

CRIME PREVENTION PART II

TCOLE Course #2102



Your Instructor

- **Name:** John Gabrielson, Senior Police Officer/C.C.P.S.
- **Department:** Austin Police Department
- **Assignment:** District Representative/Community Engagement
- **Years of Service:** 16 Years

Cell Number
512-686-1377



Course Objectives

Four Concepts of CPTED

Surveillance, Access Control,
Territoriality, Maintenance

Implementation and Understanding Evidence Based Policing

HARM Focused Policing

Commercial Security Survey / Assessment

Learning the process and basic concepts of Assessments

Business Structure and Information Technology

TCP/IP, Corporate Policy,
Employee Relations

Theft, Robbery, and Burglary Prevention

Power of Prevention



Course Guidelines

Attendance

Be Punctual. You must attend all sessions to receive TCOLE credit

Out of Class Assignments

You will be required to do some research and preparation outside of class

Class Presentation

Community Awareness Presentation

Business Site Survey

Group Presentation and completed survey.



Course Guidelines

Emergencies

If you have an emergency notify the course instructor. They will determine eligibility for make-up work.

Cell Phones

Please silence all cell phones by setting them to silent / vibrate.

Breaks

Class Sessions at 45 minutes and breaks are provided on the hour. There is 1.5-hour lunch

Weapons

Please, always keep weapons holstered.



Administration Forms

- You must list your TCOLE PID# to get credit (No SSN).
- Course is Crime Prevention Part II, TCOLE Course #2102
- Please print legible and complete all required information





Evaluation Forms

- Please evaluate the instructor appropriately as to ensure quality instruction.
- These forms will be handed in before the completion of the course.



Grading Scheme

- **TEST – 50 questions** from material presented up to test time 2-points for each question
- Survey Presentation
- You must achieve a combined passing score of 70% to complete the requirements of this course



Course Grading Matrix

Written Test =	50 Points
Survey =	30 Points
Presentation =	10 Points
Writing Assignment =	5 Points
Class Participation =	5 Points
Total:	100 Points

Participants must complete out-of-class assignments to complete course requirement



Questions



EVIDENCE BASED POLICING & PROBLEM SOLVING

Intermediate Crime Reduction Principles



Learning Objectives

- Review the SARA model
- Review the Five I's of the preventative process
- Review the Problem Analysis Triangle
- What do you think Evidence Based Policing is?
- You will learn the PANDA Model for reducing crime and the implementation of a long-term plan
- You will learn the meaning of HARM focused policing



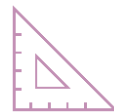
Problem Solving Review



SARA Model

5

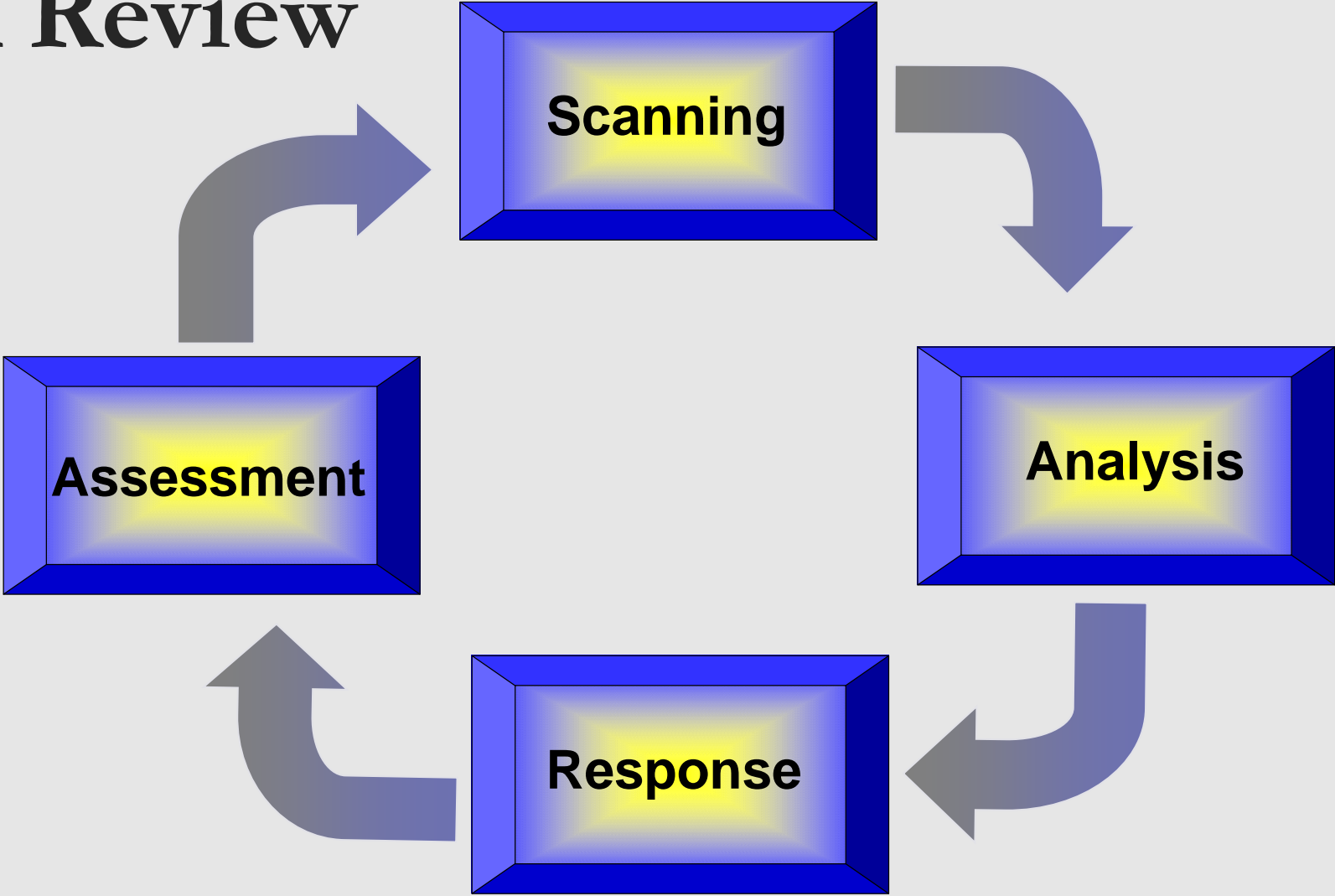
The Five I's



Problem Analysis
Triangle



SARA Review



The Five I's

(Review)

- Intelligence
- Intervention
- Implementation
- Involvement
- Impact



Intelligence

Intelligence is about gathering information while considering the following:

- Crime and disorder problems and their consequences for community safety
- Offenders and their modus operandi
- Causes of the crime problem



Intervention

Intervention is about blocking, disrupting or weakening the causes of criminal events. (3 levels of Intervention)

- Define Crime prevention objectives
- Understand the generic principles of intervention (take or remove opportunity)
- Have practical methods for prevention customized to prevent specific crime



Implementation

IMPLEMENTATION is about converting the intervention principles and methods into practical action on the ground.

- Funds and Human Resources
- Practical actions (i.e. targeting offenders, victims, buildings, places, products, management. etc.)
- Real world outputs (i.e. houses adding security equipment, young people attending youth clubs...etc.)
- Impact long term, medium term, or short-term impact on crime
- The scope of the actin – whether it tackles a board range of crime types or narrow range.



Involvement

Mobilizing other agencies, companies and individuals to play their part in implementing the intervention.

- Who were involved
- What broad roles or specific tasks they undertook
- How they were alerted, informed, motivated, empowered or directed

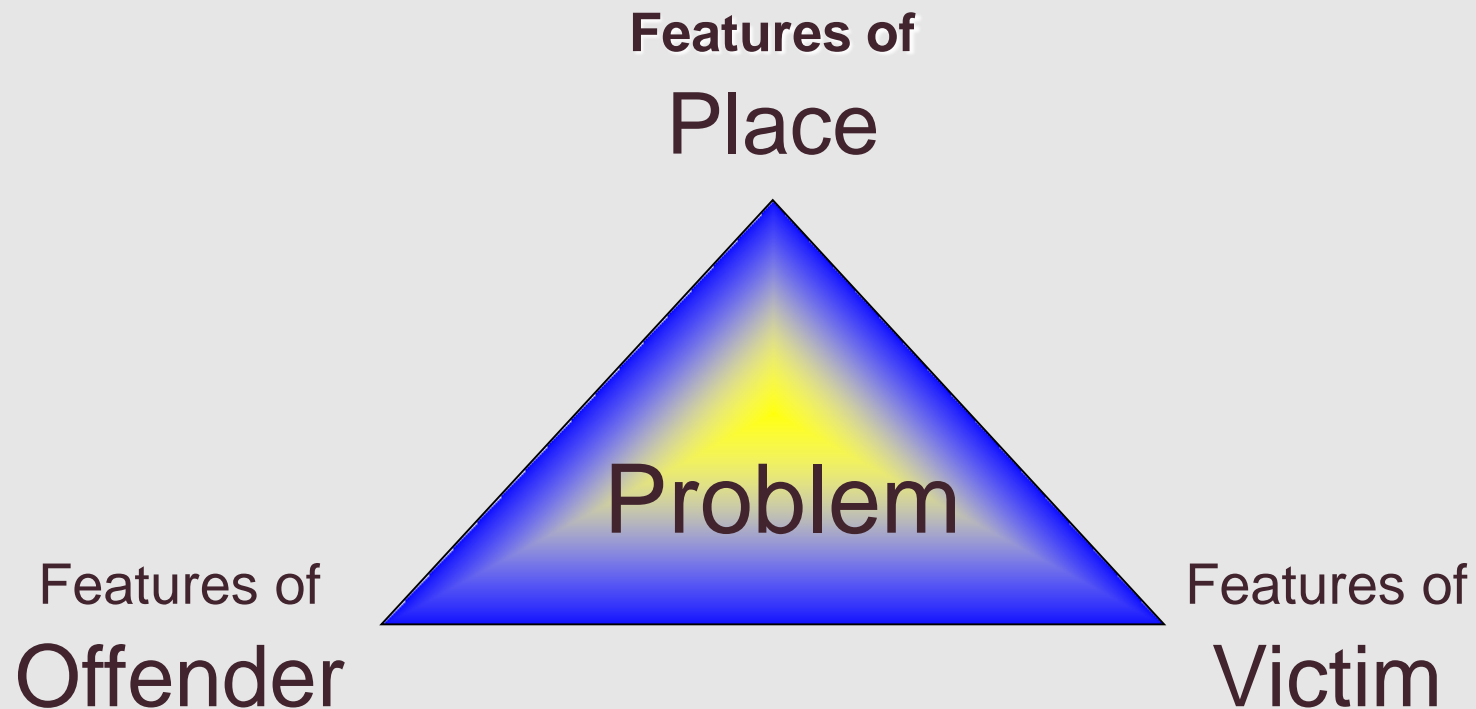


Impact

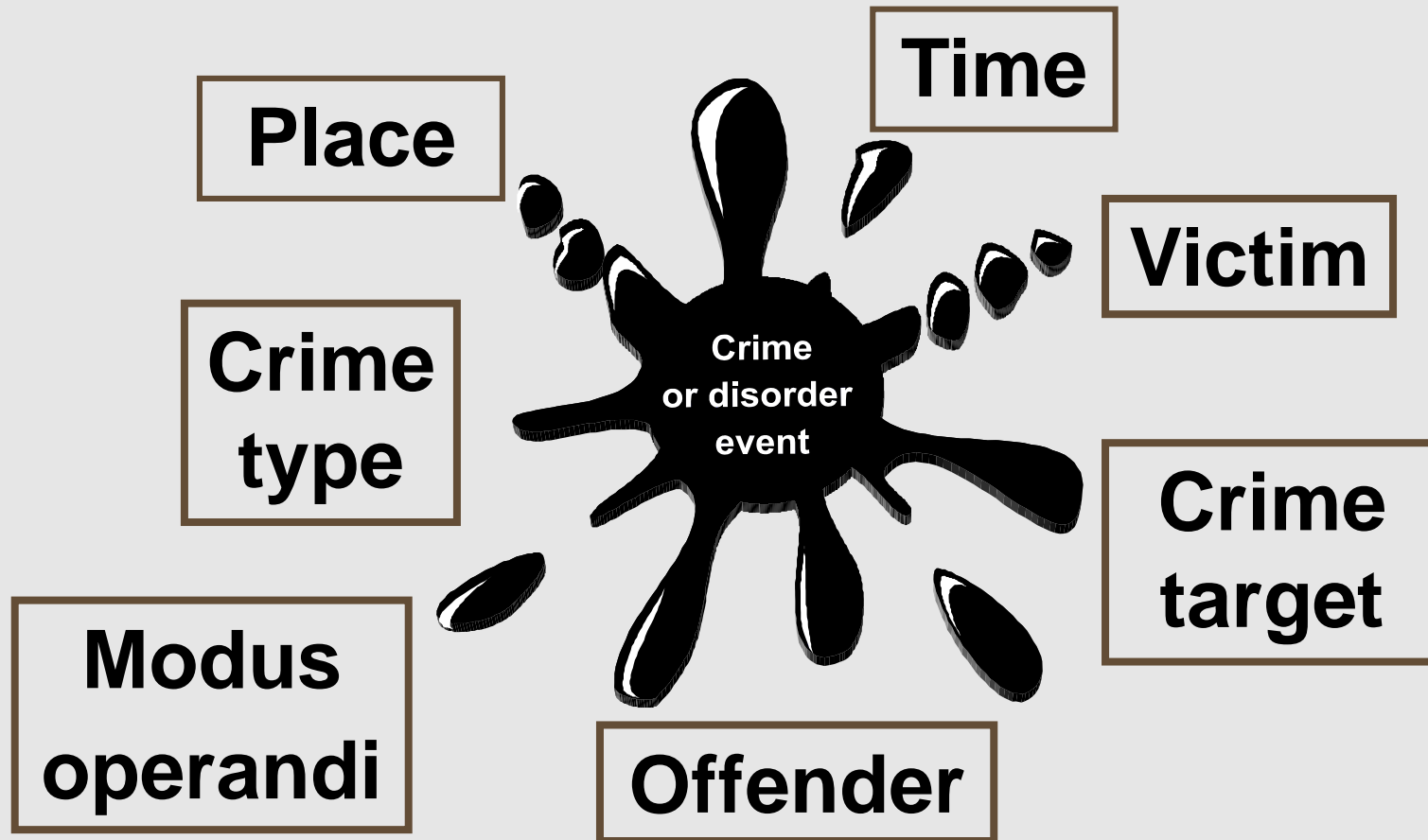
- How the project was assessed, by whom; whether this was a reliable, systematic and independent evaluation; and what kind of evaluation design and statistical tests were used?
- Impact results focusing on the ultimate outcome – how much crime reduction was achieved and how much community safety was improved.
- Was there a change in attitude of young people or to the ownership of property?
- Evaluate the results for each of the Five I's.



Problem Analysis Triangle (Review)



Defining Crime and Disorder Review



Evidence Based Policing

- Professor Sherman – Father of the term evidence-based policing.
- “Police Practices should be based on **scientific evidence** about what works best”
(Sherman 1998)



Two Dimensions of Research

1. Using the result of scientific evaluations of tactics, strategies, and policies
2. Generating and applying analytical knowledge from internal and external sources

This information must be digested and then usable.

It must be become institutionalized and put into actual practice.

“Evidence Based Policing” pg. 3 Lum/Koper



Scientific Approach vs. Traditional Approach

- **Science:** Values Outcomes generated from the rigorous application of accepted methods.
- **Traditional Policing:** The traditional approach values standard operating procedures and legal rules, emphasizing the process over the outcome.



Different Policing Models

- **Community-Based Policing:** Responds to citizens and values their input.
- **Problem-Oriented Policing:** Is based on malleable features of the social and physical environment of the public.
- **Intelligence-led Policing:** Targeting serious offenders, triaging crime problems, using surveillance and informants, making intel the central focus in decision making





RESEARCH



ANALYSIS



EVALUATION



SCIENCE

“Evidence Based Policing” pg. 12 Lum/Koper

Evidence-Based Policing

Suggests: Any actions, strategy, tactic, or internal management approach used to achieve an outcome should not be based on guessing, anecdotal experience, tradition, or a gut feeling. All things need to be tested.



Evidence Based Policing Defined

“Evidence Based Policing doesn’t just require the generation and use of research knowledge to guide decision making. It includes the process and efforts used to make that information digestible, to translate into usable forms, and to incorporate and institutionalize it into the regular system of policing.”

“Evidence Based Policing” pg. 13 Lum/Koper



AN INTRODUCTION TO

Evidence Based Policing

Part of the Evidence-based Policing video series from:



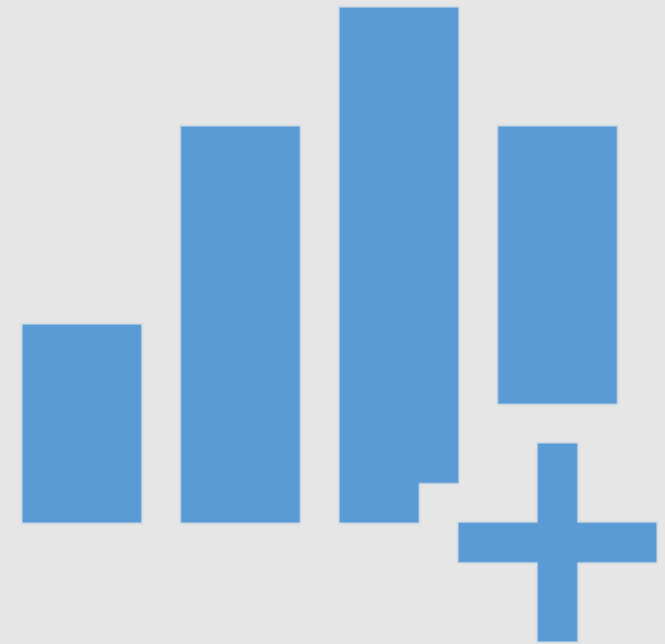
Devon & Cornwall Police



Four Types of Evidence Useful for Policing

- **Scientific Evidence** - Found in Academic Journals, Books, and Reports.
- **Organizational Evidence** – Department Data, Crime History, Old Reports, etc....
- **Professional Evidence** - Knowledge learned from doing the job (i.e. investigators, your own history, and other units knowledge base)
- **Stakeholder Evidence** – Information for the community, those who have a vested interest.

“Reducing Crime” pg. 187 (Dr. Jerry Ratcliff)



Evidence Based Policing & Problem Solving

- **‘Problem-solving’ is the adoption of an evidence-based approach to crime reduction. In practice, this means:**
 - making use of data and information to establish the existence of a problem
 - to analyze its nature and source
 - to plan intervention measures to reduce it
 - and to monitor and evaluate the effectiveness of the selected response
 - (whether the interventions have worked, whether they have produced their effects in the expected way, and whether there have been any significant (positive or negative side-effects))



Challenges of Evidence Based Policing

Lack of good data

Poor information sharing across agencies

Failure to consider what works

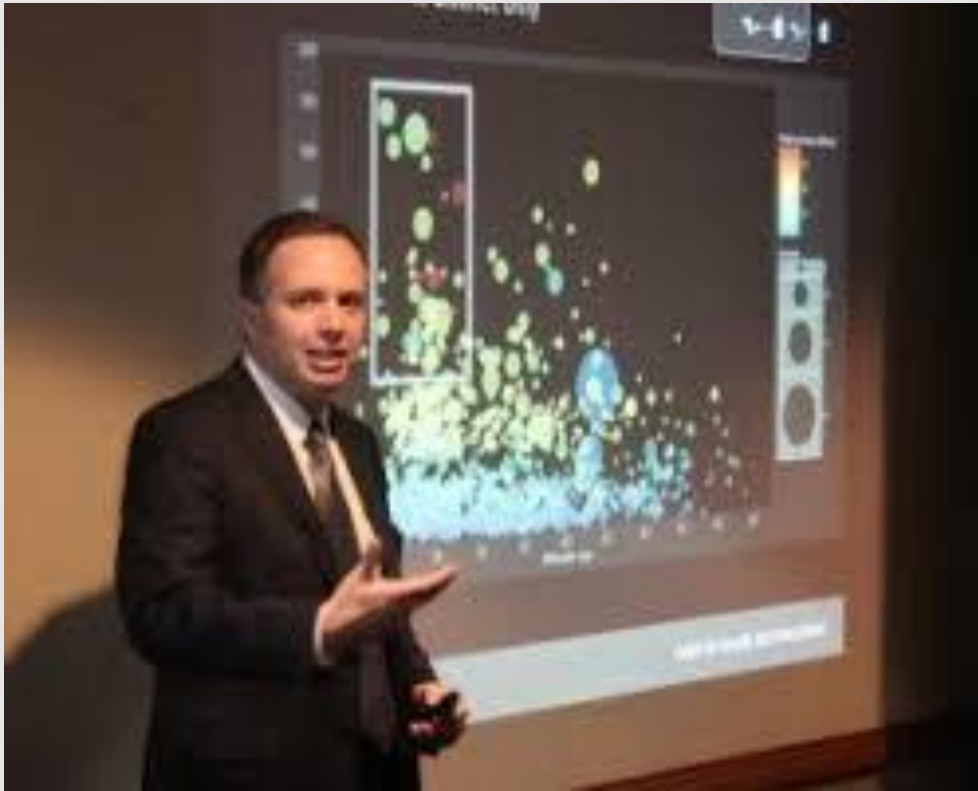
Failure to stay focused on the problem

Too many quick wins – not enough long-term solutions

Poor monitoring and evaluation frameworks



How do we avoid Quick Wins in Crime Reduction?



- Dr. Jerry Ratcliffe – HARM Focused Policing
- “Where police can often see only crime and disorder, community experiences are more nuanced and diverse.”



HARM Defined

“Harm-focused policing aims to inform policing priorities by weighing the harms of criminality together with data from beyond crime and disorder, in order to focus police resources in furtherance of both crime and harm reduction.”

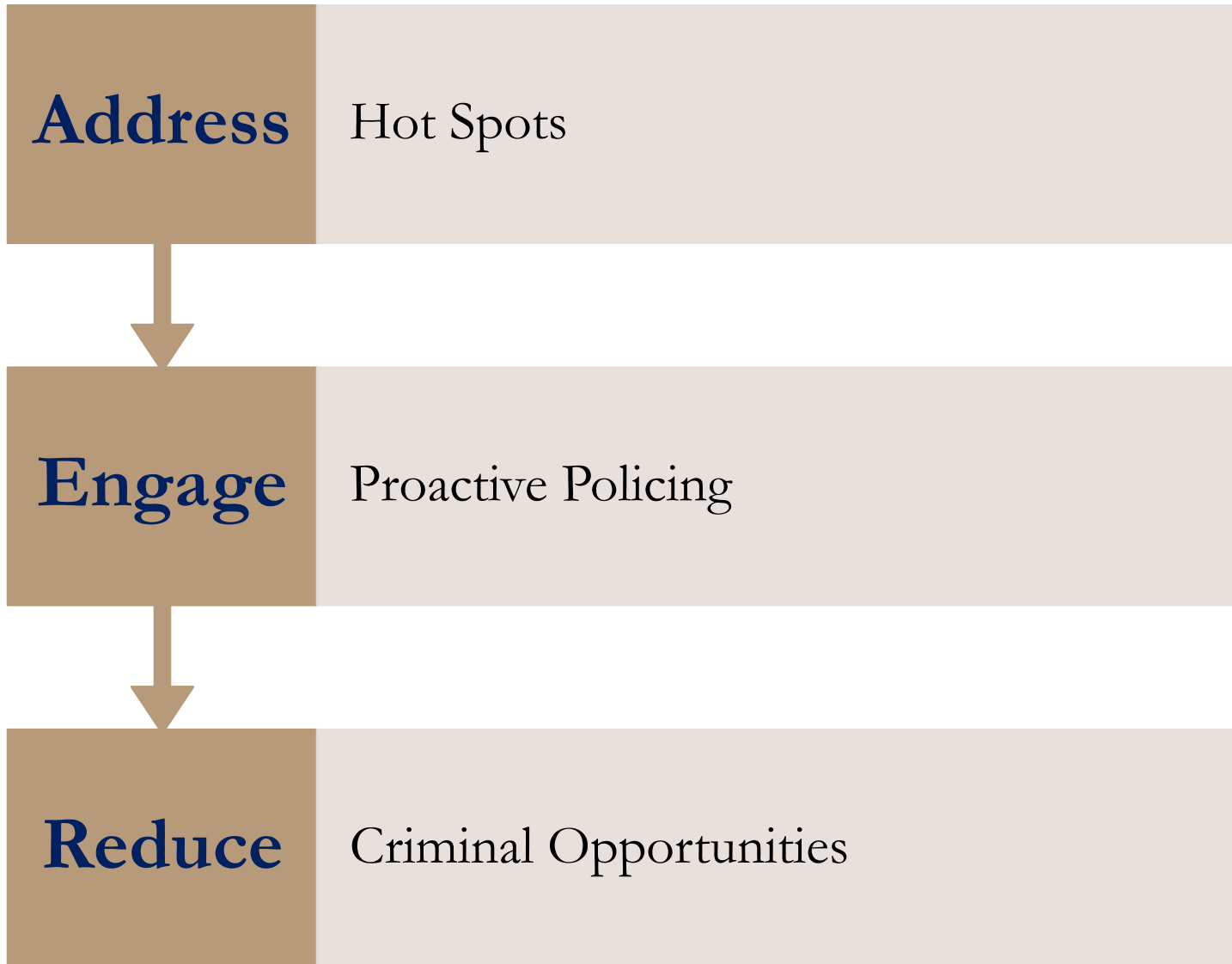
Do no Harm!!



Keys to Successful Crime Reduction

- **H**arm Focused
- **I**ntelligence Lead
- **P**roblem Oriented
- **E**vidence Based





A Deliberate Process for Crime Reduction

More than 90% of police department use hot spots, offender focused, and problem-oriented policing for crime fighting.



Problem

Problem Scan: Scan, describe, frame the problem, select priorities for attention

Analyze

Analyze Problem: establish what is known, not yet understood, what needs to be learned, form a mission statement

Nominate

Nominate Strategy: Use VIPER to address victim support, intelligence gaps, prevention, enforcement, reassurance.

Deploy

Deploy Strategy: have clear objectives, geography, time frame, and assignment of people responsible for leading and implementing, and analyzing.

Assess

Assess Outcomes: Assess the success of your deployment.

Using PANDA for Crime Reduction



P – Problem Scan

- Chronic?

Long term (months or years)?

- Spike?

Short-Term flare-up in Crime?

- Panic?

Possible single crime or public panic?



A – Analyze Problem

- When analyzing the problem the following acronym will guide you: VOLTAGE
- **V**ictims – Are there patterns of victimization?
- **O**ffenders – What is known about offenders?
- **L**ocations – What makes this location a target?
- **T**ime – Are their hot times? Time of Day?
- **A**tractors – Looking for crime clusters? Identify those places.
- **G**roups – Criminal Gangs, criminal organizations
- **E**nhancers – What may be contributing? Drug use, alcohol, mental health



N – Nominate Strategy

- When devising a strategy this acronym will assist: VIPER
- **V**ictim Support – What activities will help aid victims?
- **I**ntelligence Gaps – What assets will help fill those gaps?
- **P**revention – What can be done without police resources?
- **E**nforcement – Where can focused police enforce help?
- **R**eassurance – Is public reassurance needed?



D – Deploy Strategy

- When deploying an initiative the following acronym will assist: GOALS
- **G**round Commander – Who is the case agent?
- **O**bjectives – What is the project or initiative objectives?
- **A**nalyst – Who will monitor and analyze the data?
- **L**imits – Territorial Boundaries/Time Frame?
- **S**upport – What if any additional support is needed?



A – Assess Outcomes

- Was the outcome achieved?
- Was the initiative implemented as planned?
- What additional lessons have been learned?
- Where the results acceptable?
- Was any useful intelligence gained?
- Do the goals need to be revised?



Student Workshop

- **Complaint:** You receive a citizen complaint about a possible drug house and criminal activity in a townhome community on June Lane. This community traditionally has low crime. As a result you may be facing a crime spike, a crime panic, or the start of a chronic crime problem.
- **Area:** Residential, two schools one public and one private in the community. There is also a church, a community center, and park in the area. One major roadway Verdugo Rd is 3 blocks away from June Ln to the north. June Ln is a short street 3 blocks long. North of June Ln is April Ln which connects to Verdugo Rd. Pecan St is to the south of June Ln connecting to Amherst. The public School is directly across the street from the town homes on June.



