicated security, however, many typically contract out security to an independent firm.

Vulnerabilities:

- *Temporary employees*: Have little to no training on security, are not as loyal or invested to the organization; easy insider threats
- *Threat Actors*: Not all threat actors come into the venue as threats, and security concerns develop during the event.
- *Building Security*: Security equipment is often temporary and improperly used. Side-doors or poorly restricted areas may lead to secure areas being vulnerable. Elevators often grant great amounts of permanent access.
- *Poorly prioritizing security*: staff and venue managers risk safety of patrons when ignoring security practices for customer satisfaction. Some areas deemed 'unimportant' may go unmonitored.
- *Credential Stealing*: Credentials for legitimate workers are often cheap for temporary use; they are easy to copy and recycle badges and name tags.
- *Wardrobe / False credentialing:* Some venues do not provide credentials to volunteers or temporary employees, relying on a standard outfit that their volunteers will already own (wearing all black, khakis and a button down shirt) which are easy to clone.
- *Crowd Chaos*: Security exceptions are easy to slip by, blending into the crowd of the venue
- *Temporary equipment*: Equipment left out, unsecured from public

Examples of Large Venues:

- Sporting Arenas
- Convention Centers
- Hotels (hosting events)
- Concert Venues
- Fairs
- Tourist Attractions
- Rallies / Protest locations
- Large Commerce (malls)

Threat Actors:

1. Disgruntled/Obsessive Fans
2. Radicals, Terror Groups
3. Hijackers
4. Criminals
5. Insider threats

Data Collection:

- Long term engagement with a large local venue
- Qualitative and quantitative data gathered through surveying software, pictures, anecdotal reports, and spreadsheets

Recommendations:

- Regular security auditing of security staff, building, and equipment
- Train staff on security concerns and how to handle special situations
- Teach staff to recognize security exceptions (special needs patrons, individuals with equipment, etc.) versus deceitful individuals trying to gain access to restricted areas
- Have policies in place on how to stop fraudulent/dangerous actions and how to report them
- Review building guidelines before an event to ensure no doors, stairways, hallways, backstage areas are left unlocked or unsecured.
- Crowd source security with patron reporting systems

PURDUE UNIVERSITY Discovery Park

PURDUE UNIVERSITY
Department of Computer and Information Technology
POLYTECHNIC INSTITUTE

CERIAS