Student Workshop

- **Concerns:** Citizen's say they found meth on the ground in a baggie, they state there is foot and vehicle traffic mostly after dark. A major concern is the proximity of the schools. The citizen complaining, Adrian, stated he is also concerned about possible retaliation.
- **Facts: The** HOA and the bank holding the mortgage are working on a possible foreclosure on the property in question, Unit #216. There are 3 to 4 people living there possibly renters. Owner may be out state. Patrol has made some stops with one arrest for POCS and a stolen gun maybe linked to the house / townhome.
- Using the PANDA model how would you address this problem . Write a paper referring to the PANDA outlining each part in your approach.
- 700 words or less.



CRIME PREVENTION TERMS

Understanding Crime Prevention



Crime Analysis

- It can be defined as the study of daily reports and crime to determine the location, time of day, special characteristics, and similarities to other crimes as well as any significant data that will or may identify the existence of patterns of criminal behavior. - Handbook of Crime Prevention pg 39



Crime Analysis

- Crime Control Programs
- Crime Displacement
- Crime Prediction
- Crime Prevention
- Crime Resistance
- Crime Specific Countermeasures
- CPTED
- Defensible Space
- Deterrence
- Designing Out Crime



Displacement of Crime

- Can you move crime from one location to another?
- **Dynamic Risk** - A risk situation that carries the potential for both benefit and cost or loss
- **Environmental design** - Selectively creating variables in the planning, design, and the effective use of physical space to create physical and social conditions,



Environmental Security

- It is an urban planning and design process that integrates crime prevention with neighborhood design and urban development.



Enterprise Security Risk Management

- Defined as a strategic security program management approach that ties an organizations security practices to its mission and goals using globally established and accepted risk management principles.



Holistic

This concept is integrating all the components of the security process so that they all work together.



Hot Spots

- The use of hot spots is convenient as they show both the **density and intensity of crimes** in each location and are ideal to summarize areas of concern and the types of incidents that occur
- **Information Transfer** - A means by which professionals and practitioners exchange ideas, concepts, and programmatic information to facilitate the development and the practice of crime prevention.



Creating a Master Plan for Business

- **Security Assessment**
 - Mechanical Crime Prevention
 - Media Campaigns
 - Physical Crime Prevention
 - Private Security
 - Pure Risk



Risk Assessment

◦ It is the process of assessing security-related risks from internal and external threats to an entity, its assets, and its personnel.

- Getting facts
- Analyzing the facts
- What works best for their environment?
- Helping to implement security measures

- Help develop a “culture” of security
- Help ensure “buy in”



What to consider in Risk Assessment

Robbery Awareness

Security Systems

Lighting

Target Hardening





BUSINESS CRIME PREVENTION MODELS

Disaster Planning, Risk Assessment, Vulnerability
Assessment, Internal Theft Controls



BCP Model / A Master Plan

- Crisis Plan
- Emergency Plan
- Disaster Recovery Plan
- Business Resumption Plan
- Business Continuity Plan
- Mechanical Crime Prevention
- Media Campaigns
- Physical Crime Prevention
- Private Security
- Pure Risk



What are you Planning for?

- Strategic Interventions for a Disaster:
 - Loss of a facility
 - Loss of employees
 - Loss of a business system
 - Loss of a key supplier
 - Loss of the ability to communicate with employees and/or our customers



Type of Disasters May Vary

- Weather
 - Hurricanes, tornados, rain, snow, ice
- Natural
 - Volcano, earthquakes, tsunami, floods
- Man-made
 - Fire, vandalism, terrorism, power grid



The Reasons for Having a Plan

- A BCP is meant to protect business assets such as revenue
- Maintain customer relations and good will through a disruption of services
- Minimize the impact on employees, vendors and partners



What Should You Think About?



- Who sets policy?
- Who enforces policy?

- How will awareness be built?
- Training?
- Testing?

- What are the critical areas of the business?
- Replacement of equipment?
- Protection of the employee?
- Continuing operation?

The Steps in Creating a BCP

- There are typically five steps
 - Business Impact Analysis and Risk Assessment
 - BCP Strategy Development
 - BCP Plan Development
 - Training and Validation of Your Plan
 - Maintenance and Exercising of Your BCP

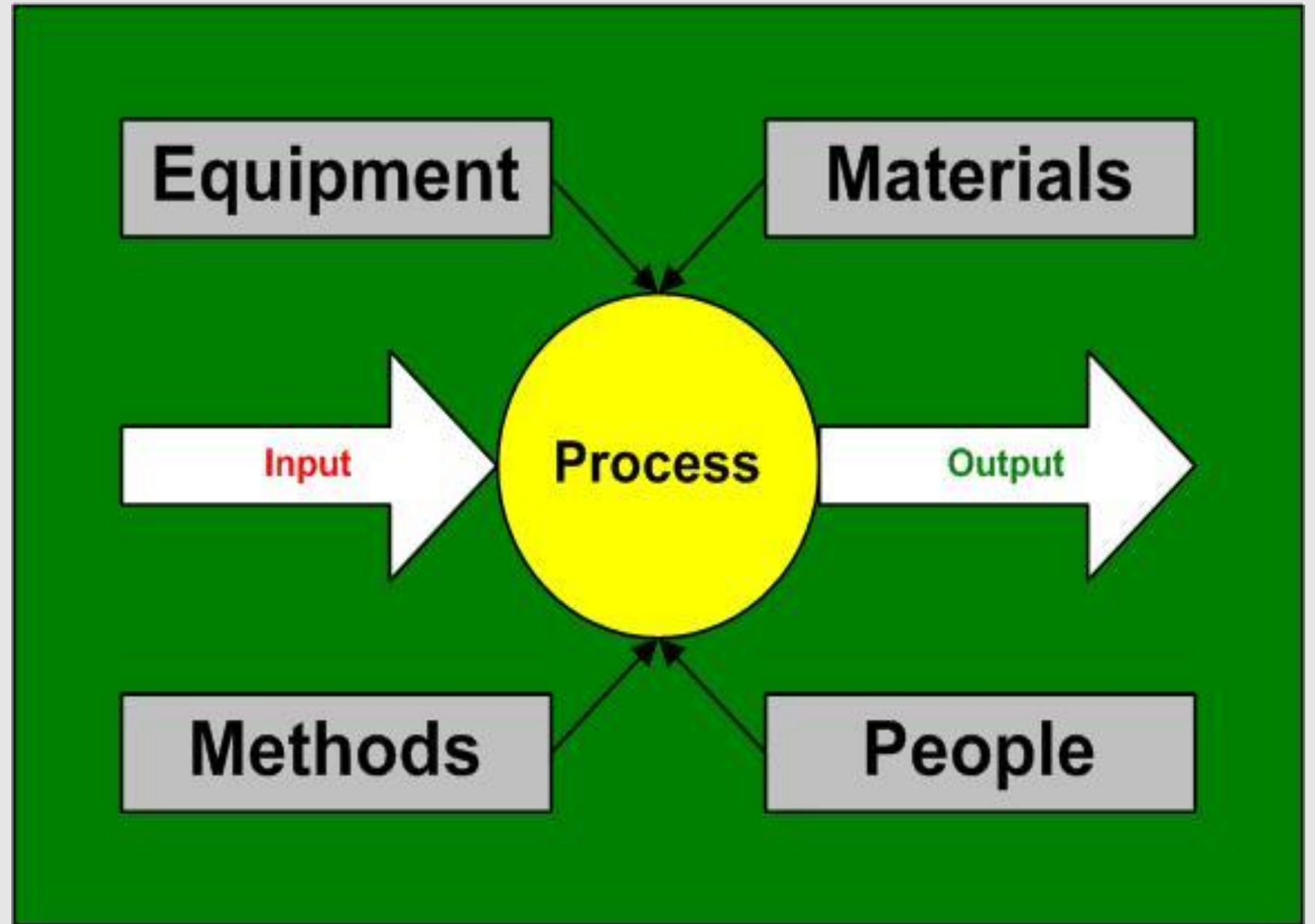


The Business Impact Analysis

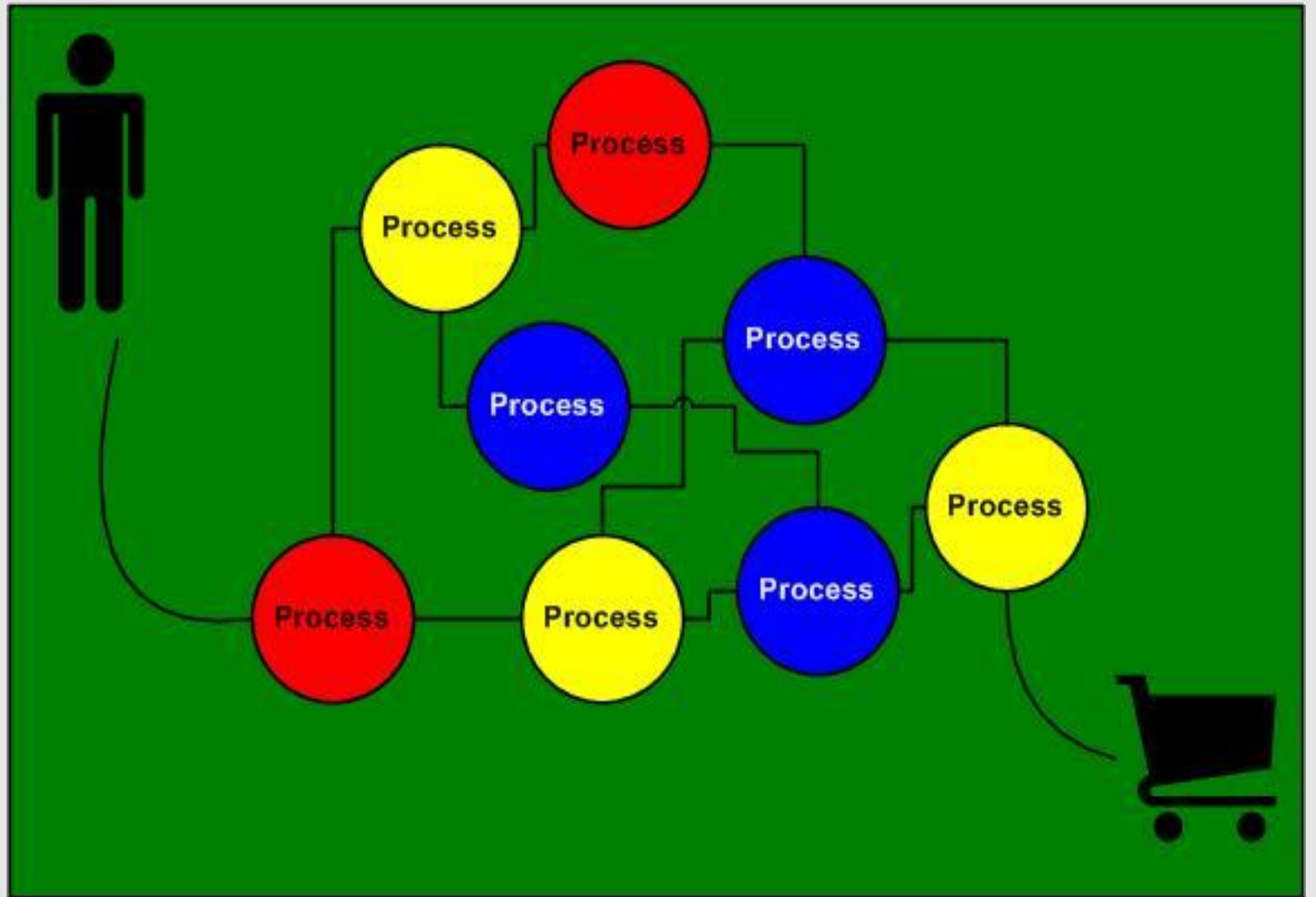
- A Company needs to understand:
 - The business processes, departments, customer touch points, or any other classification that describes how the business interacts people.
 - How long can you do without them?
 - The size of the impact in terms of liability, revenue, good will, etc.
 - What is the minimum number of people to keep going?



*A Process
View*



*Pulling
Views
Together*



Developing a Strategy

- The strategy (response) may vary depending upon the nature of the disaster.
- Disasters may vary significantly depending upon your location
- Risks may vary based on location
- The business must consider how long then can be without a specific process. (that which the company operate)



A Sample Strategy

- Listing where there is interaction with customers or departments.
- Determination of how long each can be out of service
- Estimate the cost to prepare for implementing a strategy
- How many people are needed to keep services going

Process	Days	Alternative Location	Cost	Strategy
Phone orders	<1	Employee homes	\$500	Rerout phones to ring at employee's houses
Shipping	5	Sister plant	\$0	Send orders to sister plant out of state
Training	21		\$0	Will suspend training until recovery is complete



Some Considerations

- **The disaster's impact on community?**
 - Power, Curfews, Transportation
- **What is the impact on people?**
 - Children, Service People, Emergency Response
- **Would contractors or materials be available?**
- **Think about the company facility?**
 - Computers, and other records, employee safety, payroll



Putting Together a Plan Outline

- The scope and objectives of your plan
- How and who will activate it
- The organization and teams responsible
- How people will be notified
- Alternative sites
- Computer files and vital records
- Office equipment and supplies
- Phone numbers, maps, etc.
- Your action plan for keeping the critical processes running



Training for and Testing Your Plan

- Teams or individuals need to be trained on the plan
- An untested plan is no plan at all



Maintaining Your Plan

- People change, phone numbers change.
- Business processes change
- Businesses grow
- Key vendors and partners change

Your plan must change also!



Concluding Points

- A good plan takes time
- It is evolutionary, not revolutionary
- Protect against the most obvious first
- Having a recovery strategy can save time, money and even a business



RISK ASSESSMENT



What is Risk?

- Risk is a subjective concept
- Risk needs to be viewed and quantified on an individual basis.
- **Basic Questions:**
 - What risks do companies face?
 - What is a company's tolerance of risk?



Risk Management Program Defined

- **A risk management program is the formal process utilized to quantify, qualify, and mitigate specific concerns an organization may discover or define.**
- Two questions that will aid in defining the risk management program
 - What is the company's assessment process?
 - Who manages the overall risk management program?



Risk Management Programs

- Two Approaches
 - **Enterprise Approach:** is a concerted effort by various divisions within a company to measure risk across the company.
 - **Key Business Divisions Approach:** Its focus is on divisions that have regulatory mandates for reviewing specific risks or have been identified as businesses that operate within a risk culture.



Components of a Risk Program

- Risk Analysis
- Risk Assessment / Risk Taking
- Risk Mitigation
- Risk Reporting



Risk Analysis

- Risk analysis includes identification of the assets to be protected and the risks to those assets.
 - People (employees/customers, etc.)
 - Facilities (owned/leased properties)
 - Property (sensitive documents/financial instruments/vehicles)
 - Reputation (public perception/client perception).



Typical Risks to Assets

- Natural disasters (hurricane/flood/earthquake)
- Man-made disasters (fire/workplace violence)
- Criminal behavior (fraud/embezzlement)
- Terrorism (international/domestic)



Risk Assessment /Risk Rating

- The risk assessment validates the risk and measures the likelihood of occurrence and the extent of the impact the risk could have



The Assessment

- A risk assessment will measure the following:
 - Qualification of the risk (whether the risk exists)
 - Probability (is likely to occur, very likely, not likely at all)
 - Other risks/vulnerabilities to the asset
 - Knock-on effect (fire in the facility also damages trucks in loading bays)
 - Total effect of risk (probable loss/total maximum loss)



Measuring the Probability of Risk

- Two Parts
 - **Balancing the craft:** Personal experiences, intuition, and insight into a situation
 - **Applying the facts:** Requires a review of all facts related to the risk and asset to assign a high, medium, or low rating of probability



Rating Probability

- **The following indicators should be viewed:**
 - Previous occurrences (whether the facility has been prone to fires in the past)
 - Occurrences in the area or business sector (burglaries in the neighborhood/protests like businesses)
 - Activities in the business sector (whether the business is a target based on its product; e.g., animal rights)
 - Company profile (whether the company is well known and thus more of a symbolic target)
 - Geography (whether the plant is next to a terrorist target or likely to be collateral damage to an attack on a neighbor).





Risk Mitigation

The mitigation phase is where review of the plan to minimize the probability and effects of the identified risk to a company assets.

Risk Mitigation Musts:

- Be goal oriented
- Designed to mitigate specific risks identified

The goal of risk mitigation is to minimize the potential impact of the identified risk to the point, where the concern of the risk is minimal.



Risk Reporting

- The written presentation will “live” longer than the oral presentation.
- Understand the stakeholders to whom you will be reporting.
- Where will this report go? The client may share it with the insurance company; a supervisor may pass it to another supervisor, and so forth.
- Present the facts without exemption; there are many reasons for accepting or ignoring risk. Present the findings and proposed plan, and then allow the decision process to begin.
- Include the security survey and other supporting products utilized to identify the facts.
- There is always a measure of risk acceptance—no plan is absolute.





VULNERABILITY ASSESSMENT

Establishing Protection Objectives



Concepts of Vulnerability Assessments

- Defining the threat
- Identifying assets and prioritizing them by consequence of loss
- Creating a matrix relating threats and assets
- Characterizing a facility to perform a VA



Defining the Threat

- Threat definition establishes the performance required from the physical protection system. By describing the threat, the assumptions that were made to perform the assessment are documented and used to show how they influence required upgrades.
- Threat definition is a tool, which helps site managers understand the impact of successful attacks by defined adversaries and helps PPS designers understand the requirements of the PPS.



The Process for Threat Definition

1. Listing the information needed to define the threat
2. Collecting information on the potential threat
3. Organizing the information to make it usable



Threat Definition Methods

1. Develop threat from historical or intelligence data.
2. Use a policy-based threat issued by an appropriate agency or organization.
3. Create a range of potential threats (threat spectrum).
4. Use defined scenarios of adversary attack.



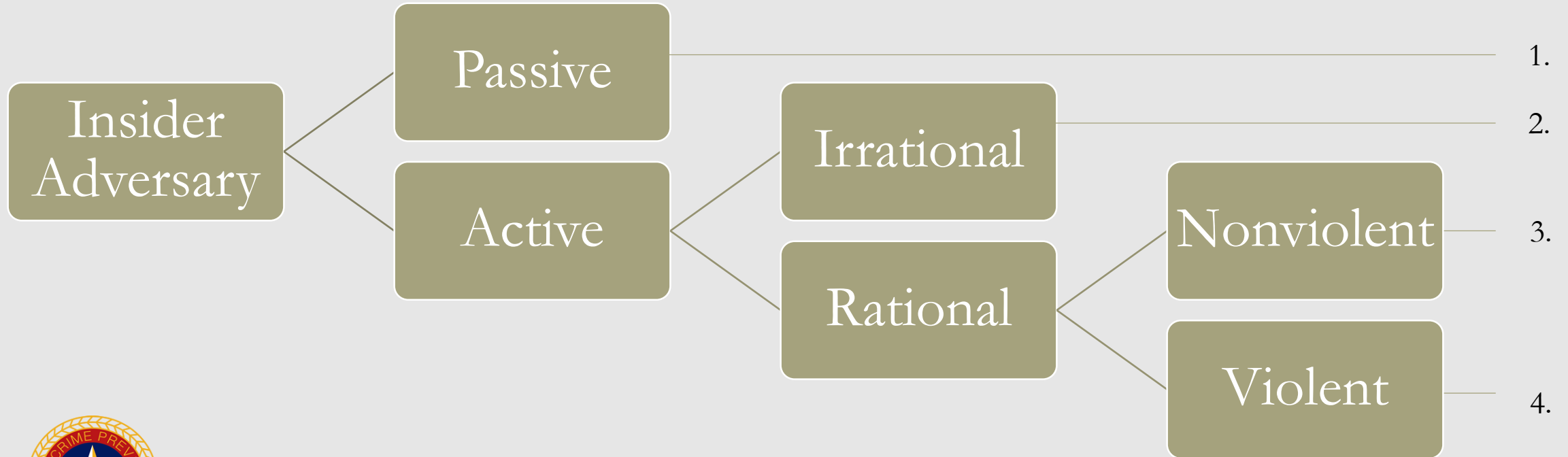
The Insider Threat

- This threat poses one of the highest risks to a security plan and system.
- Why is the insider threat a higher risk than an outside threat?

An insider attack may include: Theft of Equipment, Money, Proprietary, information, high value products, embezzlement, acts of sabotage, vandalism, arson, bomb threats, equipment tampering



4 Insider Threat Categories



Characteristics of Insiders

Passive

- Provides information to a colluding adversary or an outside group

Irrational

- Does not follow a clear decision; uses violence indiscriminately

Rational Nonviolent

- May tamper with and use limited covert force against protections elements; is not willing to be identified

Rational Violent

- Uses overt force, weapons, and explosives against hardware, barriers, or personnel to increase chances of success



Estimating Likelihood of Attack

- **Ways to Determine the likelihood of attack**
 - Historical Data
 - Criminal Statistics
- The probability of attack may be expressed as frequency or likelihood
- **What is Conditional Risk?**
 - The use of conditional risk allows the organization to focus on the **protection around the asset**, rather than spend a lot of time debating the likelihood of attack.



Asset Identification

- Is an evaluation of what to protect by considering the value of the asset to the facility or enterprise.
- **3 Steps for identifying assets:**
 - Specify undesirable consequences
 - Select asset identification technique
 - Identify areas, components, or material to be protected.
- **3 Methods for asset identification**
 - Manual Listing
 - Logic Diagrams
 - Consequence Analysis



Facility Characterization

- The goal of a Vulnerability Assessment is to identify Physical Protection System (PPS) components in the functional areas of **detection, delay, and response** and **gather sufficient data for estimating their performance against specific threats**.
- Data collection is the core of PPS characterization





TCPA COMMERCIAL SECURITY SURVEY

Scope, Purpose, and Objective



Commercial Security Survey

- A security survey is a **critical on-site examination and analysis of a commercial business, office, warehouse, private or public institutions, and/or industrial facility**; to ascertain the present security posture; identify deficiencies or excesses, determine level of protection needed and to make recommendations.
- Crime prevention is the “**anticipation, recognition, and appraisal of a crime risk** and the initiation of action to remove or reduce it”....



Objective of the Survey Report

- **Anticipation:** A primary objective of this report is the anticipation or prevention aspects of a given situation. **Anticipation helps maintain a proper balance in the total spectrum of security surveying.**
- **Recognition:** ability to recognize and interpret what seems to be a crime risk.
- **Appraisal:** The responsibility to develop, suggest, and communicate recommendations to improve a current situation.



Crime Risk

- **An illegal or socially undesirable event, described in terms of the event and the consequences.**
 - Example - the risk of injury to community members through assault in the alley.
- Risk does not have to be quantified to be understood.
- Risk management includes the application of logical and systematic methods for communicating and consulting throughout the process establishing the context for identifying, analyzing, evaluating, treating and monitoring risks and reviewing risks reporting and recording the results.



Crime Risk

- What can happen and why (risk identification)?
- What are the consequences (various contexts)?
- What is the probability of occurrence?
- What factors mitigate the consequences or reduce the likelihood that a risk will be realized?



Alignment with CPTED Crime Prevention

- Outcomes that need to be achieved with your survey:
 - Improved quality of life, and enhanced use of space, lower crime risk;
 - Need to understand factors that run contrary to required outcomes;
 - Need to identify and implement appropriate strategies;
 - Need to be able to describe risks accurately in order to analyze/assess, but not every possible risk; and
 - Useful to draw up a matrix with key stakeholder issues/possible risk events associated with those issues/consequence considerations



Best Time to Conduct a Survey

- The most effective time to conduct a threat and risk assessment is prior to or as part of the initial planning stages of the facility or in support of major renovations.
- Prior to the survey attain some degree of assurance the merchant will implement mitigation strategies to reduce the risks posed to their facility.
- **Reason why to conduct a survey?**
 - To identify what needs to be protected
 - To ascertain current risk/security management needs
 - To determine the vulnerability of an organization's assets
 - To validate that the security management plan combats and identifies threats in a cost-effective and proactive manner.



The classifications you will use as related to businesses security surveys are very high, high, medium, and low security.

Each one of these classifications is related to deter, detect, delay, assess, communicate, and respond.

Very high and occasionally high security classifications, the addition of defend and/or deny may be used to bolster the response portion of the system implemented.

Classifications of Survey Recommendations



Examples of Security Classifications

- **High Security:** Example of high security is focused on protecting the high dollar assets, rare artifacts, and other valuables. *Example: Interior alarms and motion cameras*
- **Medium Security:** Is also focused on protection of assets. However, there are elements of the security program, which may not be implemented or will be implemented differently. *Example: interior alarm verses no interior alarm.*
- **Low Security:** A low security classification will most often be utilized to protect facilities where there are not high value assets at risk.
- When conducting a security survey, **the first step you should take is to interview the individual(s) to whom you will be submitting the report.**



Items Needed for the Survey

- Tape measure
- Floor plans
- Light meter
- Flashlight
- Camera with flash
- Small digital recorder
- Screwdriver
- Pen, pencil, and pad of paper
- Surveyor's wheel



Do's of the Survey

- Familiarize yourself with industry standards and guidance as they relate to security surveys. ISO 17799, ISO 27001, and ISO 27002 (*International Organization for Standardization*)
- ASIS International or government standards and publications
- Be confident and honest in your recommendations.
- Consider the use of simple language; short sentences are best.
- Be critical—visualize the facility and gaps in its security in your mind as part of the process.
- Keep it as simple as possible, but not simpler.



Don'ts of the Survey

- Don't exaggerate your reports. Truthfulness and accuracy are important.
- Don't inflate the reports with filler materials including unnecessary maps and floor plans. Only include these items if they effectively illustrate vulnerabilities.
- Don't repeat your statements.
- Don't make statements beyond your core capability, certifications, and training. It is acceptable to report observations outside of your purview; but, providing considerations for improvement outside of your domain experience is risky, and not a best practice.



Keys to Being a Good Surveyor

- Being able to visualize the potential for criminal activity is a skill that can be refined through practice
- Be prepared to give a property owner sound advice on the type of security precautions to consider.
- Consider environmental criminology and how crimes occur at specific places, times, and settings, and where offenders, victims, and targets of opportunity coincide
- You must be a good investigation
- You must understand criminal methods of operation and the limitations of standard security devices.
- You must be knowledgeable about the type of security systems and hardware necessary to provide varying degrees of protection.



Nine Points of Security Concerns

1. **General purpose of the building:** Consider the hours of use, people who use the building, people who have access, key control, and the maintenance schedule
2. **Hazards involving the building or its occupants:** List and assign priorities (e.g., theft of office equipment, wallet theft, and theft from stockrooms). Identify potential hazards that might exist in the future.
3. **Police or security officer applications:** What can these officers do to improve the response to the building and occupants from a patrol, investigation, or crime prevention standpoint?
4. **Physical recommendations:** Inspect doors, windows, lighting, and access points.



Nine Points of Security

5. **Locks, equipment to be bolted down, potential application of access control systems, and key control**
6. **IDS or alarms:** Would an alarm system be cost effective? Would the use of the building preclude the use of an alarm?
7. **Storage:** Does the building have specific storage problems, such as expensive items that should be given special attention, petty cash, stamps, calculators, or microscopes?
8. **Trespassing:** Are “No Trespassing” signs posted? Are the penalties for trespass noted? Are other signs needed, such as: “No Solicitation” or “No Skateboarding”?
9. **Facilities personnel:** Can facilities personnel be used in a manner that would be better from a security standpoint?



Three Types of Surveys

- **Building Inspection:** Limited to the perimeter and building exterior.
- **Security Survey:** The whole verses just one part
- **Security Analysis:** Full spectrum survey top to bottom.



TCPA Survey

- **Cover Sheet**

- **Section I**

- **Executive summary:**

- Summary of the scope, assessment, and major items for consideration

- **Introduction:**

- Date & time
 - Company Leadership / Managers
 - Company Overview
 - Reporting Police Officer / Police Civilian Surveyor
 - Methodology (describe your approach)
 - Company Overview: (Who, What, Where and How)



TCPA Survey

◦ **Section II**

◦ **Identification of site:**

- Describe in detail location. You can include a digital photo
- Include complete physical address.
- Use county records or google earth for site identification via CAD systems
- Dimensions of property, building, property, attached structures

◦ **External Environment:**

- Number of fire stations, police stations, types of law enforcement, response time.
- Crime Stats, business history, past surveys if any,
- Roadways, traffic flow, parking lots, grass fields
- Surrounding neighborhoods / surrounding stores / border locations



TCPA Survey

- **Section III**

- **Exterior Physical Characteristics: Perimeter Grounds**

- **Observations:**

- Is the fence strong and in good repair?
 - Are there weeds or trash adjoining the building that should be removed?
 - Are the fence gates properly locked?
 - Does lighting illuminate all roads?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

◦ **Section III**

◦ **Outdoor Natural Barriers / Territorial Enforcement:**

◦ **Observations:**

- Is there shrubbery near windows, doors, gates, garages, and access roads being kept to a minimum?
- What are the physical boundaries of the residence's grounds?
- Is proper signage in place?

◦ **Recommendations:**

- Minimum and Maximum



TCPA Survey

◦ **Section IV**

◦ **Exterior Doors:**

◦ **Observations:**

- Are all doors strong and formidable?
- Are all door hinge pins located on the inside?
- Are all door frames well constructed and in good condition?
- Are the exterior locks double cylinder, dead bolts, or jimmy proof?

◦ **Recommendations:**

- Minimum and Maximums



TCPA Survey

- **Section IV**

- **Exterior Windows:**

- **Observations:**

- Are nonessential windows bricked up or protected with steel mesh or iron bars?
 - Are all windows within 14 feet of the ground equipped with protective coverings?
 - Is security glass used in any of these windows?
 - Are windows located under loading docks or similar structures protected?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section IV**

- **Other Exterior Openings:**

- **Observations:**

- Do you have a lock on manholes that give direct access to your building or to a door that a burglar could easily open?
 - Are your sidewalk doors or grates locked properly and secured?
 - Do fire escapes comply with city and state fire regulations?
 - Can entrance be gained from an adjoining building?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section IV**

- **Exterior Lighting:**

- **Observations:**

- Is the lighting adequate to illuminate critical areas (alleys, fire escapes, ground level windows)?
 - Is there sufficient illumination over entrances?
 - Is there an auxiliary system that has been tested?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Interior Physical Characteristics:**

- **Observations:**

- Which hours and days represent high-activity use?
 - How many people have access to the site?
 - List the number of rooms occupied by the various departments and offices.
 - What area contains the most sensitive material?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Interior Lighting:**

- **Observations:**

- Is there a backup system for emergency lights?
 - Is the lighting provided during the day adequate for security purposes?
 - Is the lighting at night adequate for security purposes?
 - Is the night lighting sufficient for surveillance by the local police department?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Interior Doors:**

- **Observations:**

- Are doors constructed of a sturdy and solid material?
 - What type of hinges, and is there a need for peep hole?
 - Are interior doors equipped with locks, door returns, safety bars?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Interior Offices:**

- **Observations:**

- Are office doors locked when unattended for long periods?
 - Does the receptionist desk have a clear view of the entrance, stairs, and elevators?
 - Are maintenance people and visitors required to show identification to the receptionist?
 - Are desks and files locked when the office is left unattended?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Key Control:**

- **Observations:**

- How many keys are issued?
 - How many master keys?
 - Is there a key control system?
 - What is the basis of issuance of keys? Are keys marked “Do Not Duplicate”?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Locks:**

- **Observations:**

- Are all entrances equipped with secure locking devices?
 - Are they always locked when not in active use? (If not, why not?)
 - Is the lock designed or the frame built so that the door cannot be forced by spreading the frame?
 - Are all locks in working order?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Petty Cash:**

- **Observations:**

- How much petty cash is kept?
 - Are funds kept to a minimum?
 - Where is petty cash secured?
 - Are funds kept overnight in a safe, locked desk, or file cabinet?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Safes:**

- **Observations:**

- What methods are used to protect the safe combination?
 - Are combinations changed or rotated immediately on resignation, discharge, or suspension of an employee having possession of the combination? If not, why not?
 - Where is (are) the safe(s) located?
 - Is it well lit at night?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Inventory Control:**

- **Observations:**

- When was the last time an inventory of business equipment was made, listing serial numbers and descriptions?
 - Were any items missing or unaccounted for?
 - Are all computers and similar equipment bolted down or otherwise secured?
 - Has the firm marked all its business equipment?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Security Camera, Alarm Systems, Technology:**

- **Observations:**

- What type of alarm system is it, make, model, manufacturer
 - Who maintains it (maintenance) and how often is it serviced (checked), date of last service
 - What is the total number of sensors and types?
 - What is the type of camera, type, model, how many, and the angle of coverage?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section V**

- **Retail Security:**

- **Observations:**

- Loss Prevention and external theft policy?
 - What are the internal theft controls?
 - Is there workplace violence training?
 - Is there personal safety training including robbery awareness?

- **Recommendations:**

- Minimum and Maximum



TCPA Survey

- **Section VI**

- **Conclusion**

- Overall building security findings and summary
- Any Additional observations, findings and recommendations
- You may plant inspections
- You may also add vulnerability assessment



TCPA Survey

◦ **Section VI**

- **LIABILITY DISCLAIMER:** The implementation of all or any portion of the recommendations in this Security Assessment of (name of the site as listed on the cover of the report) are **NO** guarantee or assurance that crime will go down, nor will they make the property crime-proof. The recommendations should, however, reduce the probability of crime if the strategies and recommendations are properly applied and consistently maintained





INTERNAL THEFT CONTROLS

For Small and Large Business



Let's Talk About Honesty

- Defined: “Fairness and straightforwardness of conduct, speech, etc.; integrity; truthfulness; freedom; freedom from fraud.”
- “Security must be based on a controlled degree of relative honesty” - Charles Carson



The Dishonest Employee

- Maybe some reason why employees steal?
 - Resentment over real or imagined injustice
 - Maintain Status and augment their income
 - To handle a life emergency
 - Maybe they want simply indulge themselves



It all goes back to the Crime Triangle

- Motive
- Desire
- Opportunity



Identify Danger Signs

- Changes in employee lifestyle: Buying expensive cars, clothes, or live beyond means
- Poor hiring decisions are a root of many problems
- Garnishments and Inquiries by creditors
- Gambling
- Excessive Drinking / Drug Use
- Lot's of borrowing / Cash Advances / Bouncing Checks



What Employees Steal

- The employee thief will take anything that may be useful or has resale value!
- They steal in many ways
 - directly or indirectly, through collusion with vendors and outside thieves or hijackers, fake invoices, receipting for goods never received, falsifying inventories, payroll padding, false certification of overtime, padded expense accounts, computer-record manipulation, overcharging, undercharging, or simply by gaining access to a cash box.



Methods of Theft

- Twenty Percent of business failures are the result of employee in theft according to studies.
- Falsify Records
- Cheating on overtime
- Truck drivers / Receiving Clerks taking property
- Mailroom Theft
- Taking cash from the register



Program for Internal Security

- The first requirement before setting up protective systems for internal security is to survey every area in the company to determine the extent and nature of the risks.
- Second every company needs Management Support
- Third is Communicating the Program
- Continuing supervision



Program for Internal Security

- A Company may need program changes
- Violations need to be handled immediately



The Procedural Controls to Combat Theft

- **Auditing Assets:**

- Should be done by an outsider and is essential to security program
- Should be conducted once a year
- A company should examine: inventory of schedules, prices, footings, and extensions, financial audits, accounts payable, and account receivable



The Procedural Controls to Combat Theft

- Cash – is one of the most vulnerable and most sought after
- Cash by Mail – rare but still used by some small business
- Daily Receipts – Cash accounting must be done daily along with spot checks



The Procedural Controls to Combat Theft

- Bank Statements: Should be received and reconciled by someone who is not authorized to make deposits.
- Petty Cash: Petty Cash should never be comingled with other funds. There should be a voucher system in place

Petty Cash Voucher NO. _____

DATE _____ AMOUNT

PAID TO _____

FOR _____ ACCOUNT _____

FOR _____ ACCOUNT _____
(attach documentation)

RECEIVED BY _____ PAID BY _____



The Procedural Controls to Combat Theft

- **Separation of Responsibility:** The principle of separation of responsibility and authority in matters concerning the company's finances is of prime importance in management
- **Access to Records:** Many papers, documents, and records are proprietary or at least available to only a limited number of people who need such papers in order to function.
- **Forms:** They should always be secured and accounted for. They should be sequentially numbered and recorded regularly so that any loss can be detected immediately.



The Procedural Controls to Combat Theft

- **Computer records or electronic mail and funds transfer or fax:** Computers must be password protected
- **Purchasing:** Is broken down into two areas
 - **Centralized Responsibility:** Makes controls centralized
 - **Competitive Bids:** Is good practice and allows a level playing field (Example: Through out high bid low bid keep middle bid)
- **Other Controls:** Audit Vendor Invoice, Audit Purchasing, payments authorized for product received



The Procedural Controls to Combat Theft

- **Payroll:** It is important that the payroll be prepared by persons not involved in its distribution.
 - Personal Records
 - Unclaimed Payroll Checks
 - Payroll Audits



The Procedural Controls to Combat Theft

- **Accounts Payable:** Should be centralized to handle all disbursements on adequate verification of receipt and proper authorization for payment.
- **General Merchandise:** Merchandise is always subject to pilferage, particularly when it is in a transfer stage, such as being shipped or received.



The Procedural Controls to Combat Theft

- Three ways to Combat theft of General Merchandise:
 - Separation of Functions – Receiving, Warehousing, and Shipping
 - Inventories – Should be conducted by a third party
 - Physical Security – Restrict access with security guards



The Procedural Controls to Combat Theft

- **The Mailroom:** The mailroom can be a rich field for a company thief.
 - **Why?** Some firms have taken the view that the mailroom represents such a small exposure that close supervision is unnecessary.



The Procedural Controls to Combat Theft

◦ **Trash Removal:**

- Employees hiding stolen equipment in trash cans,
- Trash cans being close to receiving areas and unsecured merchandise
- Sensitive papers not shredded or secured.



When Control Fails

- Are there times when a company is beset by internal theft that cannot be identified?
- Things to consider
 - Hiring an outside security firm
 - Use undercover agents to blend in.
 - These agents must proper qualifications for the level of employment being given
 - Must work alone
 - Don't use well-meaning amateurs



Prosecution or No Prosecution

- Three Alternatives
 - Prosecute the Thief
 - Discharge the Thief
 - Retain the Thief



5 Reasons Why Discharging is Best

1. Discharge is a severe punishment, and the offender will learn from the punishment.
2. Prosecution is expensive.
3. Prosecution would create an unfavorable public relations atmosphere for the company.
4. Reinstating the offender in the company—no matter what conditions are placed on the reinstatement—appears to condone theft.
5. If the offender is prosecuted and found not guilty, the company is open to civil action for false arrest, slander, libel, defamation of character, and other damages.



Borderline Cases

- What might be considered a borderline case?
 - The pilferer,
 - The long-time employee,
 - The obviously upright employee in financial difficulty, who steals out of desperation.

These cases each have a common theme
Offender Freely Admits Guilt and Pleads Guilty



Summary

- Internal Theft is single most important issue for the Loss Prevention Manager
- More Companies fail due to internal theft than any other security issue
- Understanding the of theft provides a solid basis for control
- Background checks reduces employee problems dramatically





EXTERNAL THEFT CONTROLS

Shoplifting, Skimmers, ID Theft



Understanding Shoplifting

- The National Association for Shoplifting Prevention (NASP) found that shoplifting costs retailers about \$13 every year, and the American taxpaying public a total of about \$33.21 billion yearly, or about \$75,000 every minute!
- 1 in 11 people will commit retail or shoplifting in their life
- In the last years only about 10 million shoplifters have been caught
- The cost of retail is theft is passed onto the consumer
- According to NASP, both men and women shoplift in approximately equal proportion.
- 25% of shoplifters are underage
- 55% of adult shoplifters say they started shoplifting in their teens



Shoplifting Patterns

◦ Time

- After School
- Wednesday through Sunday
- Peak retail seasons (Holidays)
- School Summer Vacation

◦ Location

- Businesses that open to the street
- Store lay out that prevents surveillance
- City Centers
- High Traffic Areas
- Small Retailers

◦ Merchandise

- Concealable
- Removable
- Available
- Valuable
- Enjoyable
- Disposable



Addressing Shoplifting

- Shoplifting is a common occurrence but **it is the least detected and reported crimes affecting retailers**
- Why should Shoplifting be addressed?
 - The losses overtime impact on net profits
 - These losses often put small retailers out of business thus leaving empty store fronts



Define the Nature of Shoplifting

- **Questions to have retailers ask themselves when defining an external theft problem:**
 - What is the difference between your store's sales and inventory value for the previous quarter?
 - Can you distinguish whether your loss is due to shoplifting or from internal/employee theft?
 - How many documented shoplifting incidents has your business experienced over the past quarter?
 - What time of day and day of week did documented shoplifting or losses occur?
 - What items are most often stolen from your store or area businesses?
 - Is theft affecting particular stores in addition to yours? If so, what do you have in common with them?
 - Are you and other area businesses having similar items stolen?
 - Do the documented shoplifters share any particular demographic or other characteristics?



Sample Response Strategies for Retailers

Measurement	Data Source	Response	Outcome
General Theft			
<ul style="list-style-type: none"> • Repeat Offenders • Sales / Profit • Number of Incidents • Location 	<ul style="list-style-type: none"> • Police • Business Records 	<ul style="list-style-type: none"> • Reduce the Number of exits • Train staff on detection • Post No Shoplifting Signs • Cameras 	<ul style="list-style-type: none"> • Fewer Repeat Offenders • Increase Profit • Incidents less concentrated
Youth and Theft			
<ul style="list-style-type: none"> • Times • Number of incidents • Demographics • Products being stolen 	<ul style="list-style-type: none"> • Police • Business Records 	<ul style="list-style-type: none"> • Work with local school officials and police • Package cd's/dvd's in oversized packaging • Keep high value targets behind the counter, in show cases 	<ul style="list-style-type: none"> • Fewer Incidents after school • Fewer Youth offenders • Less likely to target video games, cd's/dvd's



Other Prevention Tips for Retailers

- **Double Check Merchandise:** Check incoming merchandise against invoices and outgoing products against shipping documents or other sales data.
- **Reorganize your space:** Eliminate Blind spots, increase lighting, move checkout stands near exits
- **Post Staff Around the Store:** Have staff greet customers while moving around the store paying attention to blind spots
- **Require Receipts for cash returns:** Require customers seeking a return for cash to produce a receipt for the item(s). This policy is zero tolerance and enforced 100% of the time.
- **Ask for ID:** Ask customers for a piece of identification when they make a return or exchange.



Skimming Overview

- Skimmers rely on sophisticated data-reading electronics to copy the magnetic stripe information from the victims credit card or debit card.
- When a victim slides the plastic into point of sale device the skimming device reads it first followed by the original card reader.
- Skimming Devices can be read by the thief via Bluetooth, or cellular



Three Payment Points Related to Skimming

- **Fuel dispensers:** Convenience stores sell 80% of the gas purchased in the United States, and there are more than 122,000 convenience stores that sell fuel.
- **Restaurants and bars:** An unscrupulous server can swipe a customer's card in a skimmer in addition to swiping the card legally when taking payment.
- **ATMs:** Skimming devices can be attached to ATMs to gather card information. There are about 425,000 ATMs



Types of Skimmers

- **External skimmers:** Overlays that can be quickly installed by criminals to the keypad or card reader. They collect data strokes. The thief does not need access to the inside of the machine.
 - Look to see if the keypad is raised to an unusually high level. While thin, the overlays will still be obvious if you look closely.
 - Look to see if the keypad is secure. Overlays are typically secured with an adhesive and may be crooked or not adhered fully.
 - Look for telltale visuals. If a keypad appears new yet the rest of the dispenser is weather beaten, that could be a signal a skimmer has been recently installed.



Types of Skimmers

- **Internal skimmers** are attached inside a fuel dispenser. These are box-like devices usually 2 to 3 inches long.
- **Two Methods of Installation of internal skimmers:**
 - Thief has a key
 - Pry the device door open
- **Ways to guard against internal skimmers:**
 - Regularly inspect dispensers to detect signs of entry
 - Use tamper-evident labels on door entries







IDENTIFICATION THEFT



Definition

- Identity (ID) theft is a crime in which a thief steals your personal information, such as your name, your social security number (SSN) or your credit card information to commit fraud.
- **Types of ID Theft**
 - **Tax ID theft**—Someone uses your SSN to falsely file tax returns with the Internal Revenue Services (IRS) or your state.
 - **Medical ID theft**—Someone steals your Medicare ID or health insurance member number. Thieves use this information to get medical services or send fake bills to your health insurer.
 - **Social ID theft**—Someone uses your name and photos to create a fake account on social media.





ID Theft Prevention

Secure Social Security
Cards / EIN Numbers

Don't share personal
Information

Collect mail daily

Set firewalls on servers and
protect work Wifi network

Create complex passwords

Review credit reports





PROTECTING PROPRIETARY INFORMATION

Introduction and Overview



What is Proprietary information?

- Proprietary information is information owned by a company or entrusted to it that has not been disclosed publicly and has value.
- **The following conditions make information proprietary:**
 - Not readily accessible to other
 - It was created by the owner through the expenditure of considerable resources
 - The owner activity protects the information from disclosure



Patents

- What is a Patent?
 - These are grants issued by a national government conferring the right to exclude others from making, using, or selling the invention within that country.



- Most common
- Related to technology
- Includes drawing charts, and software

Utility
Patent

- Only in the US
- Function is not important
- Covers drawing or design itself

Design
Patent

- Involving plants/
flowers

Plant
Patent

- Each country has
different rules

Non-
US
Patents



Overview of Common Patents Infringements

- Direct Infringement
- Indirect Infringement
- Contributory Infringement
- Induced Infringement
- Willful Infringement
- Literal Infringement



Trademarks

- What is a trademark?
 - These are words, names, symbols, devices, or combinations thereof used by manufacturers or merchants to differentiate their goods and distinguish them from products that are manufactured or sold by others



Ways to violate:
Counterfeiting or Infringement



Copyrights

- What are copyrights?
 - These are protections given by a national government to creators of original literary, dramatic, musical, and certain other intellectual works.
 - Violations are known as **infringement and piracy**



Trade Secrets

- **What is considered a trade secret?**
 - These can be formulas, patterns, compilations, programs, devices, methods, techniques, and processes that derive economic value from not being generally known and not ascertainable except by illegal means.
- **What are the key Elements of a Trade Secret?**
 - The maintenance of **confidentiality, limited distribution, and the absence of a patent.**



Data Protection is Important

- Data is a valuable corporate asset. Here are a few examples to consider:
 - In the minerals extraction industry, finding ores depends on data (seismic/scientific data)
 - Hotels routinely build patron-oriented information databases that enable them to provide personalized service
 - Retailers collect data to help their managers monitor the flow of products moving from manufacturing plants to warehouses, stores, and ultimately purchasers.
 - Transportation firms routinely track movement of packages,
 - Manufacturers have refined data-dependent “just-in-time” techniques to ensure that source materials reach the beginning of the production line not a day sooner or later than required



Proprietary Information

- Defined:
 - It is any type of data that the owner wishes to restrict who know about it or its contents. **(another way of saying trade secret)**
- Three dynamics at play in successful companies:
 - Knowledge has become an economic resource
 - Information technology is expanding
 - The number of people familiar with information technology is growing by leaps and bounds.

Knowledge is emerging as an economic resource



The Dynamic of Information Technology

- The use of information is in all functions and subfunctions of business are addressed in the information technology marketplace.



Competing Dynamics Use of Data v. Loss of Data

- **Common sense solutions to enhance data protection:**
 - Stay on top of the issue.
 - Keep pace with data-related technology
 - Look for countermeasures that take advantage of new techniques and leading-edge technology.
 - Maintain a frank and ongoing dialog with data managers about risk avoidance.
 - Spread the word among supervisory employees that data protection is their responsibility.





WORKPLACE VIOLENCE

2020 and Beyond



A Safe and Secure Workplace

- What is workplace violence:
 - Is the use of physical force against or by a worker that causes or could cause
 - Physical injury
 - Threatening behavior
 - Harassment
 - Veiled threats
 - Intimidation, or anger-related incidents,
 - Rape, arson, property damage, vandalism, and theft

Risk is managed through Training, Planning, Preparation



Harassment / Sexual Harassment

- **Definition of Harassment:** Harassment is unwelcome conduct that is based on race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability or genetic information. Harassment becomes unlawful where:
 - Enduring the offensive conduct becomes a condition of continued employment, or
 - The conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive. Anti-discrimination laws also prohibit harassment against individuals in retaliation for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or lawsuit under these laws; or opposing employment practices that they reasonably believe discriminate against individuals, in violation of these laws.



Harassment Workplace Policy

- Must include the Harassment definition
- Company should strong grievance and complaint process
- Companies should provide training on Harassment for employees
- Should include conduct that is considered offensive behavior:
 - Example: Offensive jokes, slurs, epithets or name calling, physical assaults or threats, intimidation, ridicule or mockery, insults or put-downs, offensive objects or pictures, and interference with work performance.



Sexual Harassment

- **Sexual harassment:** Is unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature.
- Both victim and the harasser can be either a woman or a man, and the victim and harasser can be the same sex.



The Workplace Violence Risk Assessment

- This is a targeted assessment addressing specifically workplace violence. It would look at:
 - Indicators of violence, vulnerability of specific threats, likelihood of an event, impact of specific threats
 - Creation of Threat Team (they make decisions for the company)



Workplace Violence Variables

External Variables

- Domestic violence
- Stalking
- Other aggressive behavior that enters the workplace.

Internal Variables

- Co-Worker Conflict
- Bullying
- Toxic Supervisor

Goal:

Identify threats that might pertain to a particular industry type or organization, relationships that exist between a perpetrator and an organization, or relationships that may exist between a perpetrator and a current or former employee.



How to Identify Threats

- Important Considerations:

- Are employees working alone, at a remote location or at night?
- Do employees handle cash or other valuable assets?
- Do employees work with the general public?
- Is the workplace in a high-crime area?
- Is your business targeted for terrorism, animal or human rights?
- Is this workplace known for high stress, threatening behavior?
- What physical security is currently in place? ID badges, access control, camera systems, and lighting



Components of a Workplace Violence Plan

- **Workplace Violence Prevention Plan**

- This will allow that proper resources are allocated for the development of a workplace violence prevention plan and execution of the plan. Considerations: Senior management buy in, physical security design, training

- **Threat Assessment Team**

- Includes a representative from security, legal, human resources, mental health, and employee assistance program (EAP), Union Rep if a union house, may include a local law enforcement officer.
- The team may need extra training conflict resolution, employee relations, personal security....etc.

- **Workplace Violence Prevention Policy**

- Use firm, clear, concise language
- Clearly communicated to new hires and ongoing
- Needs to be zero tolerance



Train to Identify Warning Signs

- Prior history of violence
- Domestic Situations
- Suspicious Behavior Indicators
- Mental Disorders
- Life-Changing Events
- Financial Stresses
- Obsession with other employees
- Chemical Dependence
- Increased interests in weapons
- Disgruntled Employees



Education and Training

- Training should include: Acceptable Behavior, Understanding Workplace Violence, Identification of Early Warning Signs
- Individual Responsibility is important
- Internal Notification to HR Department
- Supervisor and Manager Training:
 - De-Escalation Training
 - Behavioral Clue Recognition Training







CORPORATE POLICY AND PROCEDURE



Employee Manual

- It is recommended that every company large or small have a company-wide policy and procedure manual.
- A hotel should have company-wide policy manual in addition to its own facility manual. The facility manual is broken down by department.
- What should a policy manual include:
 - Company Policies
 - Company Procedures
 - Department Manuals
 - Employee Handbook



Security Department Manual

- A separate manual specifically for the security department is an indispensable tool for assuring that all security personnel have been given the same information regarding the purpose, functions, and procedures carried out by the department.
- **Manuals should be designed for quick reference** whenever a need arises and they should also be readily accessible.
- **Manuals need to be objective** in nature
- Three basic categories of a security manual:
 - **General Information:** include a description of the department's mission, organizational chart, dress code, and job descriptions for security personnel.
 - **Department Policy:** Objective statements that indicate the objective of the policy and any relevant procedures that the officer is expected to follow
 - **Emergency Procedures:** detailed information on the steps to be taken by security and other hotel personnel during an emergency.



Constructing Policy and Procedures

- Companies need policies and procedures for every aspect of their security operation.
- Example of security policy and procedures:
 - **Patrolling:** Check all employee areas, including locker rooms, and service areas to include the kitchens. Check all bars, restaurants, and function rooms. It is important to utilize a checkpoint in all of these areas.
 - **Lobby Patrols:** Maintain a visible presence in the lobby checking all doorways, escalators, retail shops, and so forth.
 - **Basic Patrols:** Check all guest room floors for suspicious persons, vandals, and misguided individuals. Check all fire exits, fire exit signs, lights, pipes, guest room doors, peepholes, and so forth to ensure a safe and secure environment.



Constructing Policy and Procedures

- Many areas that fall under the realm of security, and all employees need to be aware of the appropriate steps to be taken in all situations that are likely to arise. Such situations may include:
 - Dealing with employee theft
 - implementing emergency fire evacuation procedures,
 - actions to take/avoid during strikes or collective bargaining negotiations,
 - sexual harassment involving employees,
 - lost and found, dignitary protection,
 - escorting terminated employees,
 - providing first aid and CPR and Stop the Bleed program,
 - key management and access control,
 - Confidentiality procedures
 - Safety Deposit box procedures for cash handling
 - Suicide and alcohol related incidences



Security Report Writing

- A security department is an integral part of a business; therefore the security manager should think and act like a business manager.
- **Warning to companies:** Don't spend too much time trying to assimilate with law enforcement and lose sight of the fact that their departments are a vital component of the business.
- **Security Reports should include:** issues, problems, and concerns encountered by the security department.
- **Reports provide:**
 - An accurate record of the number and types of incidents it deals with, determines trends, establishes records
 - Gives insight on effectively using man power
 - Determines area of weakness and potential security violations
 - Ascertain which policies and procedures need modification, identify new areas of concern
- **Accurate report writing:** Requires names, descriptions of individuals, vehicles, buildings, surroundings, and correct dates, and times are critical



Security Record Retention

- Incident reports—Should be maintained for a period of **5 years** or based on your statutory laws.
- Records relating to pending litigation—Until final settlement and released by legal advisor.
- Records involving minors—Maintain until a minor reaches the age of majority.
- Record of General Liability claim—Maintain until final settlement and released by legal advisor, could be 16 years after actual settlement.



Conclusion

- Every security manager who assumes a position in a corporation also assumes that the corporation has a security department manual.
- if a department has been operating without a security manual, the hard part is not writing the manual, it is implementing it.
- **Every 5 years** all policies should be reviewed and updated.





INTRODUCTION TO CPTED

Crime Prevention Through Environmental Design



What is CPTED?

- **Crime Prevention Through Environmental Design**

- Rather than introducing visually unappealing safety measures such as surveillance cameras, security guards, and hard barriers (locks, fences, security gates,.), CPTED focuses on creating a visually pleasing space that encourages positive human behavior.
- It is proactive verses reactive
- It discourages criminal behavior and boost a sense of security among residents or employees



4 Basic Concepts of CPTED

Surveillance

Access Control

Territorial
Reinforcement

Maintenance

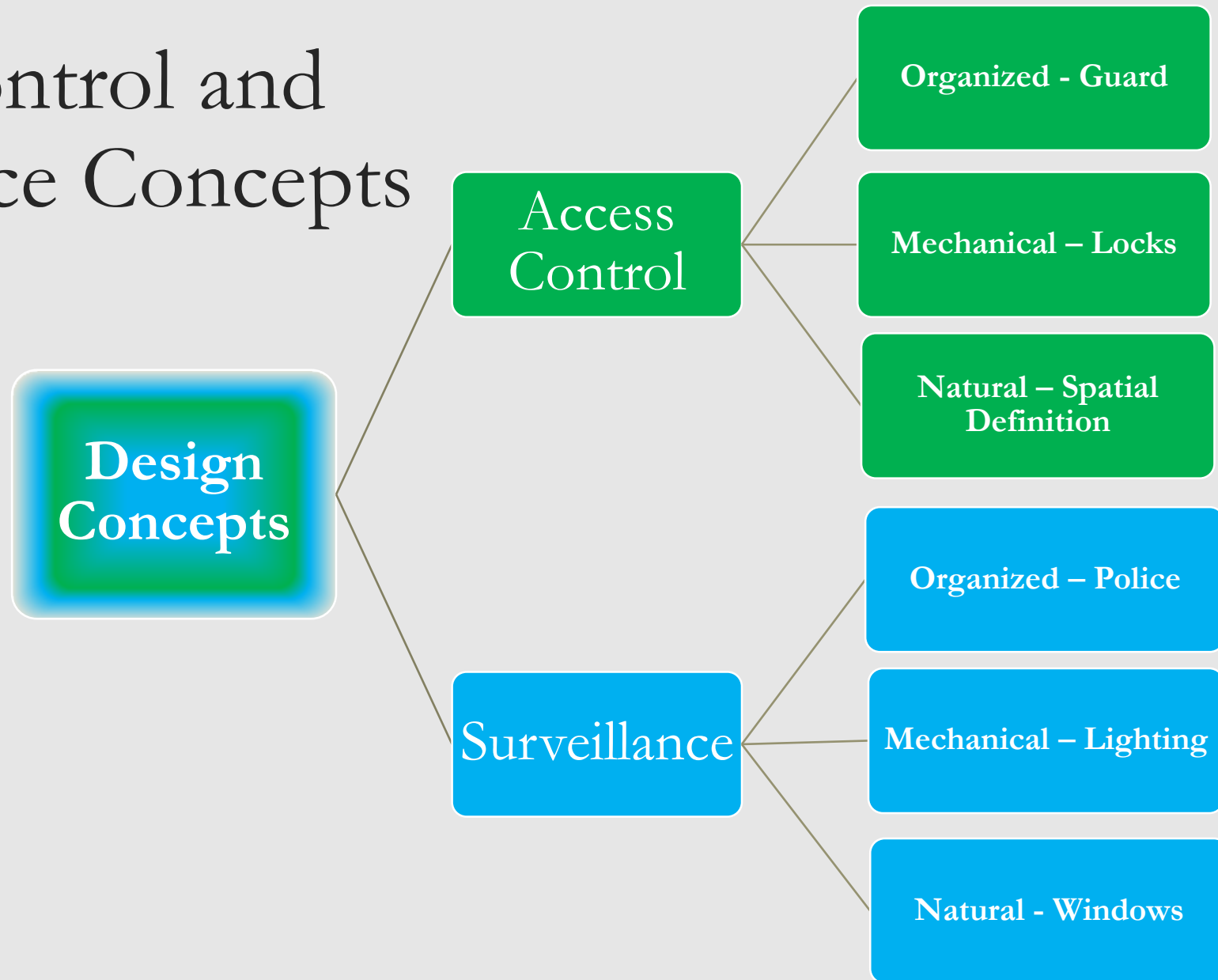


Seven Overlapping Strategies in CPTED



Seven concept of CPTED. Designed by Marianna Perry

Access Control and Surveillance Concepts





Surveillance

- **Organized:** Police Patrols, Private Security
- **Natural:** Makes a place unfavorable for illegal activities (see or be seen)
- **Mechanical:** Lighting, technology, cameras, perimeter alarms. Etc.



Good Natural Surveillance



Access Control

- **Organized:** Private Security
- **Natural:** Shrubs, trees, pathways, fences, locks, and other means.
- **Mechanical:**
 - IOT: Internet of things Ecosystem
 - Biometrics
 - RFID Access Control
 - NFC – Access Control
 - Physical Access Control
 - Power of Ethernet
 - Mobil Access Control
 - Bluetooth Access Control
 - Wired Access Control Technologies
 - Wireless Access Control Technologies

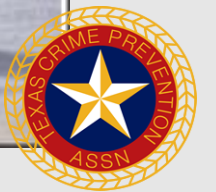


Territorial Reinforcement

- Territorial reinforcement is about establishing a clear demarcation between a business, school, or property premises and the surrounding areas.
- Two Purposes:
 1. **Sense of belonging**
 2. **Makes it difficult for intruders to blend in**



Good Territorial Reinforcement



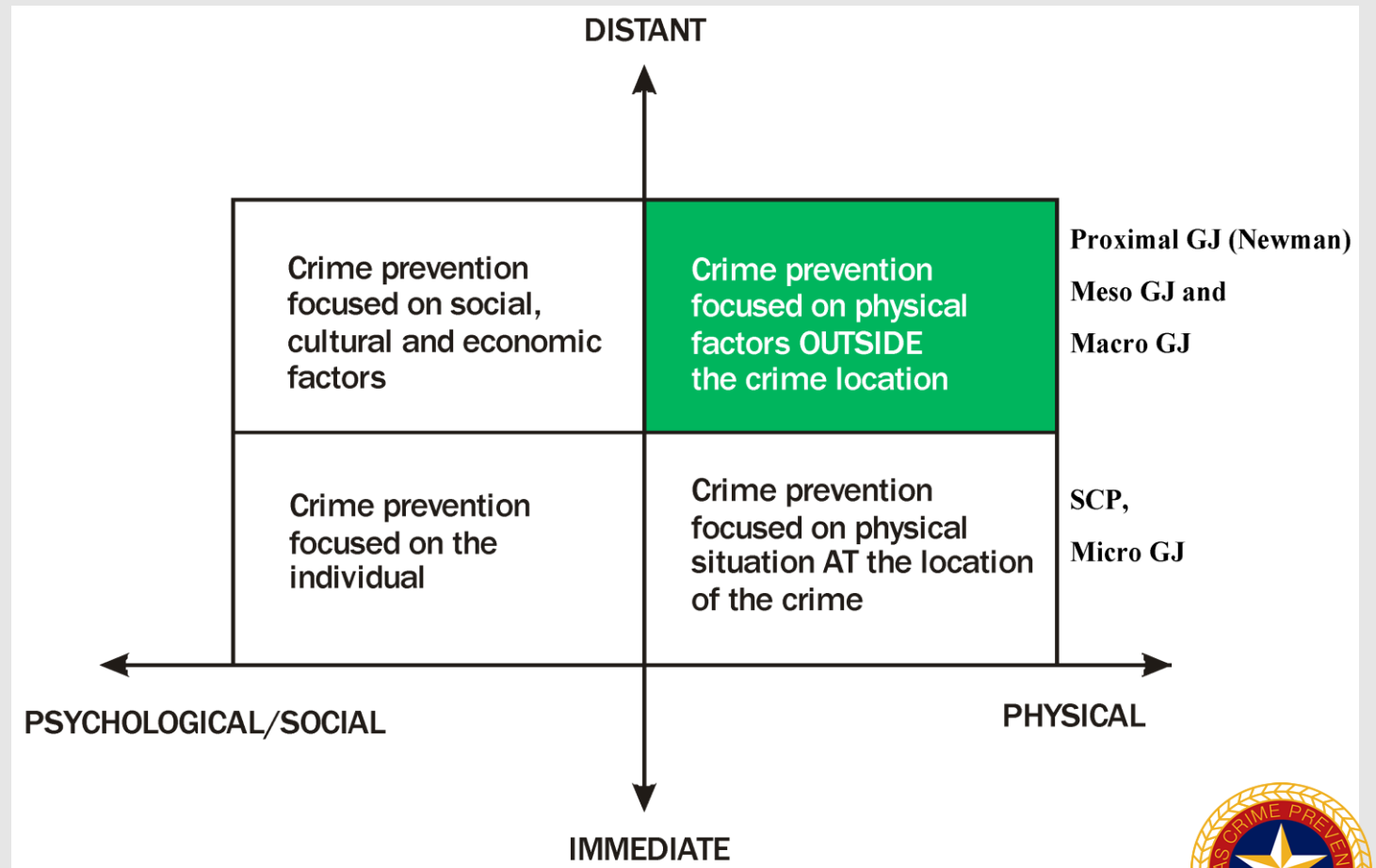
Maintenance and Management

- The more neglected an area is, the more likely it is to become a target for criminal activities.



Geographical Juxtaposition in CPTED

- Assessing the **potential influence** on crime levels, of proximal land-users that may generate crime. (Wider Environment)
- Focuses on **social and economic causes of crime** and combining those factors to the changing of the physical environment.



Three-D Approach to CPTED

- To determine which CPTED strategies are needed for a particular environment, you have to first assess the space you are evaluating. To do this the 3Ds approach is normally used.
- **Function of Space:**
 - All human space has some **DESIGNATED** purpose.
 - All human space has social, cultural, legal, or physical **DEFINITIONS** that prescribe the desired and acceptable behaviors.
 - All human space is **DESIGNED** to support and control the desired behavior.



Three-D Approach to CPTED

I. Designation

- What is the main purpose of the place?
- Was it originally built for the same purpose?
- If not, how can you change it to maximize functionality and security?



Three-D Approach to CPTED

II. Definition

- Is the place well defined, or does it merge with its surroundings instead?
- If the boundaries set it apart from the public property, is it clear who the place belongs to?
- Are the administrative aspects covered in the legal policy?



Three-D Approach to CPTED

III. Design

- Does the design and layout of the place match its intended use?
- Does the physical layout temper with the security measures you have put in place?
- If the answer to the above two questions is no, which of the four principles of CPTED, do you need to work upon the most?





TCPA SURVEY REPORT

Completing the Report (Practical Exercise)



Project Overview

- Break into Groups
- Select a Secretary
- Break the report down in your group and have one person complete a section. The secretary will then put the report into a final document.
- Each person will give a presentation on Friday over their section of the report.
- Report breakdown
 - Section I & II
 - Section III
 - Section IV
 - Section V
 - Section VI





SURVEILLANCE

Lighting, Sight Lines, Windows & Glass, Technology



Commercial Lighting

From a business perspective, lighting can be justified because it improves sales by making a business and merchandise more attractive, promotes safety and prevents lawsuits, improves employee morale and productivity, and enhances the value of real estate.



Commercial Lighting & Security

- Two Perspectives on Commercial Lighting
 - **Business:** improves sales by making a business and merchandise more attractive, promotes safety and prevents lawsuits, improves employee morale and productivity, and enhances the value of real estate
 - **Security:** two major purposes of lighting are to create a psychological deterrent to intrusion and to enable detection.



Lighting Levels

- What lighting level aids an intruder?
- Three Levels of Light
 - Bright Light
 - Dim Light
 - Darkness



Illumination

- Lumens (of light output) per watt (of power input) is a measure of lamp efficiency (rating is based when the light is new)
- Illuminance is the intensity of light falling on a surface, which is measured in foot-candles. (foot-candle is a measure of how bright the light is when it reaches one foot from the source)
- Sun light on a clear day is about 10,000 fc
- Overcast Days is about 100 fc
- Full Moon .01 fc



Outdoor Lighting Recommendations

- Illuminating Engineering Society of North America are as follows:
 - Self-parking area, 1 fc
 - Attendant parking area, 0.20 - .90 fc
 - Covered parking area, 5 fc
 - Active pedestrian entrance, 5 fc
 - Buildings and surroundings, 1 fc.
 - Gates and Doors, at least 2 fc,
 - Office Space should have a light level of about 50 fc.



Are the Foot-Candles Horizontal or Vertical?

- A good understanding of the photometrics can assist with understanding what levels of light are needed in order for natural and/or technical surveillance is needed (4:1).
 - **Horizontal Illuminance** – is the amount of light that lands on a horizontal surface, such as a tabletop
 - **Vertical Illuminance** - is the amount of light that lands on a vertical surface, such as a wall.



Review the Types of Lamps

- **Incandescent** - Passing electrical current through a tungsten wire that becomes white and hot produces light, least efficient and expensive. Good Color Rendition
- **Halogen and Quartz Halogen Lamps** - Incandescent bulbs filled with halogen gas. 25% better efficiency and life than ordinary incandescent bulbs.
- **Fluorescent Lamps** - Passing electricity through a gas enclosed in a glass tube to produce light. They are not used extensively outdoors, except for signs. Good Color Rendition
- **Mercury Vapor Lamps** - They also pass electricity through a gas. Maybe illegal to use in some states



Review Types of Lamps

- **Metal halide lamps** - They are also of the gaseous type. They are often used at sports stadiums because they imitate daylight conditions and colors appear natural. Most expensive light to install and maintain. Slow restrike time (10-15 minutes) (Good Color rendition 60-90 out of 100)
- **High-pressure sodium lamps** - These are gaseous. These lamps are often applied on streets and parking lots and are designed to allow the eyes to see more detail at greater distances through the fog. (Poor Color Rendition 21 out of 100)
- **Low-pressure sodium lamps** – They are also gaseous. Long life span expensive to maintain. Slow restrike time (7 -15 minutes) with a color rendering index that is around 0 out of 100. Poor Color Rendition



Review Types of Lighting

- **LED (light emitting diodes)** - This type of lighting is becoming more and more popular. low energy consumption and are long lasting up to 50,000-80,000 hours. Used in garages, street lighting, and rear taillights in motor vehicles. Instant restrike, excellent color rendition.
- **Quartz lamps** - These lamps emit a very bright light and snap on almost as rapidly as incandescent bulb. They have a very high wattage. Excellent for perimeter use and troublesome areas.
- **Electroluminescent lights** - These lights are similar to their fluorescent cousins; however, they do not contain mercury and are more compact.



The Good and Bad of Different Lamps

- Incandescent, fluorescent, and halogen lamps provide an excellent CRI of 100%
- Preferred outdoor lamp for camera systems is metal halide.
- Low-pressure sodium lamps, which are used extensively outdoors, provide poor color rendition, making things look yellow. Low-pressure sodium lamps make color unrecognizable and produce a yellow-gray color on objects.
- Mercury vapor, metal halide, and high-pressure sodium take several minutes to produce full light output if turned off.
- Incandescent, halogen, and quartz halogen have the advantage of instant light once the electricity is turned on.
- LED gives instant light with no warmup. It also provides excellent color rendition.



Industrial Lighting Systems

- Industrial security consists of the following:
 - Perimeter Lighting
 - Area Lighting
 - Flood Lighting



Seven Basic Types of Protective Lighting

- **Continuous Lighting** - fixed and the most common type of lighting where lights are installed in a series to maintain uniform lighting during hours of darkness.
- **Standby Lighting** - turns on with alarm activation or when suspicious activity is suspected.
- **Moveable Lighting** - manually operated search lights.
- **Emergency Lighting** - can duplicate other lighting systems in the event of an emergency.
- **Controlled Lighting** - used outside a perimeter to illuminate a limited space.
- **Area Lighting** - used in open areas and parking lots.
- **Surface Lighting** - used on the surface of structures and buildings.



Perimeter Lighting



- **Perimeter lighting** is used to illuminate the property **line or fence itself and an area beyond** (i.e., the detection zone).
- **What is the objective of Perimeter Lighting?**
 - It is to reveal an intruder's approach and produce glare toward him, thus reducing visibility into the site.



Illumination and Glare

- **Illumination intensity** - as light bulbs age, the light that they emit out decreases.
- **Illumination distribution** - lighting fixtures have to be spaced correctly so that there is no area without proper illumination.
- **Illumination quality** - color perception may or may not be important.
- **Illumination reliability** - may be problem if the lights are vulnerable to physical attack or vandalism.



Lighting and the Intensity

- **General Rule of Lighting:** “at night, outside of a building or at a parking lot, one should be able to read a driver’s license or newspaper with some eyestrain” (Purpura, 1979).



Cost and Return on Investment

3 Categories of Cost

- Energy Cost (88%)
- Capital Cost (8%)
- Maintenance Cost (2%)

Categories on Investment Return

- Efficiency and Energy Saving
- Reduce cost by shutting off unnecessary units
- Concept of going green



Strategies for Good Exterior Lighting

1. Locate perimeter lighting to allow illumination of both sides of the barrier.
2. Direct lights down and away from a facility to create glare for an intruder. (Overlapping Illumination)
3. Do not leave dark spaces between lighted areas for burglars to move in. Design lighting to permit overlapping illumination.
4. Protect the lighting system.
 - Locate lighting inside the barrier, install protective covers over lamps, mount lamps on high poles, bury power lines, and protect switch boxes.



Strategies for Good Exterior Lighting

5. Photoelectric cells enable light to go on and off automatically in response to natural light. Manual operation is helpful as a backup.
6. Consider motion-activated lighting for external and internal areas.
7. If lighting is required in the vicinity of navigable waters, contact the US Coast Guard.
8. Try not to disturb neighbors by intense lighting. Some local laws govern light pollution or support a “dark sky initiative.”



Strategies for Good Exterior Lighting

9. Maintain a supply of portable, emergency lights, and auxiliary power in the event of a power failure.
10. If necessary, join other business owners to petition local government to install improved street lighting.



Interior Commercial Lighting

- Most Effective Interior Lighting is LED
 - **Design and Fashion**
 - **Reduce Cost**
- After Hours Burglary Prevention



Lighting Check List

1. Is all of the perimeters lighted?
2. Is there a strip of light on both sides of the fence line?
3. Is the illumination sufficient to detect human movement easily at 100 yards?
4. Are lights checked for operation daily prior to darkness?
5. Is extra lighting available at entry points and points of possible intrusion?



Lighting Check List

6. Are lighting repairs made promptly?
7. Is the power supply for lights easily accessible (for tampering)?
8. Are lighting circuit drawings available to facilitate quick repairs?
9. Are switches and controls
 - a. protected?
 - b. weatherproof and tamper resistant?
 - c. accessible to security personnel?
 - d. inaccessible from outside the perimeter barrier?
 - e. equipped with centrally located master switch(es)?



Lighting Check List

10. Is the illumination good for guards on all routes inside the perimeter?
11. Are the materials and equipment in receiving, shipping, and storage areas adequately lighted?
12. Are bodies of water on perimeter adequately lighted?
13. Is an auxiliary source of power available for protective lighting?



Commercial Sight Lines

Sight line is defined as the desired line of vision in terms of both breath and depth. The inability to see what is ahead along a route due to sharp corners, walls, earth berms, fences, bushes or pillars can be serious impediments to the feeling of being safe.



3 Considerations for Commercial Sight Lines

- **Design Visibility** - Design visibility in the built environment means allowing for clear sight lines and avoiding isolated or hidden spaces.
- **Problematic Spaces** - Visibility should especially be considered when designing or planning spaces where risk to personal safety is perceived to be high (i.e. stairways, multi story car garages, or lobby entrances to buildings)
- **Future Sight Line Impediments** - As the landscape matures over time, unintended screens, barriers or hiding places could be created.



Sight Lines



Landscaping and Site Lines

- When installing new or replacing plants consideration needs to be given to the mature size
- Plants may cover walls and open spaces eliminating space deterring graffiti
- Provide landscape and fencing that does not create hiding places.
- Use Transparent, rather than opaque fencing (tubular steel, wrought iron)
- Utilize spacing to maintain visibility and don't forget the 3 and 7 rule for shrubs and trees
- In commercial properties plants should at least 30'' from the building unless it is a vine growing on the wall.
- Consider shape and size of trees. Trees should not be planted within 10' feet of light poles.





What do you see?

Tree Spacing

Hedges

Light Poles

Windows

Overall Design



Public Spaces and Sight Lines Considerations

- Public Space around buildings needs to promote a safe environment
- Avoid low walls, planters, and water features that encourages transient use
- Avoid dark or hidden areas near high activity areas on property
- Ensure proper lighting
- Restrict Use of covered outdoor areas
- Use single seating furnishing and small tables to discourage sleeping



Commercial Windows & Glass

Windows are encompassed in the concept of Sight Lines.

Windows provide the ability to:

- See Out – Observe Behavior
- See In – Plus and Minus
- Let Sunlight In
- Provide Ventilation



Commercial Windows Types and Use

- Weather ability
- Durability
- Thermal performance
- Triple-insulating glass
- Thermal barriers
- Solar windows



The Cardinal Direction of Windows

- **North facing** – adds light with little heat gain
 - Generally little heat gain
 - Minimum Glare
- **South facing** – most advantageous for day lighting
 - Winter Sunlight in
 - Moderates Seasonal Temperatures
- **East / West facing**
 - Morning / evening heat gain
 - Adds glare
 - Little Contribution to Solar heating in winter



Considerations in Commercial Windows

- Inside looking out
 - Allows viewing of possible intruders, weather, etc....
 - Good line of sight increases reaction if needed.
- Outside looking in
 - Legitimate viewers can see potential problems before entry
 - Illegitimate viewers can see persons / property



5 Types of Glass Used in Commercial Windows

- **Laminated glass.** This is a type of safety glass that contains polyvinyl butyral or a similar substance and therefore holds together when shattered. It comes in high-performance laminated glass for structurally efficient glazing
- **Sheet glass.** This is least expensive and most vulnerable to breakage, with a thickness of typically 34 mm.
- **Float glass/annealed glass.** It has the quality of plate glass combined with the lower production cost associated with sheet glass manufacturing and is virtually distortion and defect free.
- **Tempered glass.** Tempered glass is the most widely used commercial glass and is often required by law.
- **Bullet-resistant glass.** It is constructed using a strong, transparent material such as polycarbonate thermoplastic or by using layers of laminated glass.



Glass and Security

- **How do they work together?**
 - You may recommend a **glass security barrier** at a convenient store or bank.
 - Install a glass door in an office so a receptionist can see who approaches.
 - This is the concept of “**See and be seen**”.



Window Glazing

- **Glazing:** Glazing refers to the number of glass panes that make up the window.
 - Single
 - Double
 - Triple and Higher glazes
- Glass is the most popular and the traditional material used for glazing.
- Glazing may also be done with plastic sheeting (acrylic or polycarbonate)



Factors to be considered in commercial Windows

Type & Size

- Energy efficiency and quality of the unit
- Amount of sunlight, ventilation, and visibility
- Material and desired finish:
 - Wood
 - Metal, aluminum, and stainless steel
 - Finish color and “green” products

Window Hardware

- The effectiveness of weather stripping and wind pressure, explosion blasts, and fire
- To prevent access, and the cost to replace if vandalized
- Glass type
 - Plate glass, sheet glass, float glass, annealed glass, tempered glass, laminated, wired etc..



Tinting of Glass Windows

- Tinted glass is made by altering the chemical formulation of the glass with special inorganic additives.
- The color is durable and does not change over time.
- Tinted glazing is more common in commercial windows than in residential windows.
- In retrofit situations tinted plastic film may be applied to the inside surface of the glazing.



Bullet- Resistant Materials

- Bullet-resistant glass comes in acrylic, polycarbonate, and glass-clad polycarbonate
- Providing protection against guns ranging from a 9 mm to a 12 gauge
- Used in banks, credit unions, gas stations, and convenience stores
 - Interior/ exterior transaction windows,
 - Bulletproof doors, ballistic counters,
 - Package passers,
 - Bullet-resistant barriers and framing, bullet-resistant transparencies and fiberglass.



Bullet-Resistant Fiberglass Walls / Doors

- These are used to provide bullet-resistant protection to the walls of corporate executive offices, boardrooms, conference rooms, lobbies, reception area counters, customer service counters, and safe rooms.
- Bullet-resistant doors to meet different needs, for example, solid executive-style veneered doors to match existing doors but with bullet-resistant protection.



Window Film / Bullet Resistant Glass

- Window film is not bulletproof, and there is no film product out there that is.
- Window film can be resistant to small arms and shotguns
- Lumar window film products have a bomb blast proof film product.
- Four Categories of Window Film
 - **Security or safety film** - retail, commercial, and residential buildings and other types of window structures from the damages of flying glass due to earthquakes, windstorms, attacks, vandalism, theft, and accidents.
 - **Decorative film** - allows you to customize your space with a corporate logo
 - **Anti graffiti window film** - prevent scribbling or other defacing a base surface
 - **Solar film** - it reflects and absorbs heat and light, and it increases energy efficiency,



Window Views and Surveillance

- **Surveillance is the principal weapon in the protection of defensible space**
 - Criminals least likely to go to high visibility areas
 - Legitimate users can observe and report criminal acts



Basic Window Guidelines

- **Provide two-way visibility to areas open to public**
 - Convenience Stores, check cashing, etc
- **Provide one-way visibility to areas closed to public**
 - Private residences, office buildings, etc.
- **Careful selection of the types of glass, coatings, and window coverings can be cost-effective when implement or improve these guidelines**



Basic Window Guidelines

- **Where two-way visibility is desired, proper initial design is critical**
 - Place windows and glass doors where public needs to see and be seen
 - Be careful **NOT** to place windows in non-public areas, such as storerooms, office or cash counting area, etc.
 - Carefully select appropriate type of window for the location being built



Basic Window Guidelines

- **Where two-way visibility is desired, train legitimate users to not restrict that visibility**
 - Cover less than $\frac{1}{4}$ **inch** of the window with signs, etc
 - Don't place signs or coverings at eye-level
 - Turn display shelves perpendicular to windows
 - Don't place anything that restricts clerks view of outside
 - Don't place anything that restricts customers view of clerk



Basic Window Guidelines

- **Where one-way visibility is desired, proper initial design is equally critical here also**
 - Carefully select appropriate window types for the location and application
 - Carefully select types of window coverings (drapes, blinds, etc.)
 - Place windows facing critical areas (walks, yards, etc.)
 - Select proper landscaping for each window location



Basic Windows Guidelines

- **Where one-way visibility is desired, properly train legitimate users to optimize options**
 - Teach them not to open blinds, curtains, etc. at night nor even on overcast days
 - Signs may be used to inform public, even without revealing the “real” motive
 - Teach them to be observant and report suspicious behavior
 - Teach owner/user to properly maintain area



Basic Window Guidelines

- Keep windows locked when closed
- If alarmed, place alarm contact points on all windows
- Don't place objects in or around window that blocks views
- Place a secondary lock on all windows on all floors
- Keep outside plants trimmed 6" below bottom of window
- Keep trees limbs trimmed at least 7' from the ground
- Use appropriate lighting
- Be careful of the types of fences and their locations



Basic Window Guidelines

- **Two Security Concerns**
 - Any opening of more than 9” square
 - Any opening less than 18’ from the ground is a security concern





VIDEO SURVEILLANCE

In the 21st Century



History of Video Surveillance

1942 - CCTV was used to view the launch of V2 rockets in Germany

1947 - US, commercial surveillance applications began around

1957 - General Precision Labs, provided CCTV camera systems for education, medical and industrial applications.



The 1970's: Video Surveillance

- Sony sold the first commercially available video cassette recorders (VCRs) in 1971. The VCR eventually paired with CCTV allowed users to record remote surveillance for later viewing
- Banks and retailers installed CCTV with VCRs to prevent theft.
- The charge-coupled device (CCD) enters the picture in 1976
- Using microchip technology, it made it possible to create cameras with more pixels to produce higher quality images in low-light situations and provide 24/7 video surveillance.



Continuing Evolution of Technology

- **Axis introduced the first IP cameras in 1996.**
 - Ethernet network for communication rather than coax cable.
 - Video signals were now sent as digital encoded signals instead of analog signals.
- **The first IP cameras provided 4CIF (704 x 480 pixels) or VGA (640 x 480 pixel) resolution.**
- **One of the first megapixel IP cameras was introduced in 2002 by IQinvision.**
 - This 1.3 megapixel (1280 x 1024 pixels) cameras provided over four times the resolution of old VGA cameras
- **By 2014 there were more IP cameras sold than analog surveillance cameras.**
- **Today, it is estimated that over 30 million surveillance cameras are used in just the United States**



Split Market

Consumer Cameras

- 2011 - Lower cost cameras were introduced by large Chinese camera companies such as Hikvision and Dahua.
- Dramatic increase in home IP surveillance systems.
- Ease of installation have made it possible for large organizations to self-install instead of relying on CCTV installers

High Performance Professional Cameras

- IP cameras were introduced for the professional security market.
- Ultra-high resolution cameras (better low light, long range lens)
- 2015 very high resolution 4K cameras were introduced
- IP cameras that provide at least 4,000 horizontal pixels, are considered 4K,



What it is an IP Camera?

- An Internet Protocol camera, or IP camera, is a type of digital video camera that receives control data and sends image data via an IP network.





IP Camera System

Two Types:

- Internet Protocol
- DVR with web server technology



Business Considerations for IP Cameras

◦ **Camera Considerations:**

- HD video,
- Long-range surveillance,
- Pan Tilt Zoom (PTZ),
- Time-lapse video
- Thermal imaging

◦ **Companies still need to think about:**

- video review and analysis,
- system maintenance,
- and surveillance services.

Companies rely on video surveillance to enhance security, improve processes, and watch the business after hours.



Advantages of an IP Camera System

- Produce high resolution images
- Minimum image resolution of 640 x 480 pixels.
- Screen resolution can be increased to high definition or HD quality with a 30 frames per minute rate
- Easy to use and can be repositioned anywhere the property requires so long as an IP network is available.
- Large commercial and residential properties to take advantage of the scalability these security cameras provide
- Remote viewing options
- Real time viewing on multiple devices





CCTV

- Records video footage and then transmits that footage to a video storage unit known as a Digital Video Recorder
- Is comprised of a cable, typically an RG-59 coaxial cable or a CAT5 ethernet cable.
- Maybe Wireless using Wi-Fi and be non-IP security camera system



- Person
- Vehicle
- Unknown Object
- Transient Object
- Anything



- Tripwire
- Multi-line Tripwire
- Partial View
- Full View
- Scene Change

Benefits of Video Surveillance in the 21st Century

- Accurate Intelligence
- Better evidence in court
- High Quality video at the point of capture
- Real Time monitoring



Video Quality a Guide for Emergency Response (Government Sector)

- A video system must deliver video to the end users in such a way that they are able to accurately recognize objects and acts based on what they see.
 - **Use Case:** It is a set of functional requirements based on the content of the observed scene and the task being performed by an end user.
 - **Use Classes: Represent combinations of shared features across various use cases**



Use Cases and Use Classes Work Together

Five questions about a particular use case, to determine which general use class applies:

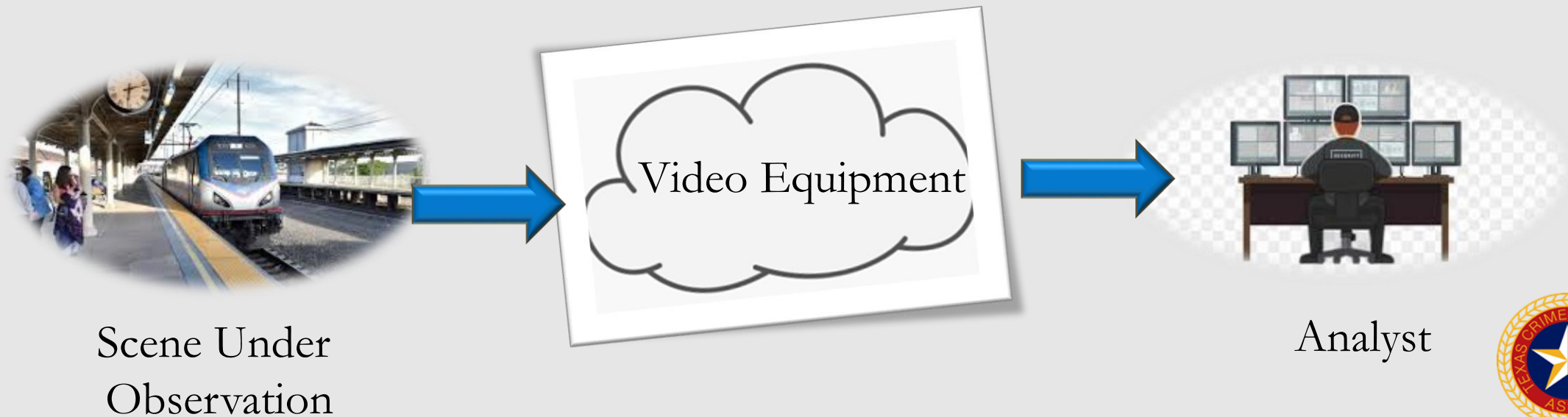
- 1. Discrimination Level** - What is the end user's ultimate goal?
- 2. Target Size** - How much of the frame does the object or person of interest occupy?
- 3. Motion** - How much motion (either target or camera) and how much spatial detail are in the video
- 4. Usage Timeframe** - Is the video used for real-time applications or recorded for later use?
- 5. Lighting Level** - Is the lighting generally uniform, or are there near-black to daylight ranges in the video frame?



The Use Case

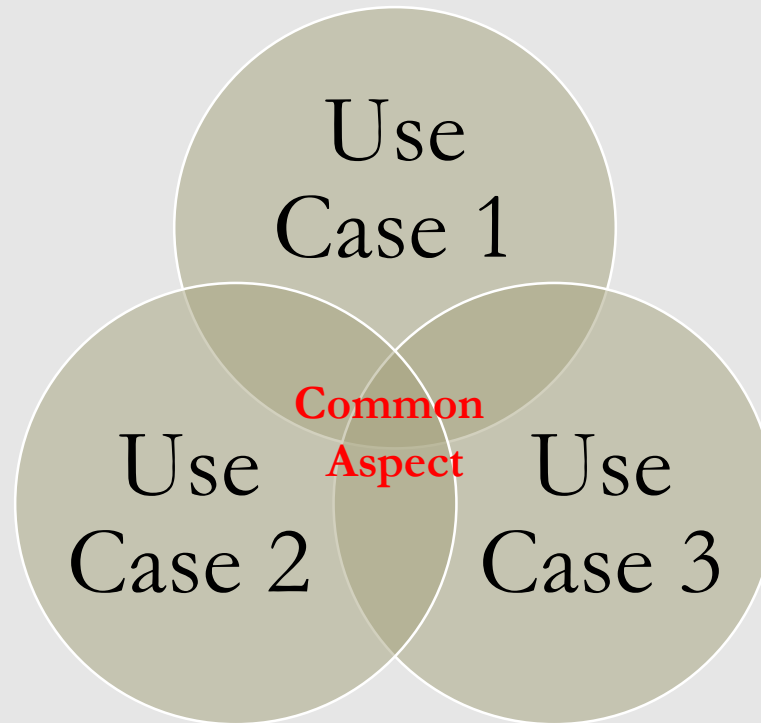
◦ 2 Main Questions

- What is in the scene of interest, or scene content?
- What is the desired task to be accomplished from viewing that scene?



Generalized Use Class

- The fundamental premise is that use cases for seemingly different applications have similar quality requirements. Thus seemingly disparate video applications may have the same minimum requirements to perform a desired recognition task.



Generalized Use Class Aspects

- **Use Characteristics**

1. **Discrimination Level** - Video may be used to identify a wide range of detail, from motion detection to positive identification of a person for forensic evidence.
2. **Usage Time Frame** - To what level of discrimination does the user need to recognize the target?
 - **General Elements of the Action**
 - **Requires large-scale recognition**, such as the distinction between a car and a van,
 - **Target Characteristics** indicates the need to recognize gender and markings, and distinguish smaller actions,
 - **Target Positive ID** indicates the most specific discrimination level.



Generalized Use of Class Aspects

- **Scene Content**

3. **Target Size** - The size of the region of interest (target) with respect to the size of the field of view directly affects the ability to recognize that target when the camera is at its maximum optical zoom.



Large Target



Small Target



Generalized Use of Class Aspects

4. **Motion in the scene** - Motion can come from the target (e.g., a car driving by), the background (e.g., a large crowd), or from the camera itself moving (e.g., a dash-mounted camera in a police car)



Generalized Use of Class Aspects

5. **Lighting Levels** - Lighting levels can vary from very dark (e.g., nighttime or indoors) to very bright (e.g., daylight or spotlight), affecting the ability of the camera to capture the image.



Live/Real Time
Or
Recorded

Choose Usage
Time Frame

Choose Target
Size

Large or Small

High
or Low

Choose Motion

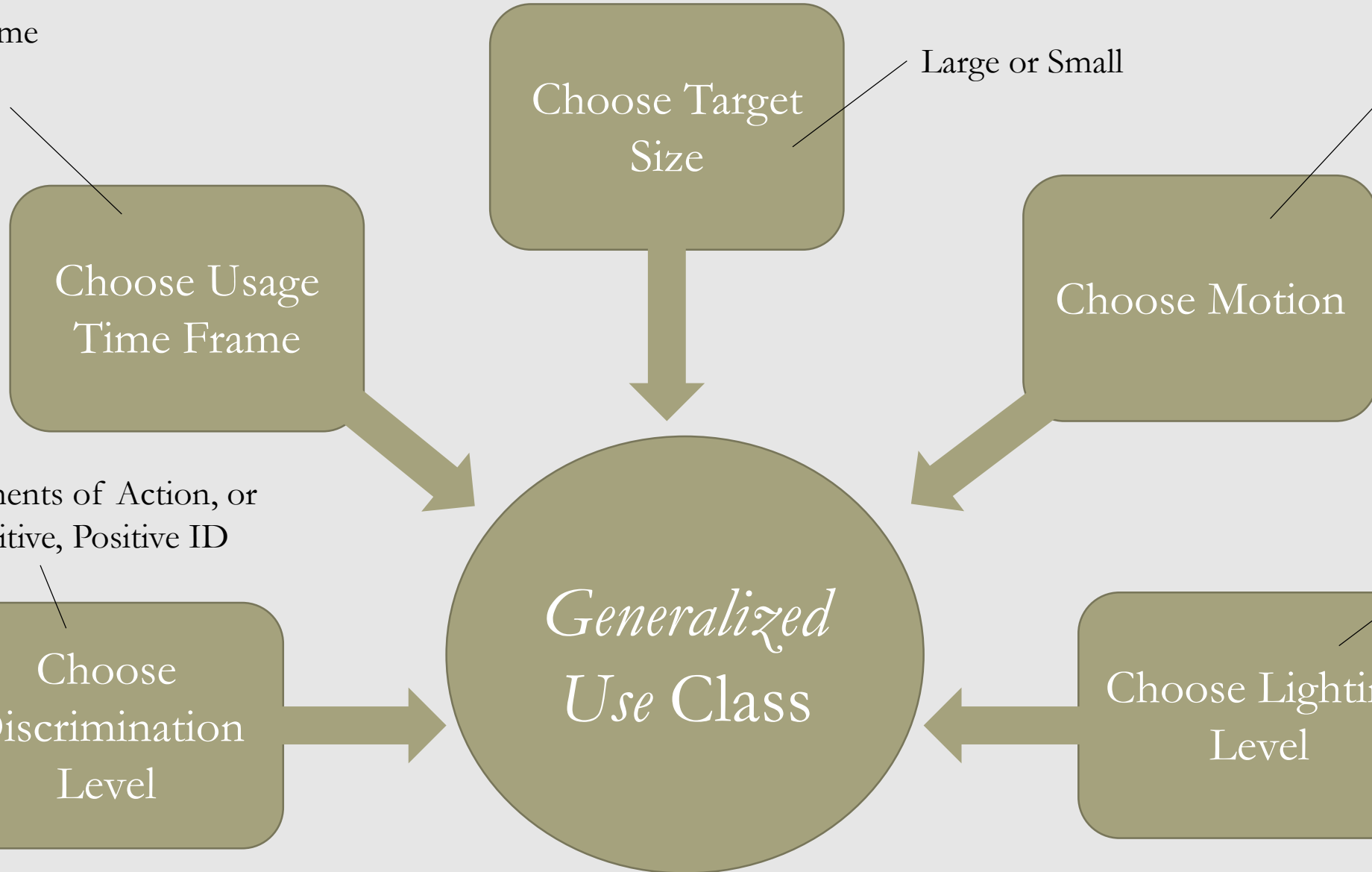
General Elements of Action, or
Target Positive, Positive ID

Choose
Discrimination
Level

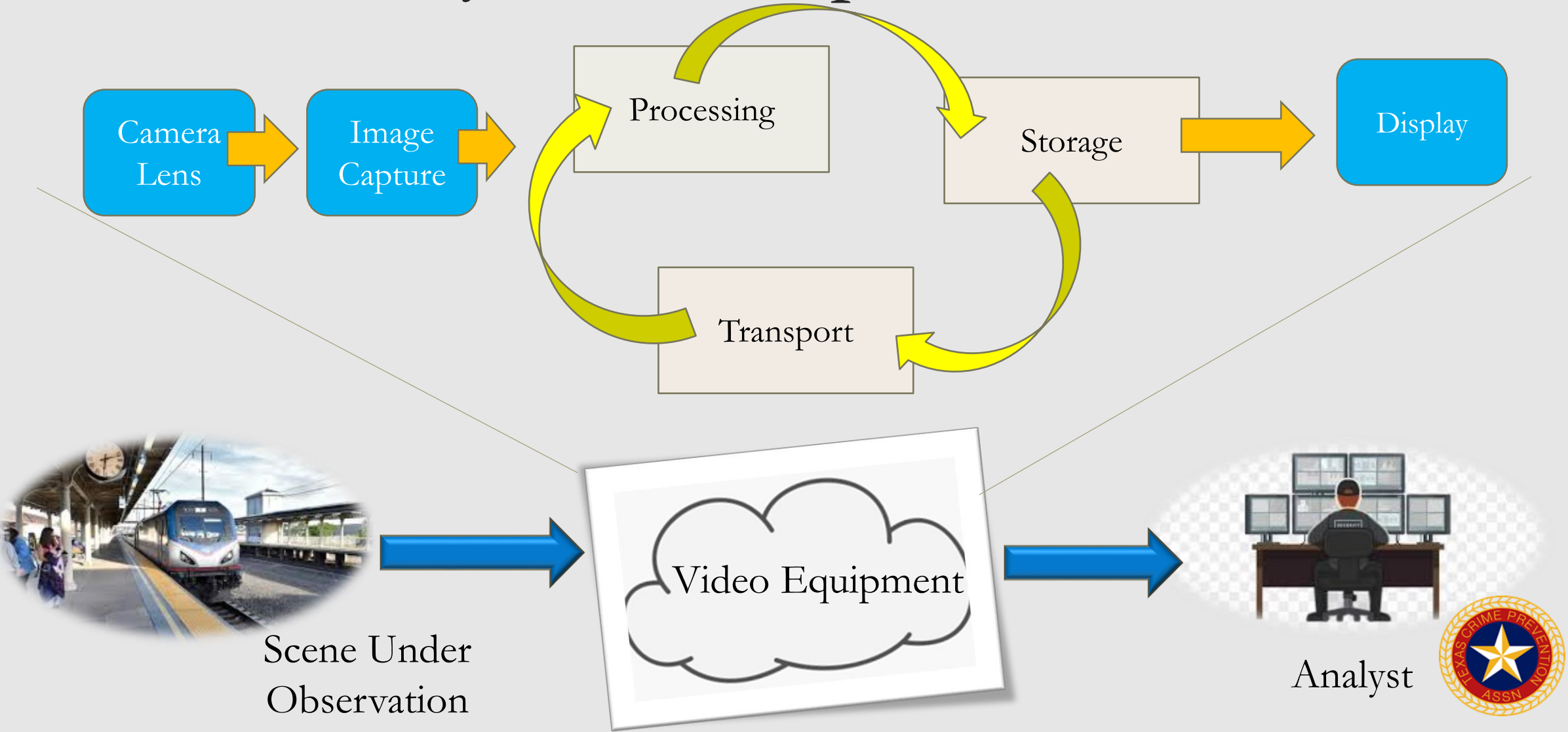
*Generalized
Use Class*

Bright
Dim
Variable

Choose Lighting
Level



Core Video System Components



The Lens

- The optical component of a camera system is a lens or series of lenses used to create an image on some sort of media, such as photographic film or electronic means.
- **Attributes**
 - **Lens Aberration** - Lenses do not form perfect images; there is always some degree of distortion or aberration introduced by the lens
 - **Field of View*** - Extent of the observable world that is seen at any given moment through the lens.
 - **Focal Length*** - Determines the field of view, and the apparent size of the objects relative to the image size.
 - **Aperture*** - Relates to lens opening to reduce or increase light that reaches the image capture surface. Controls the brightness of the image and the fastest shutter speed usable.
 - **Depth of Field*** - The range of distances that appear acceptably sharp in the image.



Image Capture

- Image capture is the process of recording data, such as an image or video sequence.
- **Attributes**
 - Resolution at which it captures
 - Frame rate at which it captures
 - Fidelity of the colors used
 - Dynamic range of the recording medium
 - Number of bits per pixel (digital cameras)
 - Noise (analog cameras)
 - Infrared capability of image capture system



Processing, Storage, Transport

- **Processing:** Processing refers to any enhancement, restoration, or other operation that is performed on a video signal
 - Compression, Digitization, Enhancement, Delay
- **Transport:** refers to the effects of moving or copying from one location to another.
 - Available Bandwidth, Loss of Data, Delay
- **Storage Description:** Video can be used for real-time (e.g., monitoring or tactical) applications or stored for future analysis
 - Physical degrading of storage media over time (e.g., tapes stretching, breaking, or being exposed to magnetic fields)
 - Physical custody of the media



Display

- To present a true quality picture of video footage captured, the emergency response community depends on a good quality image display unit to aid in accurately communicating information to the end users.
- **Attributes:**
 - "Trueness" of the colors displayed
 - Aspect ratio used





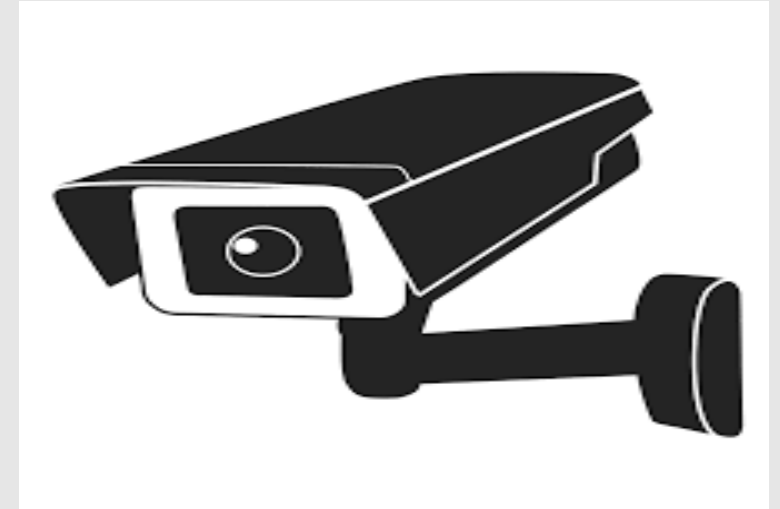
SECURITY CAMERAS

Image Resolution, Frame Rate, and Field of View



Security Camera Overview

- **Digital Camera & Analog Camera with digital codec converters**
- **What is a Codec Converter?**
 - A codec is a device that converts analog to digital.
 - Types of Codec following categories
 - Number of Channels: Single or Multiple-Channel
 - Number of Video Streams: One or two streams
 - Audio/No Audio: Audio Will have its own channel
 - Input and Output contacts: Dry-contact inputs & outputs
 - Compression Schemes: How video is compressed



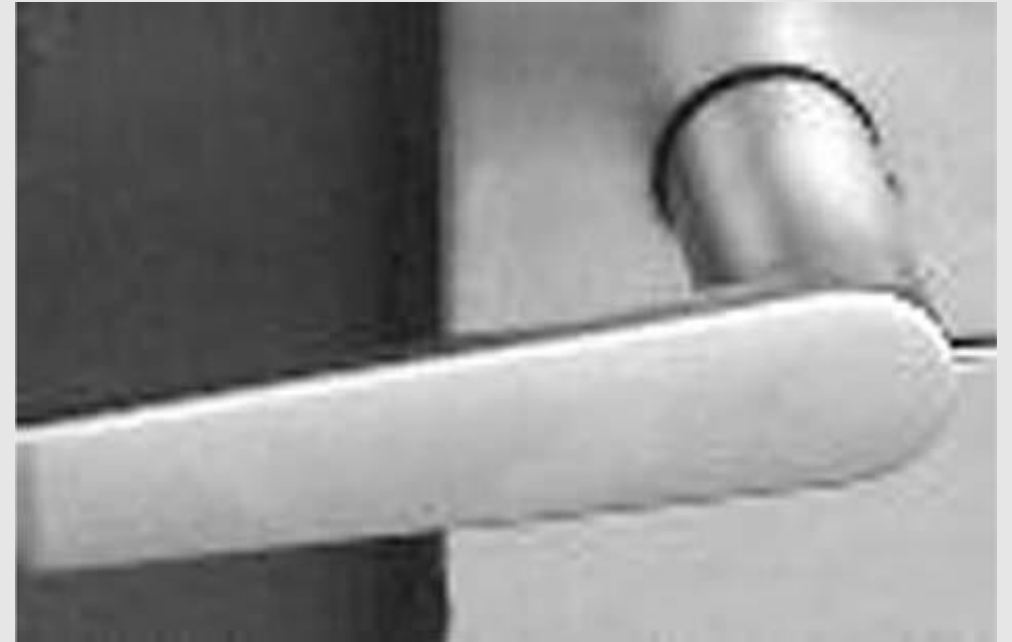
Picture Compression

- **JPEG:** series of fixed images, strung together like a movie.
- **MPEG:** is a similar group that from its inception created compression algorithms specifically meant for moving pictures.
 - MPEG-1 was the earliest format and produced video CDs and MP3 audio.
 - MPEG-2 is the standard on which digital television set-top boxes and DVDs are based. This is very high-quality video.
 - MPEG-3 (MP3) is an audio codec.
 - MPEG-4 is the standard for multimedia for the fixed and mobile web.
 - MPEG-7 and MPEG-21 also exist but are for future projects.



Picture Resolution

- **JPEG Resolution:**
 - is measured in pixels per inch.
 - Ideally, you should be displaying 1 pixel of video image onto each pixel on the video monitor
 - If you display a JPEG image at a greater size on paper or screen than its native resolution, you will see a very fuzzy image
 - Common JPEG sizes 120 x 160 to 720 x 480

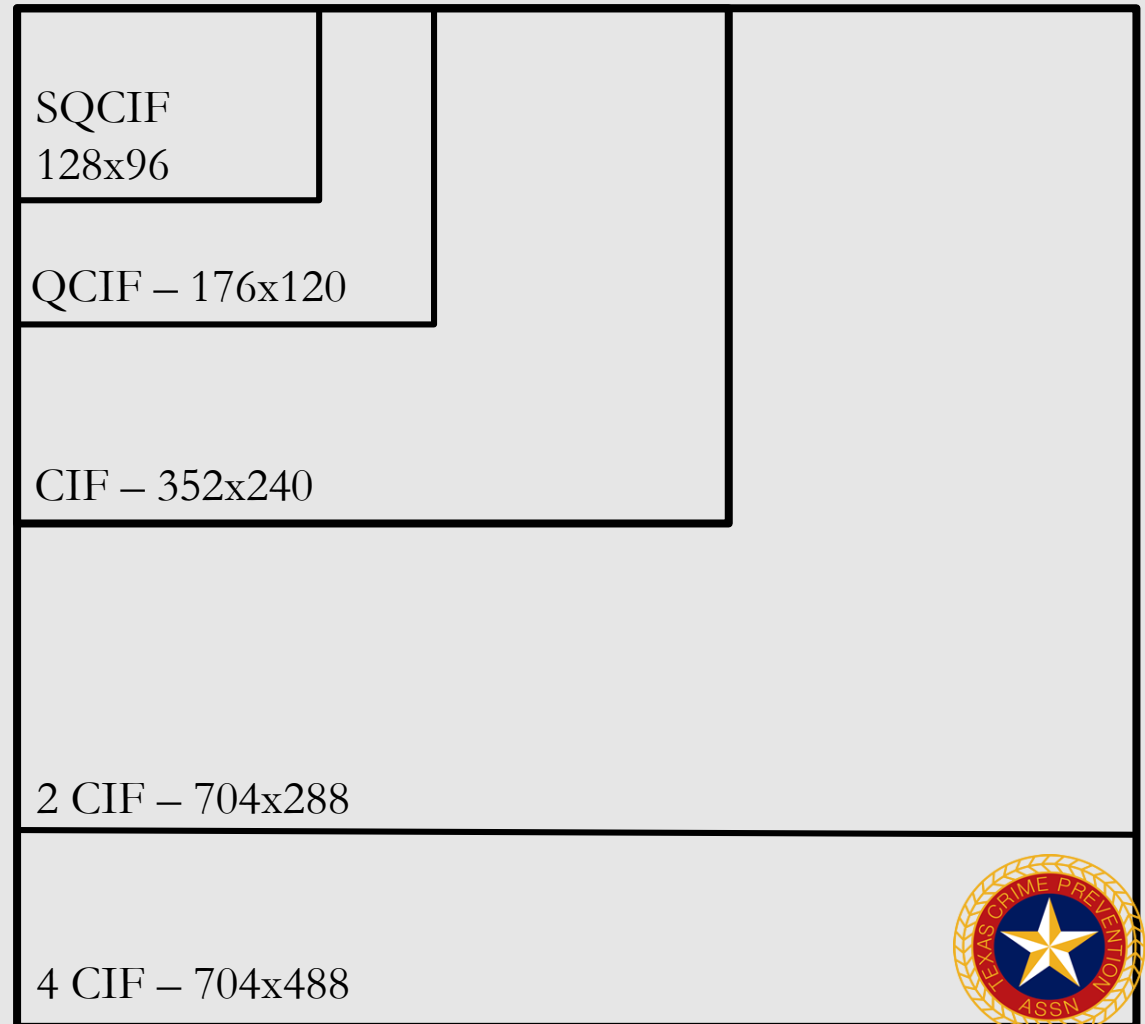


Fuzzy JPEG

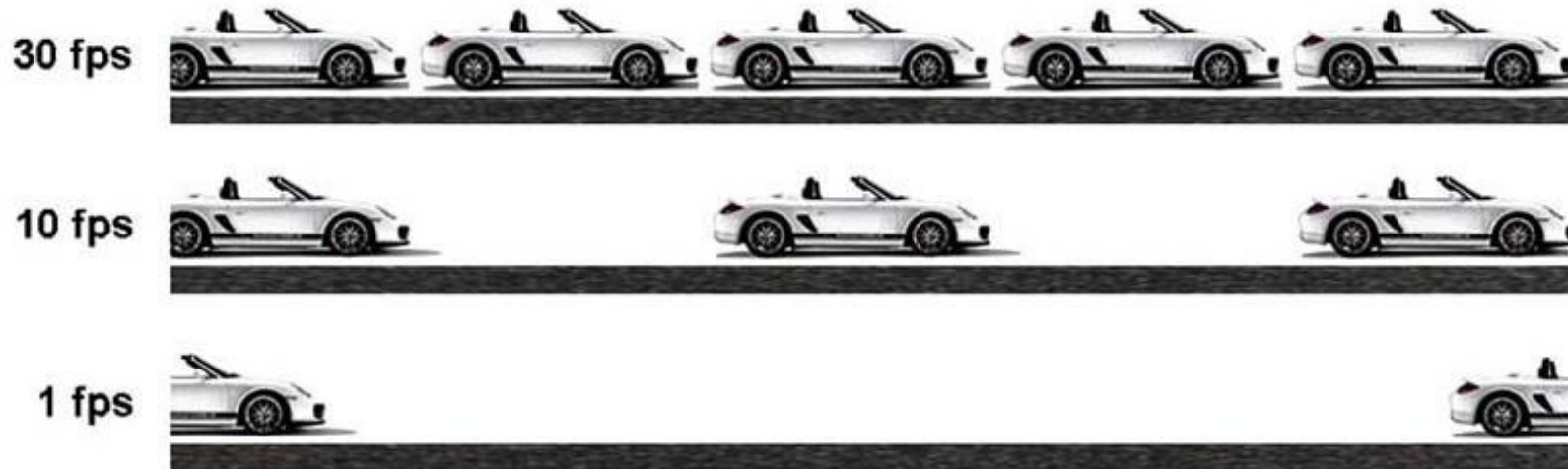


Picture Resolution

- MPEG resolution is measured in **common intermediate format (CIF)**
- In NTSC (National Television System Committee) CIF provides 352x240 pixel
- Lowest resolution MPEG image is a quarter CIF (QCIF) at 176x120 pixel
- 2 CIF (704x288, NTSC)
- 4 CIF (704x488, NTSC)
- 16 CIF will soon be available with very high resolution



Frame Rate



Frame rate (expressed in **frames per second** or **FPS**) is the **frequency (rate)** at which consecutive images called **frames** appear on a display. The term applies equally to film and video cameras, computer graphics, and motion capture systems.



Importance of the Frame Rate

- Minimum Frame Rate for security cameras is 30 fps



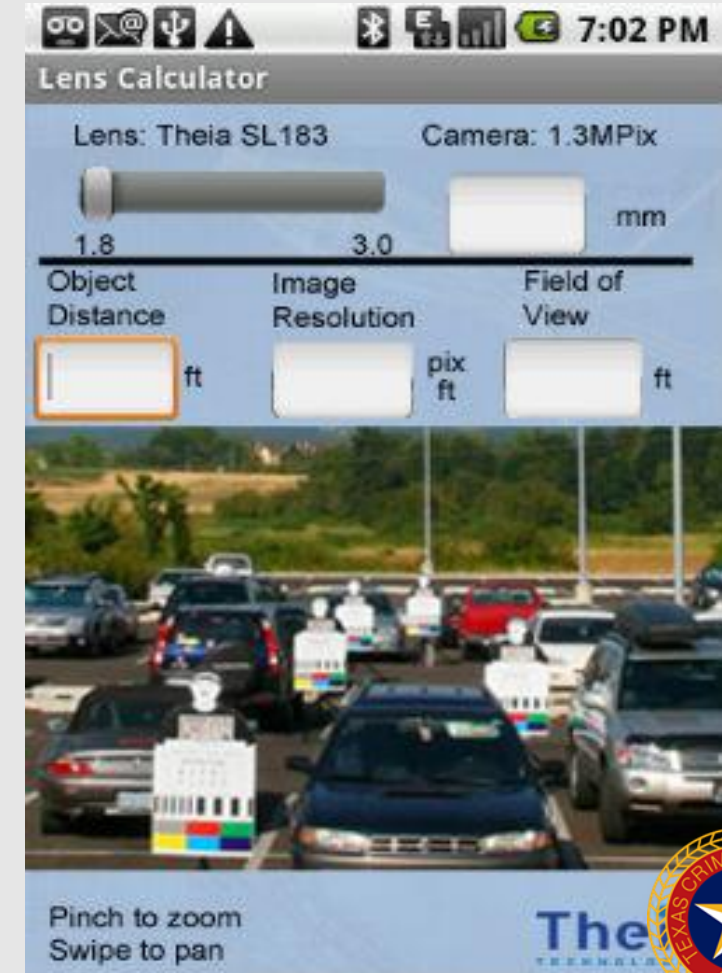
Display Issues

- **Display parity:** This is achieved when the number of pixels sent to a screen is the same as the number of pixels on the screen.
- **How to fix display parity:**
 - **Image Resolution:** There is little need to display images at 4 CIF (common intermediate format) or greater unless one is displaying at full screen. It is better to send live images to the screen at 2 CIF.
 - **Frame Rate:** Archived images do not usually need to be displayed at 15 or 30 fps. Use a slower speed and higher resolution for archived video.
 - **Processing Power:** Design systems with lots of processing power, typically dual Xeon computers as workstations. Dual-core processors are the best.



Image Resolution vs Field of View

- **Field of view** is the angular extent of the **image** scene and **resolution** is the number of pixels on target.
 - Wide View – See a large area **less** detail
 - Narrow View – Small area **high** detail
- **Ways to improve picture quality**
 - Change the distance of camera from the scene
 - Install higher resolution camera



Resolution	Image Size	Pixels per Images	Aspect Ratio
1080P	1920 x 1080	2,073,600	16:9
4 MP (1440p)	2560 x 1440	3, 686, 400	16:9
5 MP (1920p)	2560 x 1920	5, 017, 600	4:3
4 K (8 MP)	3840 x 2160	8, 294, 400	16:9

Common Resolution Security Camera

The most common resolution for security cameras on the market includes 2 MP (1080p), 4 MP (1440p), 5 MP (1920p) and 8 MP (4K/2160p).





4K
3840x2160



5MP
2560x1920



4MP
2560x1440



1080p
1920x1080





Digital Zoom



Optical Zoom





NO ZOOM



5x (OPTICAL)



**20x (OPTICAL
+ DIGITAL)**



1X



2X



4X



High Resolution Digital Zoom



Fish-Eyes Lens

The widest angles are provided by fisheye lenses – some of them even offer a 360-degree picture. The catch is the massive distortion necessary to put the entirety of a room onto a comparatively small screen.





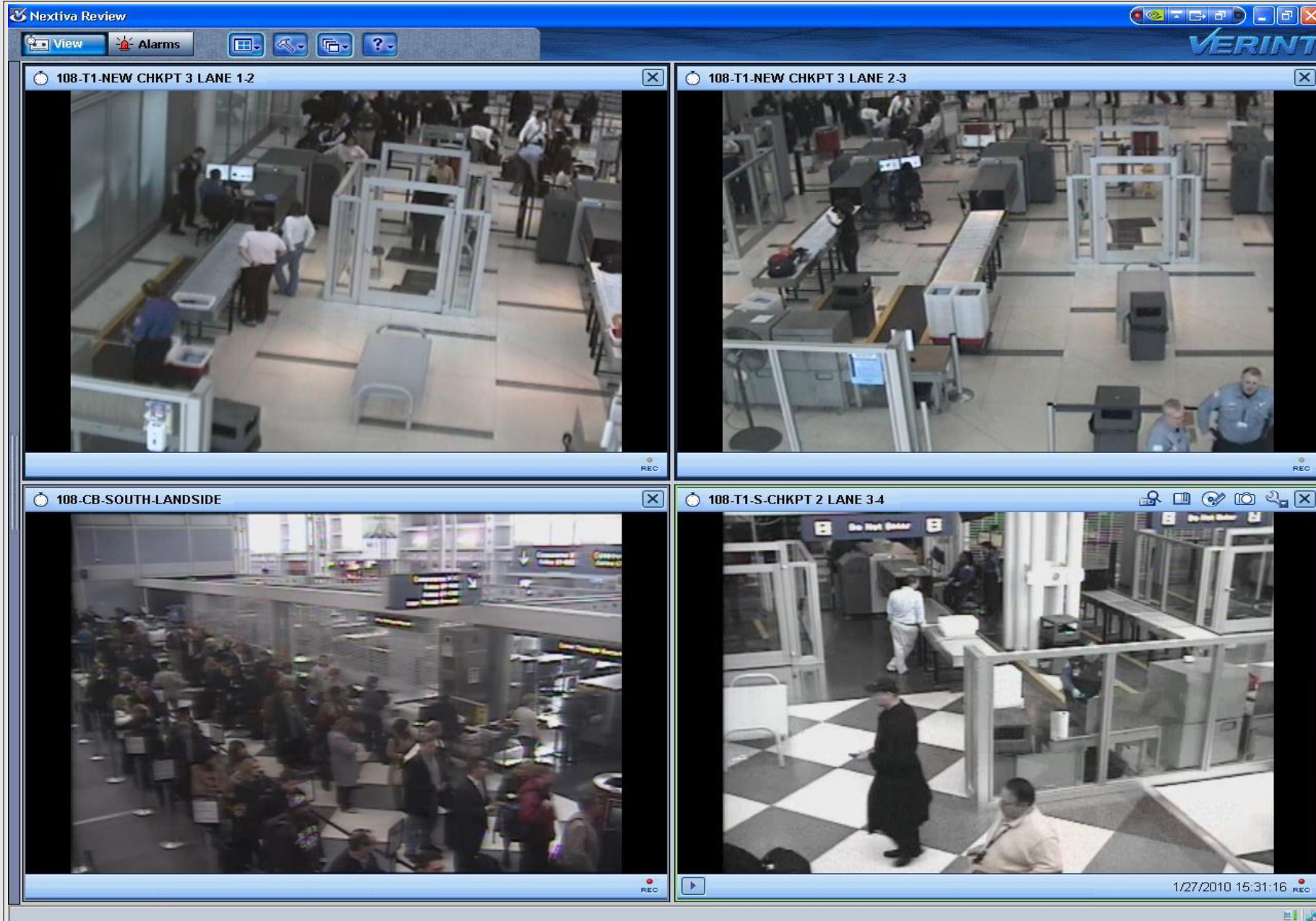
Panoramic and Multi Lens Cameras

Other cameras capture a wide field of view by simply adding more lenses facing in different directions. These systems stitch together multiple feeds to create a panoramic view.



3-Camera Stitch at U of M Stadium – 350 Feet





Traditional Camera Views





Hi-Res Cameras





Getting the Maximum out of Security Cameras

With today's high-resolution, megapixel cameras the lens might be the most important accessory to specify with each megapixel camera.



Conclusion

- Cameras have become an integral part of Commercial Security
- When conducting a site survey having a basic understanding of IP Camera systems is important.
- Today's camera security systems are mostly IP Cameras versus the CCTV (analog) systems
- The core camera systems includes the camera/lens, image capture, storage, transfer of data, and the final display to the end user.
- 4K (8 MP) Cameras offer the best digital and optical zoom.
- The most basic commercial camera must be 5 MP or higher
- Basic commercial cameras must have a minimum of 30 fps





ACCESS CONTROL

Natural Access, Commercial Doors, Biometrics, and
Beyond



Access Control and Space

- 4 Categories of Space:
- **Public Space** - Space that, whatever its legal status, is perceived by all members of a residential area or neighborhood as belonging to the public as a whole, which a stranger has as much perceived right to use as a resident.
- **Semipublic space** is accessible to all members of the public without passing through a locked or guarded barrier.
- **Semiprivate Space** - This space is restricted for use by residents, guests, and service people on legitimate assignments.
- **Private Space** - Private space is restricted for use by residents of a single-dwelling unit, their invited guests, and service people, with access generally controlled by locks and other physical barriers.



Access Control and Target Hardening

- **Eight elements in commercial properties that makes users feel unsafe:**
 1. Dark, hidden places;
 2. Large obstacles that obstruct sight-lines and transparency;
 3. Dark, solid materials like concrete;
 4. Bad or absence illumination;
 5. Easy accessible walls for graffiti;
 6. Absence of litter bins without communicating you are not allowed to eat, drink, etc., total deterioration;
 7. Possibilities for youth to hang around; and
 8. Non repaired acts of vandalism.



Modifying Space to Harden the Target

- **Five ways to modify a situation are as follows:**

1. Increasing the effort the offender must make to carry out the crime;
2. Increasing the risks the offender must face in completing the crime;
3. Reducing the rewards or benefits the offender expects to obtain from the crime;
4. Reducing or avoiding provocations that may tempt or incite offenders into criminal acts
5. Removing excuses that offenders may use to “rationalize” or justify their actions.



Natural Access Control

- **Access control is a design concept directed primarily at decreasing crime opportunity.**
- **This concept falls under the umbrella of spatial definition**
- Example 1: If unwanted visitors remain in an area because of a design feature, such as a wall or barrier, the feature should be removed (unless required) or changed to make it less attractive, thereby reducing the overall attractiveness of the area.
- Example 2: Skateboarders who use a particular plaza because of the many attractive, flat wooden benches. Pop-up seats could be installed on the benches, making it difficult, if not impossible, for skateboarders to use them.



Access Control

- What form of access control would commercial doors fall under?



4 types of Commercial Doors

Roll-up Door



Scissor Gate

Overhead Door



Fire Rated



Commercial Door Material

- **Steel** - These doors are manufactured from metal sheets wrapped around honeycombed core or insulation (may have a wooden frame).
- **Wood** - These doors are usually used on interior commercial applications
- **Aluminum with Glass** - These doors are used in commercial businesses due to its sophisticated, sleek, and clean appearance
- **Fiberglass** - These doors are manufactured using plastic matrix and fine fibers of glass.
- **Full Glass** - These door are used mainly for decorative purposes.
- **Overhead Steel** - These doors are preferred to be used in storage facilities, warehouses, and loading docks.



Commercial Steel Doors

- Resistant to cracking and warping
- Made of 16 to 25 gauge steel
- Most Durable and long lasting
- Used in many applications
 - Warehouse
 - Schools
 - Churches
 - Office Buildings
 - Etc.



Commercial Door Lites

- Door lites are glass panels that allow varying amounts of light to pass through.
- 3 Types of door lites
 - **Insulated** - These types of door lights prevent the building from overheating in the summer, and keep the inside warm during the winter.
 - **Textured** - Permits sunlight into the establishment without clearly revealing all of the interior to outsiders.
 - **Tinted** - Some business owners will choose to install tinted door lights to reduce the impact of heat and sunlight.



Example Door Lights



Aluminum Storefront with Glass doors

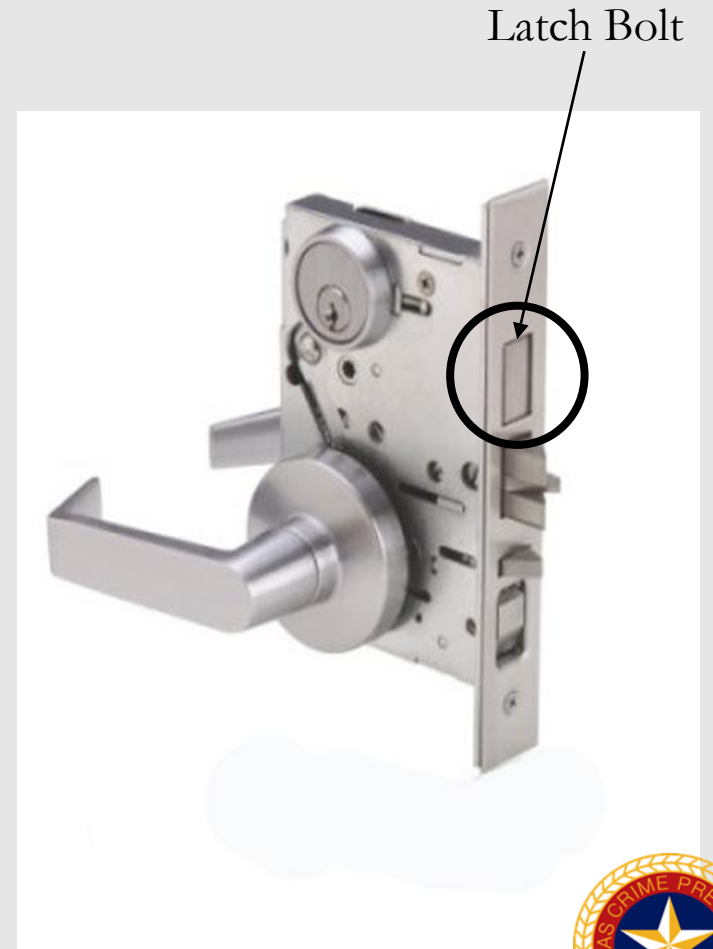
Why they are preferred by most business owners?

- **Lite weight** – easy to open and close by customers
- **Good Visibility** - reflect their honesty and transparency in business, promotes “see and be seen” principle
- **Cost Effective to Repair** - Aluminum is the metal which never corrodes or gets rust overtime. It is light in weight and safe for the glass windows.
- **Energy Efficient** - It reduces the consumption of lighting as natural light can flow into the store from the transparent glass and also offer better insulation when the cooling or heating system is functioning within the store.



Commercial Grade Locks

- Extra heavy duty mortise lockset that conforms to Federal Specification. The latch bolt can be fully retracted with 35 degree lever rotation.
- One case size for all functions.
- Armored Front
- Sample Applications:
 - **Front Door Deadbolt** – Latch bolt operated by lever from both sides. Key from outside retracts latch bolt. Toggle locks/unlocks outside lever. Key outside extends/retracts deadbolt. Inside thumb turn extends/retracts deadbolt.
 - **Store Door Double Cylinder** – Latch bolt operated by lever from both sides. Key inside and outside extends/retracts deadbolt.



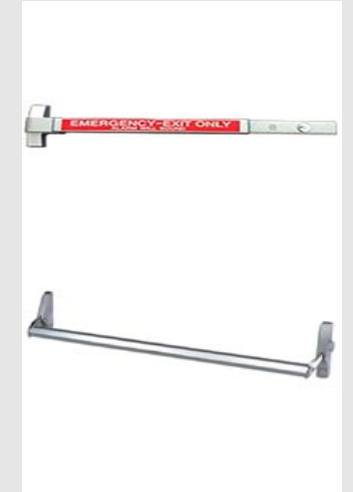
Commercial Grade Locks

- Lock features a simple rectangular shape that makes it a great choice for classic as well as more modern decors.
- The deadbolt above the lever is thrown and retracted by a thumb turn from the interior and by a key from the exterior.
- The housing is made of cold rolled steel and zinc dichromate finish for rust resistance.
- Panic Proof
 - Classrooms
 - Other Interior Applications
 - Exterior Applications



Door Panic Hardware

- **Touch bar** style exit devices are suitable for all doors (aluminum, hollow metal, or wood) where there is no projection on the door face. This bar is **non-handed** and for doors 30" - 36" wide

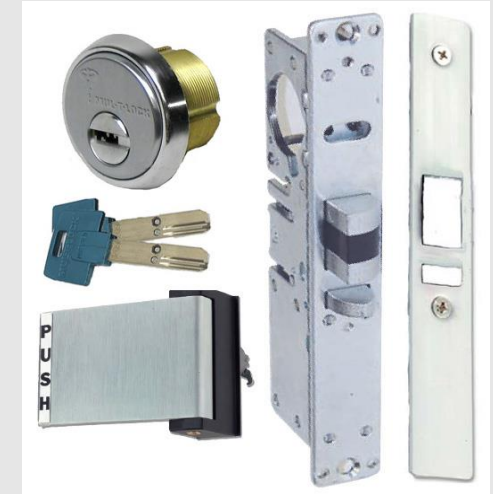
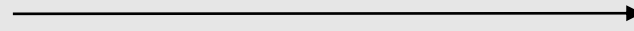


- **Surface Vertical Rod panic device** is the perfect choice for double doors without mullions. Suitable for all doors (aluminum, hollow metal, or wood), durable enough for the most demanding applications.



Other Commercial Door Hardware

- Store front glass door **Dead Latch** with Push / Pull Paddle Handle.



- Door Security Guard Plates →



- High Security Key Pads →



Commercial Electric Strike Plates

- Electric strikes are an important piece of any access control system, replacing fixed strike plates. These specialized pieces of hardware are what allows an electronic signal to “release” the latch from the frame and open the door.
- Electric strike locking mechanism— whether it’s cylindrical, deadbolt, mortise or an exit device — can be operated without the use of a mechanical key
- Electric strikes are essential to maintaining the **functionality** of card access systems, intercoms, and various other door systems.



Commercial Door Returns

Self Closing Hinge



Door Closer

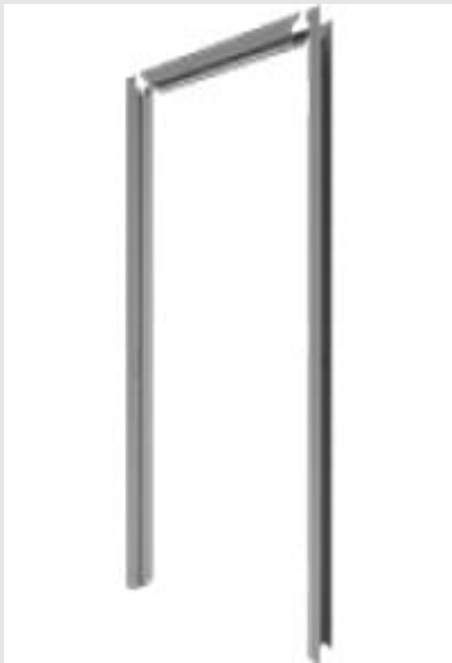


Commercial Door Frames

Wood Frame

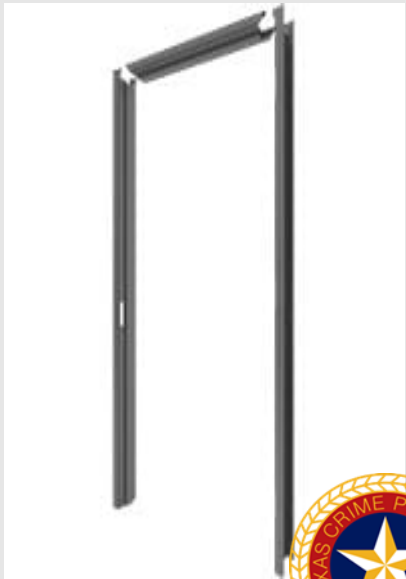


Double Door Frame



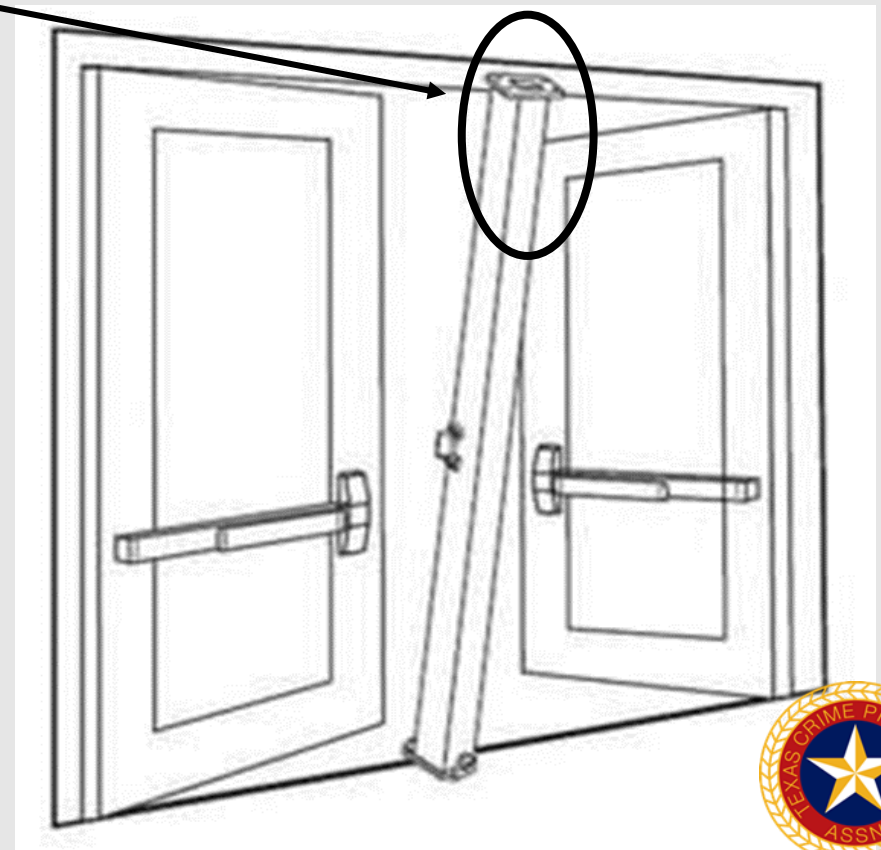
Aluminum Frame

Steel Frame



Double Doors and Mullions

Mullion - A fixed or movable post dividing an opening vertically.



Mullion Considerations

Bolt in



Lockable





COMMERCIAL ALARMS SYSTEMS

Intrusion Detection



Commercial Alarms

- Alarms today are integrated systems that create redundancy and improve reporting.
- Alarms are now connected via mobile devices and other mobile technology.
- Alarms now often integrate network video (no longer CCTV)
- 95 – 98 % of alarms are faulty
- Approximately 30% of all police calls are alarm type calls
- Approximately 1 in 1000 alarms are triggered by illegal entry



Basic Question for Selecting an Alarm System

- The threat and risk. What is the system to protect against?
- The type of sensors needed. What will be protected?
- What methods are available to provide the level of protection needed?
- The method of alarm signal transmission. How is the signal to be sent and who will respond?



Perimeter / Interior Protection

- **Video Motion Detection** – Cameras working with AI to detect intruders.
- **Door Switches** – Uses a contact system. When the magnet moves it break the circuit causing activation.
- **Glass Break Detectors** - attached to the glass and sense the breakage of the glass by shock or sound. Glass breakage sensors use microphone transducers to detect the glass breakage. **A ceiling sensor over a window covers a 30-degree radius.**
- **Interior Motion Detection** – Uses ultrasonic receivers or photoelectric beam.



Space Protection

- **Video Motion** - These cameras detect motion in a wide field of view and transmit an alert.
- **Video Analytics** - These cameras detect specific changes in a narrow field of view and transmit an alert.
- **Photoelectric Eyes (beam)** - These devices transmit a beam across a protected area. Photoelectric devices use a pulsed infrared beam that is invisible to the naked eye.
- **Ultrasonic** - They (although rarely used today) work on a low-frequency sound wave projected from the unit. The frequency is in kilohertz (2326), and its area of coverage can be anywhere from 5 to 40 ft in length.
- **Microwave.** Microwave detectors are a volumetric type of space protection and are based on a Doppler shift. They detect intruders by the use of a radiated RF electromagnetic field.
- **Passive infrared (PIR) motion detectors.** These detectors are passive sensors, because they do not transmit a signal for an intruder to disturb. (These are thermal detect body heat change)
- **Pressure mats.** These mats are basically mechanical switches.
- **Dual-techs.** Dual-technology sensors, commonly referred to as dual-techs, are a combination of two types of space-protection devices.



Object / Spot Detection

1. **Video motion detectors:** These cameras detect motion in a wide field of view
2. **Video analytics:** These cameras detect specific changes in a narrow field of view
3. **Capacitance/proximity detectors:** The object being protected becomes an antenna, electronically linked to the alarm control. When an intruder approaches or touches the object/antenna, an electrostatic field is unbalanced, and the alarm is initiated. **Only metal objects can be protected in this manner.**
4. **Vibration detectors:** These devices utilize a highly sensitive, specialized microphone called an electronic vibration detector (EVD). The EVD is attached directly to the object to be protected. It can be adjusted to detect a sledgehammer attack on a concrete wall or a delicate penetration of a glass surface. It sends an alarm only when the object is moved.



Alarm Control Systems

- **Wireless Alarms Signal Transmission:**
 - RF – It is an electromagnetic wave used to communicate
 - Wifi – radio waves
 - Z-Wave – low energy radio waves that mesh Z-Wave devices together
 - ZigBee – like Z-wave but targeted at battery powered devices
- **What do you think causes the most severe burglary losses to business?**
- Modern control panels use one or more microprocessors, which allows the control panel to send and receive digital information to the alarm station.
- Tamper protection is a feature that generates an alarm signal when the system is compromised in any way
- Individual Alarm Codes



Alarm Transmission / Signaling

- **Local alarm:** A bell, siren, and/or strobe light signal that an attempted or successful intrusion has taken place
- **Central station system:** The alarm signal is transmitted over telephone lines, the internet through the Internet Protocol (IP) rules, cellular phone, or RF to a specially constructed building called the central station.

- Direct Wire Systems
- Multiplex System
- Digital Communicator
- Alarm Dialer
- Radio / Cellular / IP
- Audio / Video Verification
- Enhanced call Verification



Alarms Deter Crime

- The National Crime Prevention Institute has long endorsed alarm systems as the best available crime deterrent, and this deterrent value is increased when warning sign(s) are placed at the protected premises indicating the presence of an intrusion alarm system
- Most criminals fear alarm systems; they much prefer to break into an unprotected building rather than risk capture by a hidden sensor.
- Problem deterrence is the alarm business
 - Sprinkler systems
 - Fire sensors
 - Watching temperature levels in buildings to supervising industrial processes



False/Nuisance Alarms

- **False Alarms:** caused by a malfunction of the system
- **Nuisance Alarms:** caused by non-intruder-related conditions
 - Lack of proper education on how to enter and exit the complex
 - Weather
 - Equipment failure (dead batteries) and installation problems



Conclusion

- Most Alarm Systems today are using Passive Infrared Sensors (these are general motion sensors)
- Most systems today are wireless
- Keypads are replacing keys
- Two-way voice modules are being used for communication
- Control Panels are just one single panel with a micro processor
- Fobs and Cellphones used for remote arming





ACCESS CONTROL & BIOMETRICS

Locks, Key Control, Card Access, Wireless Solutions



Locks and Key Control

- **Keys to good Key Control**
 - High Security Locks
 - Strict Key Control with Logs
 - Keys should have unique control numbers
 - Key Control Logs Should be confidential
 - Upon Separation Keys Should be retrieved immediately
 - **Recommend Electronic Locks**



Electronic Access Control

- Access is gained by presentation of a card, badge, token, or software token stored on a mobile device to an access control “reader.”
- “Field” or “Distributed Intelligence”: These systems connect to a host computer, internet-based system, or cloud service. These readers will have a local server for entry and maintains history.
- These systems make key control easy and, in many cases, obsolete.
- These systems are wireless, and use transmit cards or token. “Smart” cards.
- Smart cards store personal information, thumb print or retina scan.



Types of Cards and Badges

- **Proximity cards:** Proximity access cards are most often used for EA systems.
- **Magnetic stripe cards:** Magnetic cards use various kinds of materials and mediums to magnetically encode digital data onto cards.
- **Weigand cards:** Weigand-based access control cards use a coded pattern on magnetized wire embedded within the card.
- Biometrics access control. Biometrics is most accurate when using one or more fingerprints, palm prints or palm scan, hand geometry, or retina and iris scan.
- Biometric ID systems operate locks to doors. Used in high-security areas where limited access is maintained, this system checks physical characteristics that verify and allow access/entry.



Types of Cards and Badges

- **Smart cards:** These contain an integrated chip embedded in them. They have coded memories and microprocessors; hence, they are like computers.
- **Dual-technology card:** Some cards have dual technology, such as magnetic stripe/proximity card and an RFID/proximity card.
- **Card readers:** Card readers are devices used for reading access cards. Readers come in various shapes, sizes, and configurations.
- **Electronic access control (EAC) systems applications:** Part of a fully integrated facility management system. In such a system, electronic access control is interfaced and integrated with fire safety/life safety systems, CCTV systems, communication systems, and non security systems, such as heating, ventilation, and air-conditioning.



Multiple Factor / Biometrics Technologies

- **Fingerprints and palm prints:** Formed when the friction ridges of the skin come in contact with a surface that is receptive to a print by using an agent to form the print, such as perspiration, oil, ink, grease, and so forth.
- **Hand scanner and finger reader recognition systems:** These measure and analyze the overall structure, shape, and proportions of the hand, such as length, width, and thickness of the hand, fingers, and joints, and characteristics of the skin surface such as creases and ridges.
- **Iris cameras:** They perform recognition detection of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance.



Multiple Factor / Biometrics Technologies

- **Facial recognition device:** This views an image or video of a person and compares it to one in the database.
- **Voice recognition voiceprint:** This is a spectrogram that is a graph showing a sound's frequency on the vertical axis and time on the horizontal axis. Different speech creates different shapes on the graph.
- **Digital biometrics signature:** This is equivalent to a traditional handwritten signature in many respects since if the signature is properly implemented, it is more difficult to forge than the traditional type.
- **Vein recognition:** Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger.



Emerging Trends

- Optical high-speed turnstiles,
- Hand-held explosive and biohazard detection, and, most recently,
- Millimeter wave scanning.

Access Control is a vital first line of defense in the protection of people, assets, and information



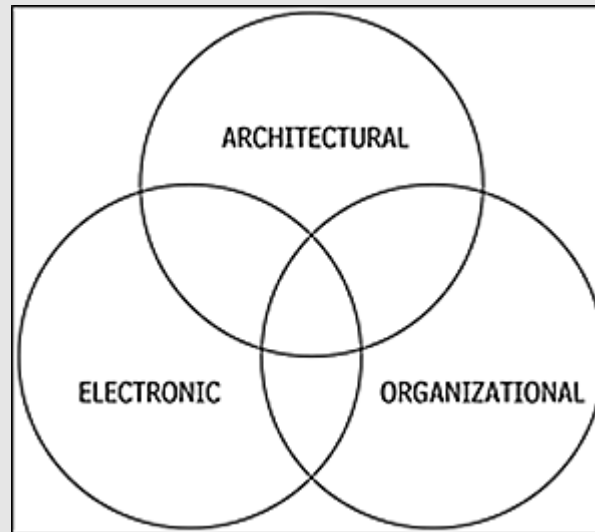


TERRITORIAL REINFORCEMENT



Definition

- Physical design can create an area of territorial influence that can be perceived by and may deter potential offenders. Examples include defined property lines and clear distinctions between private and public spaces.
- Territorial reinforcement can be created using landscaping, pavement designs, gateway treatments, signs and fences.
- Territorial reinforcement may also be defined as “Defensible Space” (Phrase coined by Oscar Newman)
- Private vs. Public Space
- CPTED implementation
 - Electronic
 - Architectural
 - Organizational



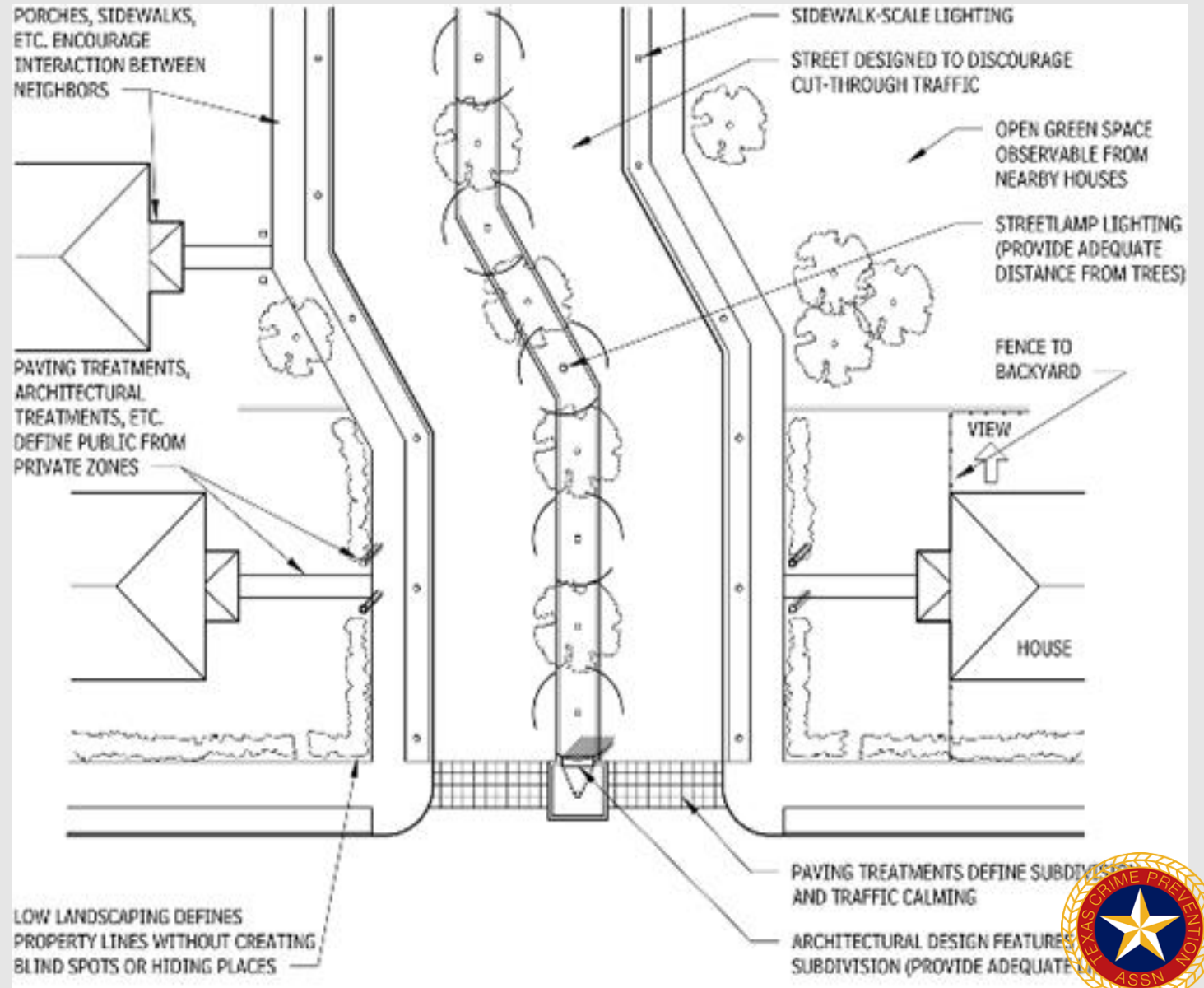
Strategies for Territorial Reinforcement

- Entryways or vestibules create a transitional area between the street and the building.
- Define property lines and private areas with plantings, pavement treatments, or fences.
- The street address should be clearly visible from the street, with numbers **a minimum of 5 in. high and made of non-reflective material.**



Sample Diagram

- Porches and Sidewalks
- Paving Treatments
- Architectural Treatments
- Low Landscaping
- Sidewalks and lighting
- Street Design
- Open Green Space
- Fence Lines



Subdivisions and Office Parks

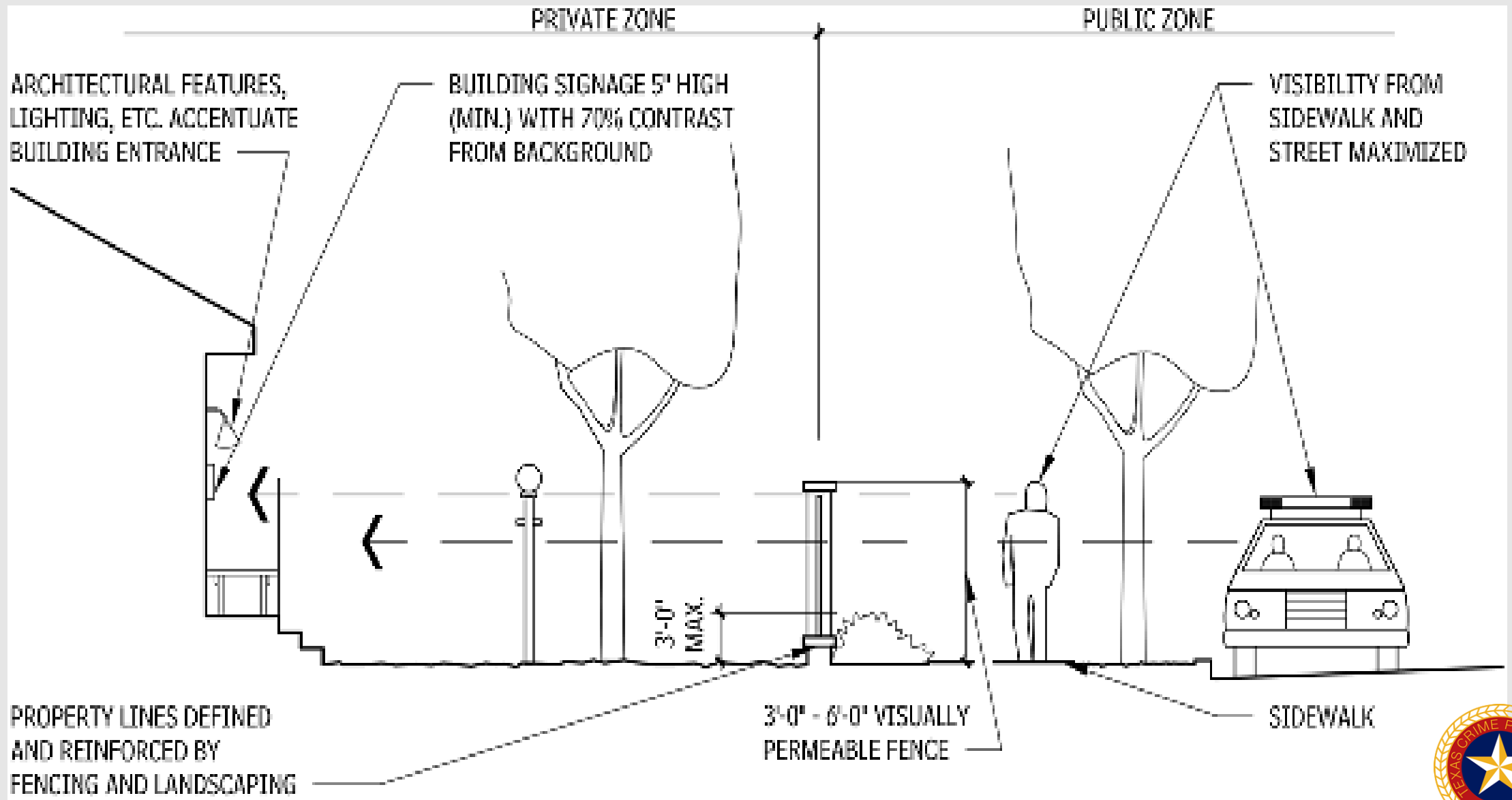
- Design lots, streets, and houses to encourage interaction between neighbors.
- Accent entrances with changes in street elevation, different paving materials, and other design features.
- Clearly identify residences with street address numbers that are a minimum of 5 in. high and are well lit at night.
- Property lines should be defined with post-and-pillar fencing, gates, and plantings to direct pedestrian traffic.
- All parking should be assigned.



Multiresident / Apartment Homes

- Define property lines with landscaping or post-and-pillar fencing but keep shrubbery and fences low to allow visibility from the street. (7' and 3')
- Accent building entrances with architectural elements and lighting and/or landscape features.
- Doorknobs should be 40 in. from windowpanes.
- Clearly identify all buildings and residential units with well-lit address numbers a **minimum of 5 in. high.**
- Common doorways should have windows and be key-controlled by residents.
- Locate mailboxes next to the appropriate residences.





Examples of Territorial Reinforcement



Examples of Territorial Reinforcement





COMMERCIAL FENCING

Territorial Reinforcement



Recommendations

- A chain-link fence is one of the primary building blocks for a facility's perimeter security system.
- Chain-link fence provides one or more of the following functions:
 - Gives notice of a legal boundary
 - Assists in controlling and screening authorized entries into a secured area
 - Supports surveillance, detection, assessment, and other security functions
 - Deters casual intruders from penetrating a secured area
 - Demonstrates the intent of an intruder by their overt action of gaining entry,
 - Causes a delay to obtain access to a facility, increasing the possibility of detection,
 - Creates a psychological deterrent,
 - Reduces the number of security guards required and frequency of use for each post,
 - Optimizes the use of security personnel
 - Demonstrates a corporate concern for facility security, and
 - Provides a cost-effective method of protecting facilities.



Chain Link Fence and Security Planning

- In-depth security planning takes into consideration the mission and function, environmental concerns, threats, and the local area of the facility to be secured, which is the A-B-C-D method pointing out the values of this fencing type.
- **Chain link fence is the common denominator of the ABCD method.**
 - A. Aids to Security:** Assist in the use of other devices.
 - B. Barriers for Security:** These can be buildings, chain-link fences, walls, temporary checkpoints, and so on.
 - C. Controls:** Supports the physical security chain-link fences and barriers, such as an access control system tied into vehicle gates and pedestrian portals
 - D. Deterrents:** such as a chain-link fence, guards, lighting, signage, and checkpoint control procedures, ensure that intruders will consider it difficult to successfully gain access.



Framework and Fabric

- The framework for a chain-link fence consists of the line posts, end posts, corner posts, gateposts, and, if required, a top, mid, bottom, or brace rail.
- Chain Link Fabric: (do not consider light weight or residential fabric)
 - **Wire gauge**
 - 11 ga (0.120 in. diameter)—minimum break strength of 850 lbf
 - 9 ga (0.148 in. diameter)—minimum break strength of 1290 lbf
 - 6 ga (0.192 in. diameter)—minimum break strength of 2170 lbf
 - **Mesh Size** (mesh size is the minimum clear distance between the wires forming the parallel sides of the mesh)
 - 2-in. mesh
 - 1-in. mesh,
 - 3/8-in. mesh



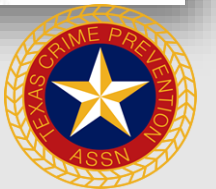
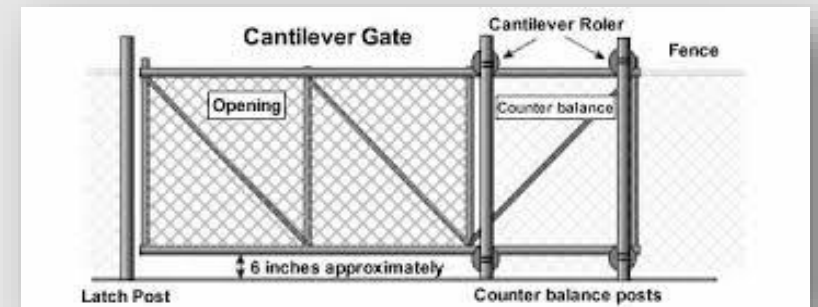
Things to Remember About Mesh Size

- The smaller the mesh size, the more difficult it is to climb or cut.
- The heavier the gauge wire, the more difficult it is to cut.
- The various mesh sizes available in the three previously discussed gauges are listed in the order of their penetration resistance/security:
 1. **Extremely high security:** 3/8-in. mesh 11 ga
 2. **Very high security:** 1-in. mesh 9 ga
 3. **High security:** 1-in. mesh 11 ga
 4. **Greater security:** 2-in. mesh 6 ga
 5. **Normal industrial security:** 2-in. mesh 9 ga



Gate Recommendations

- Gates are the only moveable parts of a fence and therefore should be properly constructed with appropriate fittings
- Limiting the size of the opening increases vehicular security and reduces the possibility of one vehicle passing another, and the smaller opening reduces the open close cycle time.
- **The cantilever slide gate is the most effective for vehicle security.**
- Pedestrian/personnel gates can be constructed using a basic padlock or designed with an electrical or mechanical lock or a keypad/card key system tied into an access control system.



Chain Link Fence Design Features

- **Height:** The higher the barrier the more difficult and time consuming it is to broach. Industry Standard is 8' fences
- **Eliminating top rail:** Omission of a rail at the top of the fence eliminates a handhold, thus making the fence more difficult to climb. A 7-ga coil spring wire can be installed in place of the top rail.
- **Adding barbwire:** Addition of three or six strands at the top of the fence increases the level of difficulty and time to broach.
 - When using the three-strand 45-degree arm, it is recommended to angle the arm out from the secured area
 - Bolt or rivet barbwire arms to post. Barbwire arms are normally held to the post by the top tension wire or top rail.





Chain Link with (3) three strand Barb Wire



Chain Link with no Top Rail



Chain Link Design Features

- **Adding barbed tape:** Stainless steel barbed tape added to the top and in some cases the bottom of the fence greatly increases the difficulty and time to breach.
- **Bury the chain-link fabric:** Burying the fabric 12 in. or more will also eliminate the possibility of forcing the mesh up.
- **Adding bottom rail:** Addition of a bottom rail that is secured in the center of the two-line posts using a 3/8-in. diameter eye hook anchored into a concrete footing basically eliminates the possibility of forcing the mesh up to crawl under the fence.
 - **The bottom of the fence, with or without a bottom rail, should be installed not greater than 2 in. above grade.**





Barbed Tape



Example of Bottom Rail



Chain Link Fence Design Features

- **Colored chain-link fabric:** Color polymercoated chain-link fabric enhances visibility, especially at night. Complete polymer-coated systems, including coated fabric, fittings, framework, and gates, increase visibility and provide greater corrosion resistance, especially for use in areas adjacent to the seacoast.
- **Double row of security fencing.** It is not uncommon to add an additional line of internal security fencing 1020 ft. inside the perimeter fence. In many cases, double rows of fencing are used with sensors and detectors or with a perimeter patrol road in the area between the fences.
- **Clear zone.** In wooded or high grassy areas, it is advisable to clear and grub a clear zone on either side of the fence to aid surveillance.



Example Colored Chain Link



Chain Link Fence Design Features

- **Internal security fencing:** Many situations require the need of a separate interior fence to add another level of security for a particular building, piece of equipment, or location.
- **Peen all bolts:** This eliminates the removal of the bolt nut.
- **Addition of a sensor system:** This adds another level of security to the fence system.
- **Addition of lighting:** It increases visibility as well as raises the level of psychological deterrent.
- **Signage:** Installed along the fence line, signs are important to indicate private secured areas (violators may be subject to arrest) and possibly note the presence of alarms and monitoring systems.



Commercial Chain Link with Lighting



Summary

- Gives notice legal boundary of the outermost limits of a facility.
- Assists in controlling and screening authorized entries into a secured area by deterring entry elsewhere along the boundary.
- Supports surveillance, detection, assessment, and other security functions by providing a zone for installing intrusion detection equipment and CCTV.
- Deters casual intruders from penetrating a secured area by presenting a barrier that requires an overt action to enter.
- Demonstrates the intent of an intruder by their overt action of gaining entry.
- Causes a delay to obtain access to a facility, thereby increasing the possibility of detection.
- Creates a psychological deterrent.



Summary

- Reduces the number of security guards required and frequency of use for each post.
- Optimizes the use of security personnel while enhancing the capabilities for detection and apprehension of unauthorized individuals.
- Demonstrates a corporate concern for facility security.
- Provides a cost-effective method of protecting facilities and signage along the fence





PROTECTIVE BARRIERS

Territorial Reinforcement

Overview

- Protective barriers form the perimeter of controlled, limited, and exclusion areas.
- Examples: water sources, transformer banks, commercial power and fuel connections, heating and power plants, or air-conditioning units)
- **Two Types**
 - **Natural protective barriers:** Mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse
 - **Structural protective barriers:** Man-made devices (such as fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.



Overview

- Considerations for protective structural barriers include the following:
 - Weighing the cost of completely enclosing large tracts of land with significant structural barriers against the threat and the cost of alternate security precautions (such as patrols, ground sensors, electronic surveillance, and airborne sensors)
 - Sizing a restricted area based on the degree of compartmentalization required and the area's complexity
 - As a rule, **size should be kept to a minimum consistent with operational efficiency**





Why Establish Protective Barriers?

- Controlling vehicular and pedestrian traffic flow,
- Providing entry control points where ID can be checked
- Precluding visual compromise by unauthorized individuals
- Delaying forced entry
- Protecting individual assets.



Perimeter Entrances

- Active perimeter entrances should be designated so that security forces maintain full control without an unnecessary delay in traffic.
- sufficient entrances to accommodate the peak flow of pedestrian and vehicular traffic and having adequate lighting for rapid and efficient inspection.
- When gates are not operational during nonduty hours, they should be securely locked, illuminated during hours of darkness, and inspected periodically by a roving patrol.
- Warning signs should be used to warn drivers when gates are closed.
- Doors and windows on buildings that form a part of the perimeter should be locked, lighted, and inspected.



Perimeter Entry Control

- Entry-control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.
- Establishing a holding area for unauthorized vehicles or those to be inspected further. A turnaround area should be provided to keep from impeding other traffic.
- Establishing control measures such as displaying a decal on the window or having a specially marked vehicle.
- Entry-control stations that are manned 24 hours each day should have interior and exterior lighting, interior heating and cooling.
- Signs should be erected to assist in controlling authorized entry, to deter unauthorized entry, and to preclude accidental entry



Perimeter Clear Zones

- Clear zones should be kept clear of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to breach the barrier.
- **A clear zone of 20 ft or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or man-made features.**
- When possible, a clear zone of 50 ft or more should exist between the perimeter barrier and structures within the protected area, except when a building's wall constitutes part of the perimeter barrier.
- Ammunition supply points (ASPs) will have clear zones 12 ft outside of the ASP and 30 ft inside, and the vegetation will not exceed 8 in. (4 in. for high-threat and highly controlled areas).

Perimeter Clear Zones

- Entry-control stations should be hardened against attacks according to the type of threat. The methods of hardening may include:
 - Reinforced concrete or masonry;
 - Steel plating;
 - Bullet-resistant glass;
 - Sandbags, two layers in depth; and
 - Commercially fabricated, bullet-resistant building components or assemblies.



Internal Barriers

- Barriers are psychological deterrents allowing unauthorized access
- 4 Functions of internal barriers
 - **Define** protection area boundaries.
 - **Delay**—slow traffic or access. Consider speed bumps.
 - **Direct access** to garages, parking lots, and building entrances.
 - **Deny unauthorized access** and allow only authorized visitors.



Commercial Barrier Design and Layout

- What are the three (3) lines of defense?
 1. Perimeter barriers or the outer edge to your property line
 2. The exterior of the building, which includes the roof and roof access and walls, doors, and windows.
 3. The interior of the building
- It is important to reduce access points by using access control and have specific areas zoned for access control and added security





Two types of Structural Barriers

1. Passive Barriers

- Jersey barriers
- Large boulders or rocks
- Large round cement stones
- Roadblocks or closed roads
- Fences
- Gates
- Bollards at entrances





Two Types of Structural Barriers

2. Active Barriers

- Hydraulic bollards
- Motor-operated lift-arm gates
- Pop-up wedges
- All geared to control traffic for entrances and exits



Planning a Barrier Recommendations

- Walls are usually more expensive than fences, observation enclosures, and a Network Video System (CCTV), and exterior cost-effective lighting. Opaque fences may provide a cheaper alternative.
- Fences and walls provide only limited delay against intruders; the least secure types can only delay a skilled intruder for a few seconds.
- combine a fence or wall with security lighting, an intruder detection system, a network video system, guards
- The perimeter should be as short as possible and illuminated.
- The perimeter should run in straight lines between corner posts to facilitate surveillance.
- Drains or culverts giving access beneath the perimeter barrier should be protected.
- The ground on both sides of the perimeter barrier should be cleared to deny cover to an intruder.



Planning a Barrier Recommendations

- A sterile zone protected by a double fence may be required for certain types of intruder-detection sensors.
- A security guard force should support the perimeter security system.
- Exterior emergency phones connected to security officer's desk.
- Barriers are deterrents. They come in a variety of acceptable sizes and shapes.
- The minimum commercial chain link fence height that is most effective in stopping an intruder is **8' excluding 1' top guard three (3) strands of barb wire**





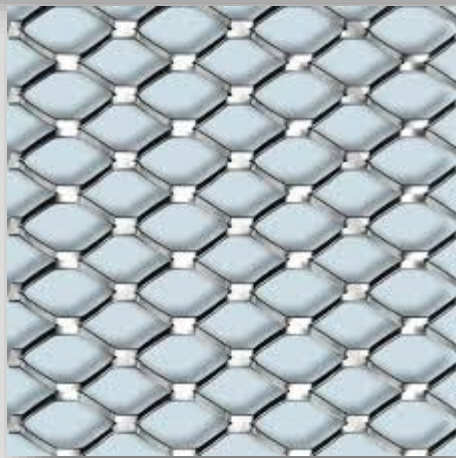
Palisade Fencing

Types of Security Fencing

- Industrial security chain-link fence.
- Standard anti-intruder chain-link fence.
- Standard steel palisade fence, security pattern standard expanded metal (Expamet) security fence.
- High-security steel palisade fence.
- Power fencing.



Palisade Fencing



- Palisade fences are more expensive than chain-link fences but have better potential upgrading to increase effectiveness against intruders and for the addition of fence-mounted intrusion detection sensors.
- Galvanized palisade fences have a much longer life than chain-link fences, Expamet, or weld-mesh fences.



Summary

- Keep in mind that structural barriers physically and psychologically deter and discourage the undetermined, delay the determined, and channel the traffic flow through entrances
- Fences and walls provide only limited delay against intruders; the least secure types can only delay a skilled intruder for a few seconds
- A perimeter barrier intended to provide substantial protection against intruders should, therefore, combine a fence or wall with security lighting, an intruder detection system, a Network Video System (CCTV), and a security guard forces.





MAINTENANCE & MANAGEMENT



Definition

- Allows for the continued use of the space for its intended purpose. Ensuring that lighting, vegetation where applicable, cameras, windows, doors, and other elements contributing to the sense of ownership and activity observation are effectively maintained



What do these ictures tell you?



Why Maintenance is Important?

Increase in physical deterioration

Increased concern for personal safety among residents and proprietors;

Decreased participation in maintaining order on the street;

Increased delinquency, rowdiness, vandalism, and disorderly behavior among locals;

Further increase in deterioration and further withdrawal from the streets by residents and other locals;

Potential offenders from outside the neighborhood, attracted by vulnerability, move into the area.



Image and Maintenance

Characteristics of an environment, express the type of ownership of the property.

Maintained Property = Pride in ownership

Deterioration in Property = Little involvement and owner does not care

Truth: If a window is broken and remains unfixed for a length of time, vandals will break more windows.



Image and Maintenance



Image and Maintenance

- Landscape design helps define semiprivate and private spaces within a complex, a commercial property, hotel, etc. It needs to be maintenance.
- **Recommendations**
 - Landscape furniture should be vandal-resistant, and if benches are installed, they need to be designed so that individuals cannot sleep on them.
 - consideration, exterior lighting, video surveillance, vegetation, maintenance, barriers, the entrances and exits on your property, and signage and the surface structure.
 - Ensure Shrubs and trees don't create blind spots
 - Is the fence strong and in good repair?
 - Are there weeds or trash adjoining the building that should be removed?
 - Are stock, crates, or merchandise allowed to be piled near the building?



Summary





GEOGRAPHICAL JUXTAPOSITION



Geographical Juxtaposition Defined

- **It is the surrounding proximal environment of a crime location.**
- Crime issues stemming from influences at a variety of levels of remoteness from the crime location.
 - Example: How could a High School influence the corner store?
How could illegal drug production in the country effect urban areas?



Laws of Geography

(Tobler 1970)

1. Everything is related to everything else, but near things are more related than distant things
2. Phenomenon external to an area of interest affects what goes on inside



Geographical Juxtaposition in CPTED and Planning

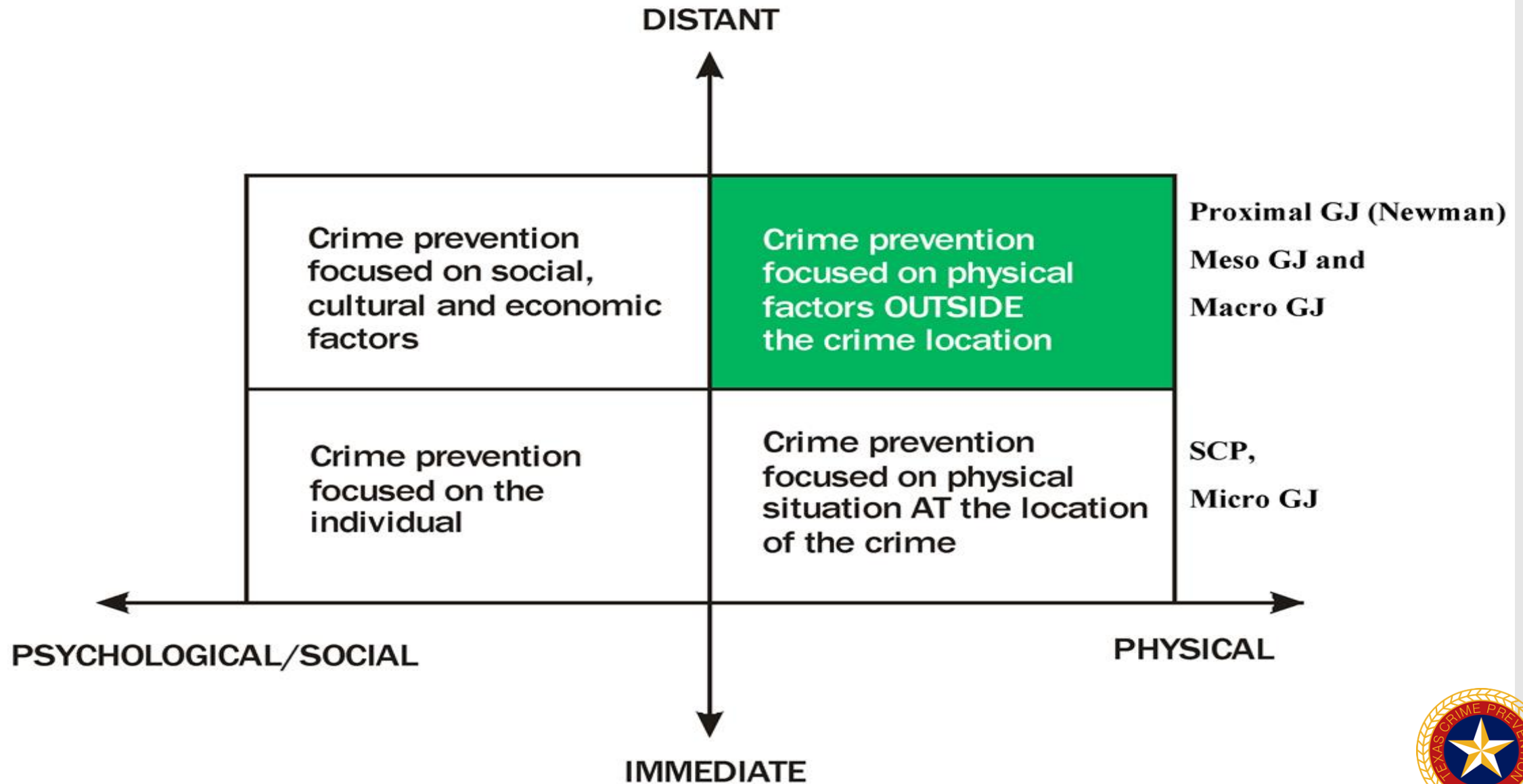
- Two further approaches to crime prevention:
 - **The social (human):** is focused on the social and economic causes of crime and on minimizing the supply of offenders.
 - **The environmental (physical):** modifies the physical environment to reduce opportunities for crime and includes situational crime prevention and CPTED



Four Categories of Geographical Juxtaposition

Geographical Juxtaposition	Location	Comments
Micro GJ	GJ factors acting AT the crime location	For example, situation crime prevention measures.
Proximal GJ	GJ factors acting from locations proximal or contiguous to the crime location.	For example; an alcohol serving premises located near a residence that would potentially attract or generate crime locally
Meso GJ	GJ crime factors originating in areas from proximal to the crime location to physically most distant to the crime location.	Effects ranging from the above alcohol serving premises, to distant factors such as a nightclub area in a city could influence crime in that residential suburb.
Macro GJ	GJ factors act as remote influences on crime regardless of the location of their origin in terms of physical distance from the crime location.	



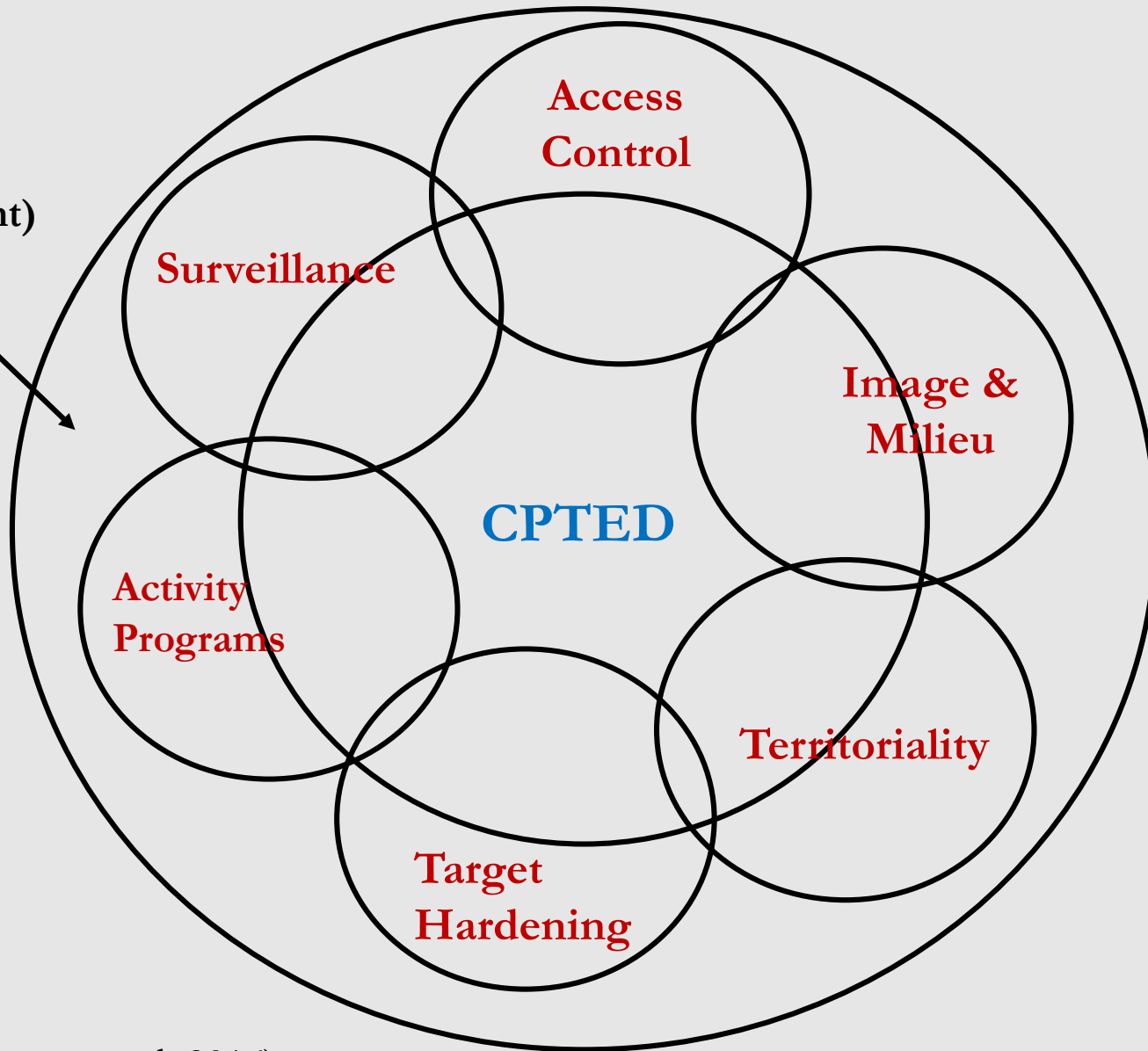
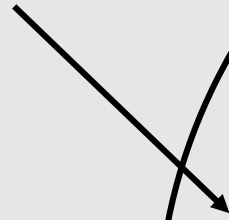


Other Terms Referencing GJ

- **Crime / Attractors:** Particular places or neighborhoods to which strongly motivated offenders are attracted due to the known opportunities for particular types of **crime**. Examples might include bar districts, prostitution areas, and drug markets.
- **Defensible Space:** Is defined as “a residential environment whose physical characteristics – building layout and site plan – function to allow inhabitants themselves to become key agents in ensuring their security”
 - Criminologist Oscar Newman gives Four (4) Factors to create defensible space:
 - Territoriality
 - Natural Surveillance
 - Image
 - Milieu (surroundings)



**Geographical
Juxtaposition**
(wider environment)



A Revised CPTED Model (Cozens et al. 2016).



Practical Examples of GJ and Crime Prevention

- **Mixed-use or land-use heterogeneity:** These terms may include land use that is 95% residential and 5% retail but it could be 25% residential, 25% retail, 25% industrial, 25% transportation.
- Two views on the relationship between mixed use land and crime:
 - “More eyes on the street” as a result of land use mixture reduces crime. (no evidence supporting)
 - Mixed use land reduces the extent that citizens perceive spaces as their own and levels of informal social control are lower, thus increasing crime since the capacity to identify and challenge strangers is diminished.



Practical Examples of GJ and Crime Prevention

- **Liquor Stores / Bars:**

- Street blocks containing bars and liquor stores experienced more crime than blocks without them.
- Assaults and violent crime were associated with the density of retail liquor stores and wine stores. Studies have reported a spatial relationship between domestic violence and liquor stores.
- Studies have shown more violent and property crime near liquor stores. Exposure to bars was positively associated with violent crime and property crime, as well as with disorder.

- **Transit:**

- Transit Centers have been linked to increased crime risks. In large cities with subway stations it has been found to attract street robberies. Studies in 2015 show how public transport can influence the geographical distribution of crime.
- Transport land uses therefore act as nodes and paths for crime to travel.



Practical Examples of GJ and Crime Prevention

- **Retail:**

- Fast food restaurants and convenience stores have been shown to attract crime. Significant correlations between money-lending facilities and both property and violent crimes have been reported. Locations with pawnshops present increased opportunities to offenders gathered nearby

- **Other Attractors:**

- Banks, parks, playgrounds, schools, public / low income housing, hotel / motels, non-use of land, etc.



Practical Examples of GJ and Crime Prevention

- **Burglaries:**

- 2011 study found that single housing and commercial buildings exhibited increased risks.
- 2013 study in Los Angeles studied 205 high crime blocks in Los Angeles and reported three key findings:
 1. Areas with residential and commercial uses exhibited lower crime than commercial only areas.
 2. Crime rates were lowest in residential only areas.
 3. Where zoning changes added residential forms to an area, crime reduced more than in places that did not change.

- **Distance Crime extends from attractors / enhancers:**

- Violent crime concentrates and extends about 400 feet from bars
- Subways and bars were associated with violent crime, property crime, and disorder at all distances, decaying gradually.
- Schools were strongly associated with increased disorder.
- Subway stations / transit exposed the surrounding environment to increased crime for up to 1200 feet away.



GJ and Routine Activity Theory

- Evidence indicates crime comes about from the geographically based juxtaposition of the routine activities of criminals, victims, and guardians.
- The geographical juxtaposition of high crime neighborhoods and the density of local offenders will also be important in assessing crime risks at a specific location.
- Theories on offender location argue criminals commonly commit offenders at locations that are within relatively short distances (within one mile) of where they live.
- Crime generators, attractors, detractors, radiators, absorbers, and reducers are all GJ issues, which affect local crime risks.



Ways GJ May Influence Local Crime

Influence on Crime and Public Order	The Potential Influence of GJ
1. Dilution and concentration	The crime rate for any location may be affected by the activities in the environment nearby.
2. Malign or benign displacement of crime and crime	Crime prevention efforts in a location can displace crime in ways that are more harmful or less harmful. They can also diffuse the benefits of reduced crime nearby areas and vice versa.
3. Behavioral modification	The culture and behaviors of people in one location can influence nearby locations. For example , when behaviors acceptable within a pub are extended to nearby streets. All environments have local cultural cues and social structures.



Influence on Crime and Public Order	The Potential Influence of GJ
4. Motivation/demotivation	The social and physical characteristics specific to a location (or environment) shape the feelings and motivations of individuals at that location. These feelings and motivations in turn, shape their behaviors.
5. Distribution of crime opportunities	Criminal opportunities are increased or decreased by geographically juxtaposed features. For example , burglary opportunities may be increased by the availability of cars in a nearby un-surveilled car park.
6. Nodes acting as crime attractors, generators, detractors, facilitators, enablers, precipitators, absorbers, radiators, and crime reducers	Crime risks in a location can be affected by activity nodes in the nearby environment. For example , crime risk in low crime locations may be raised by crime attractors nearby such as alcohol outlets, brothels, or a transport hub. Should influence CTPED interventions.



Influence on Crime and Public Order	The Potential Influence of GJ
7. Density of offenders	The number and density of offenders who live nearby or who have easy transport access from afar may affect crime rates at a location.
8. Paths and accessibility	Paths, roads, rail, and other travel routes affect the accessibility to a location and the crime rate.
9. Edges	Boundaries (physical/symbolic) of geographically juxtaposed areas affect crime risks as multiple criteria apply at the same location and this results in reduced informal social control, increased variety of crime risks and increased variety of crime opportunities.
10. Presence of capable guardians	Land uses and local population demographics in geographically juxtaposed areas may influence the number and density of capable guardians available at any location.



GJ and Crime Risk Assessments

- GJ provides a more complete understanding of the potential sources of crime risks nearby
- It provides a more justifiable means to help identify the types of crime most likely to occur when crime data for a site is either not available or is less than robust
- It provides a basis to identify the most appropriate boundaries to use for a CRA, since these may not always be the same as the physical site boundaries
- It enables the identification of feedback effects between the site and the surrounding environment that may increase or reduce crime risks
- It provides insights and guidance to help identify which CPTED methods are likely to be most appropriate and effective
- It helps to identify whether it is more effective to implement CPTED methods in the surrounding environment as well and/or instead of to the site/location to reduce crime risks in the site.



GJ and Positive and Negative Feedback Loops

- Crime and crime prevention (in this case CPTED) exist as a complex system. This implies the potential for feedback loops that can either enhance the action of the CPTED activities or increase the risks of crime.
- The concept of geographical juxtaposition provides a basis for including, analyzing, and developing CPTED methods to include feedback effects at the micro, meso, and macro scales.
- Every characteristic location exhibits a distinctive pattern of routine activities and perceived opportunities for crime.
- **Boundary Effect:** When two different kinds of land use are situated next to each other, the routine activities and perceived crime opportunities of each permeate across the boundaries—in both directions.
- This feedback process of crime and CPTED changes and outcomes can be positive or negative and can be slow or fast moving or even exponential as in the case of neighborhood decline/collapse.



GJ and Positive and Negative Feedback Loops

- **Positive crime risk feedback:**

- Positive feedback may lead to increased crime rates over time. Why?
 - It occurs when crime risk from the environment increases the crime rates and risk factors at the site, which in turn increase crime and crime risks in the environment, which then affects the site crime risks.
- Similarly positive feedback of successful CPTED can lead to decreased crime rates over time. Why?
 - when reductions in crime from the CPTED site also reduces the crime motivations in the nearby environment, which in turn help reduce crime risks on the site. This has also been referred to as the “halo effect” and “benign” displacement.



GJ and Positive and Negative Feedback Loops

- **Negative crime risk feedback:**
 - Tends to lead to stabilization of crime rates. Why?
 - It occurs when crime risks from the environment increase the crime rates and risk factors at the site, but at the same time the characteristics of the site are opposite and tend to reduce crime and crime risk factors in the environment—or vice versa. This is a common phenomenon and explains why crime rates tend to remain steady over time.
- Where feedback effects are found, it may be effective to apply targeted CPTED methods in the surrounding environment as well as at the site.



GJ and CPTED Methods

- GJ provides an essential and overarching foundational explanation of all crime and CPTED theories.
 - Example: Theft of a purse.
 - What is the GF of the crime opportunity with a person intending to steal? **The Purse**
 - Which CPTED principle would comprise the GF of creating a psychological/habitual barrier between a potential criminal and a target? **Natural Access Control**
- GJ provides an improved explanation of all CPTED methods



GJ and other CPTED concepts

CPTED Concept	How GJ Provides a Simpler Explanation
Territoriality	Territoriality comprises the geographical juxtaposition of the psychological signs of potential defenders between a potential criminal and a target.
Surveillance	Surveillance comprises the geographical juxtaposition of potential guardians between a potential criminal and a target.
Maintenance / Management	Levels of maintenance and repair send the message that the space is cared for and that crime/unwanted behaviors will not be accepted. It provides a geographical juxtaposition of the owners/managers of a space into that space in front of potential offenders.



GJ and other CPTED concepts

CPTED Concept	How GJ Provides a Simpler Explanation
Access Control	Access control is based on the existence and separation of the geographical juxtaposition of two different kinds of spaces: (a) safe and secure spaces with legitimate, private activities with legitimately owned resources; and (b) spaces with higher motivations for crime and risks that threaten to exploit the legitimate activities and resources of the former.
Activity Support	Increased levels of legitimate uses are encouraged so that their geographical juxtaposition potentially reduces crime rates nearby. A historical example is the tradition of locating churches and places of worship in higher crime environments to encourage “better” behaviors nearby.
Target Hardening	Target hardening can be seen as the geographical juxtaposition of a physical barrier between these two kinds of spaces that has high costs to cross, i.e., highly secure doors between a potential criminal and a target.



Four New Principles of CPTED

- GJ is an essential basis for, and explanation of, ALL crime and crime prevention factors;
- CPTED investments should be inversely proportional to GJ factors at a distance;
- The benefits of distance from GJ factors can be achieved by obscuring the perception of criminal opportunities, and;
- The CPTED principle of natural surveillance can be divided into two parts that include **promoting visibility of criminal acts and the obscuration of crime opportunities.**



GJ is the Basis of ALL Crime and Crime Prevention Factors

- Examples:
 - **Micro scale:** Theft of a wallet depends on the geographical juxtaposition of the wallet's location and the hand of the person intent on stealing it.
 - **Macro-scale:** Crime risks at a location depend on the geographical juxtaposition of remote conditions and remote-based potential criminals to commit crime at that location.
 - **Virtual worlds of cyber-crime:** Crime risks depend on the virtual geographical juxtaposition of the attacker's code with the victim's computer data.



CPTED Investment Inversely Proportional to the Distance of GJ Factors

- ALL crime risk factors are essentially GJ crime risk factors.
- At any location, the overall crime risk is the sum of the GJ crime risk factors acting at that location.
- The nearest GJ factors have a proportionally bigger effect than those further away.
- Remember, stronger GJ factor further away may have more influence than a weaker GJ factor whose source is nearer.
- The amount of CPTED investment that can be justifiably invested in reducing crime at any location is always assessed in terms of the overall crime risks at that location



Surveillance Obscuration and Crime Opportunities

- The influence of geographical factors on crime risks at a location depend on the crime opportunities of that location being able to be perceived by potential criminals, primarily during their routine activities.
 - **Two Factors:** Personal Interest, the other geometry (or location related to target)
- A criminals' perception and identification of crime opportunities reduces with distance.
- Many crime opportunities are “obscured” from being perceived by distance of an individual from their home base.
- **Therefore obscuration is a way of artificially creating geographical juxtaposition “distance”.**
 - Example: Hiding valuables in the car = prevention of theft



Extension of CPTED “Natural Surveillance”

- GJ points to a radical refinement in understanding relating to the CPTED principle of natural surveillance and includes two elements.
 - The first is where the traditional CPTED concept of natural surveillance is to **promote visibility and public surveillance** of potentially unlawful activities in urban space.
 - The second is the idea that natural surveillance can, at the same time, **obscure the view of potential crime opportunities and crime targets.**
 - Example: Hiding a laptop in the car.
 - How is this act an extension of Natural Surveillance?



Summary

- GJ is fundamental to the process and application of CPTED and in fact, provides a foundational explanation for all forms of CPTED and all its inter-related concepts.
- One of the most significant and recent changes in CPTED involves designing interventions that are dictated by **crime risks and the contexts of a location**.
- GJ gives context a realizes crime prevention is not a one size fits all practice.
- Another major change in CPTED is its focus on evidence-based principles, designs, and interventions.
- CPTED designs and your recommendations need to be justifiable by research evidence and by data on the local context and conditions.
- You learned about the micro, proximal, meso, and macro GJ.



ROBBERY & BURGLARY PREVENTION



Robbery Facts

- 1,206,836 violent crimes throughout the country. *(2018, FBI)*
- 7,196,045 property crimes throughout the U.S. *(2018, FBI)*
- Victims of those crimes suffered losses estimated at \$16.4 billion. *(2018, FBI)*
- 96,490 robberies with a firearm *(2018, Statista)*
- Strong-arm robberies 108,541 *(2018, Statista)*
- Businesses are robbed 10 times more often than individuals



Robbery Prevention for Business

◦ **Barriers:**

- **Bandit barriers or counter line systems:** secure enclosures that are fabricated from bullet resistant acrylic or laminated polycarbonate glazing and installed on top of teller lines or cashier areas.
- **Transactions windows:** These are typically smaller units that are being installed into individual existing openings. Normally, glass clad polycarbonate glazing can be utilized which can provide higher levels of protection.



Robbery Prevention for Business

◦ **Handling Cash**

- Keep small amounts on hand and advertise that fact.
- Make frequent bank deposits.
- Have a drop safe or time delay safe.
- Vary your deposit times and route.
- Count your cash in a private area.



Robbery Prevention for Business

◦ **Lighting, Lock, Alarms:**

- Have exterior and interior lighting that allows visibility into the store from the street.
- Have an emergency alarm system and test it occasionally to make sure it works.
- Encourage a buddy system signal with a neighboring store in case a suspicious person enters.
- Keep rarely used doors and windows locked.
- Use mirrors, cameras, or one-way glass to observe all areas of store.



Robbery Prevention for Business

◦ **Employees:**

- Have more than one person who can open and close the store;
- Carefully screen employees before hiring. Instruct employees to call the police about any suspicious person who may be hanging around the store; and
- Train your employees how to effectively handle and report a robbery situation.



Robbery Prevention for Business

◦ **Other Recommendations:**

- Arrange the stock to allow clear visibility in the store.
- Set up a signal with the police patrol officer in case of problems.
- Arrange for a security survey with the local police department or security consultant.



If Confronted by a Robber - Business

- Stay as calm as possible. Try not to panic or show any sign of anger or confusion.
- Consider your well-being and that of your employees as the highest priority.
- Do not escalate the incident into a violent confrontation in which someone may be injured or killed.
- Make a conscious effort to get an accurate description of the robber(s)—approximate age, height, weight, type, and color of clothing. After the robber leaves, call the police immediately.



Burglary Prevention Tips

- Install bright interior and exterior lighting to make all openings visible from both the outside and inside of the store.
- Purchase high-quality door locks and use them. Grilles and storefront gates delay entry.
- Use an Underwriters Laboratories listed money safe, bolted to the floor, and visible from the street.
- Know who has a key and restrict access to the front door.
- Install a good quality alarm system to detect unauthorized entry.
- Consider burglar-resistant glass in accessible areas. (Example: Polycarbonate glaze on vulnerable doors)



Burglary Prevention Tips

- Keep areas around the store clean to aid visibility.
- Display the most valuable articles near the center of the store to force a burglar to take the longest possible escape route.
- Keep merchandise displays organized to allow maximum visibility throughout the store.
- Check closets and restrooms before locking up—no “visitor” should be able to stay inside the store after closing hours
- Security surveillance system, which basically consists of a specific type of camera, monitor, time-lapse record



Other Methods to Stop Burglars

- Make it hard to find or remove valuable items
- Make it likely the thief will get caught.
- Get a system that either monitors itself or can be easily checked to make sure it is in good operating condition.
- Record all serial numbers of large-denomination bills.
- Remember Love it Lock it!!!!





INFORMATION TECHNOLOGY

Systems and Infrastructure



How TCP/IP Protocol Works

- **TCP:** Transport Control Protocol
- **IP:** Internet Protocol
- **Purpose:** The purpose of TCP/IP is to guide information from one place to another on a digital network.



Transport Control Protocol

- Developed in 1974 by Kahn and Cerf and was introduced in 1977 for cross-network connections
- TCP was faster, easier to use, and less expensive to implement
- Ensured that lost packets would be recovered, providing quality of service to network communications.



Internet Protocol

- In 1978 IP was added to handle routing of messages in a more reliable fashion
- TCP communications were encapsulated within IP packets to ensure that they were routed correctly.
- Experts quickly realized that TCP/IP could be used virtually for any communication medium, including wire, radio, fiber, and laser, as well as other means.
- 1983, ARPANET was totally converted to TCP/IP, and it became known as the Internet.

















Definitions to Remember

- **LAN:** Local –Area Network spans a small area. Example: single room, building or group of buildings.
- **WAN:** Wide-Area Network is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs)
- **VLAN:** Virtual Local Area Network is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
- **VPN:** Virtual Private Network is an encrypted connection over the Internet from a device to a network.



Seven layers of the OSI model

Layer NO.	Layer	Functions	Methods	Transmit	Receive
7	Application	Communications partner identified, user authentication, data syntax	E-mail, network, software, telnet, FTP		
6	Presentation	Encryption	Encryption software		
5	Session	Establishes and terminates network sessions between devices and software requests	CPU process		
4	Transport	Error recovery and flow control	CPU process		
3	Network	Switching and routing, network, addressing, error handling, congestion control, and packet sequencing	Switcher, router		
2	Data Link	Data packets encoded/decoded into bits	Media access control (MAC) and logical link control (LLC)		
1	Physical	Electrical, light, or radio bit stream	Cables, cards, Ethernet, RS-232, ATM, 802.11 a/b/g		

- **Application** - Data begins at **layer 7** which includes software programs
- **Presentation** – Passed to **layer 6**, which adds data compression, and encryption
- **Session** – passed to **layer 5**, provides mechanism for managing the dialog between two computers
- **Transport** – From 5 it goes to **layer 4** , which ensures reliable communications between machines. Important the information packet changes from data to segments in the Transport Control Protocol (TCP) layer
- **Network Layer** – (IP) **layer 3** is where error control and routing functions are described. The segments are combined or broken into defined-sized packet (IP) layers. Router is an example of layer 3 devices
- **Data link** – **layer 2** is where the means to transfer data between networks takes place. This were detection and correction of errors could occur. This where addressing of exact physical machines with their own **media access control (MAC)** address is found. Network switches are layer 2 devices
- **Physical layer** – **layer 1** includes cable voltage hubs, repeaters and connectors.



User datagram protocol

- **UDP** - Is a protocol that will send the data without error correction and without attempting to resend lost packets.
- **UDP is called a connectionless protocol**, because it does not attempt to fix bad packets. It simply sends them out and hopes they arrive.
- **Real-Time Protocol (RTP)**, work together to ensure that a constant stream of data is supplied for a receiving program to view or hear. RTP is used for audio and video. Typically, RTP runs on top of the UDP protocol.

As an industry default, all network data are called TCP/IP data, whether it is TCP/UDP or RTP



Transport Control Protocol/Internet Protocol Address Schemes

- Each network device has a network card, which connects that device to the network.
- The **network interface card (NIC)** has a MAC address and a TCP/IP address to identify itself to the network. Note: MAC address is hardware assigned at the factory.
- TCP/IP address is assignable and defines where in the network hierarchy the device is located.
- TCP/IP addresses are used to ensure that communication errors do not occur and that the address represents the logical location on the network where the device resides.



Transport Control Protocol/Internet Protocol Address Schemes

- **IP version 4 (IPv4)** - was the original version under which the whole Internet worked until it was determined that the number of available addresses would soon run out.
 - IPv4, addresses are broken down into decimal notation, each address is a series of binary data (ones and zeros)
 - Four groups are combined by decimals using 0 to 255 (a total of 256 numbers). This is known as an 8-bit value.
 - Example address 0.0.0.0 to 225.225.225.225
- **IP version 6 (IPv6)** - can accommodate a very large (virtually infinite) number of connected devices.
 - Replaced this sequence with a 12-bit value (0.0.0.0 to 4095.4095.4095.4095)
 - IPv6 can be represented by a 3 with 39 zeros



Network Device Overview

- **Edge devices:** include digital video cameras, digital intercoms, and codecs. These are the devices that, for the most part, initiate the signals that the rest of the system processes.
- **Wired infrastructure:** is an Ethernet cabling scheme allows devices to compete for attention. It is designed to handle collisions that occur when two or more devices want to talk simultaneously. A network can be segmented by switches and routers to reduce contention.
- **Ethernet:** is defined under IEEE3 Standard 802.3. E
 - Slowest ethernet being 10Base-T (10 Mbps). Fast Ethernet is called 100Base-T and operates at 100 Mbps. Gigabit or 1000Base-T operates at 1 Gbps.



Network Devices Overview

- **Ethernet Wiring:** Using unshielded twisted pair four-pair wiring on RJ-45 connectors
 - Category 5 (Cat5) or Category 5 Enhanced (Cat5E) wiring is used for 10Base-T, 100Base-T, and 1000Base-T (up to 328 ft).
 - Category 6 (Cat6) wire is useful for 1000Base-T runs up to 328 ft. For 1000Base-T connections, all four pairs are used, whereas for 100Base-T connections, only two pairs of wires are used.
 - Cat5, Cat5E, and Cat6 cables use four pairs, where the colors are as follows:
 - Pair 1—white/blue
 - Pair 2—white/orange
 - Pair 3—white/green
 - Pair 4—white/brown



Network Device Overview

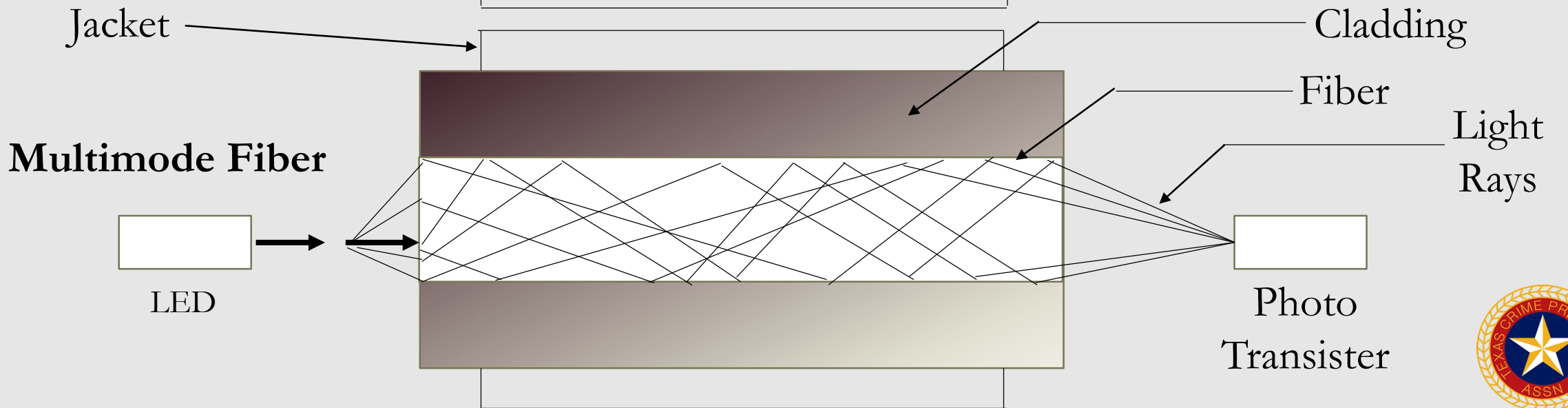
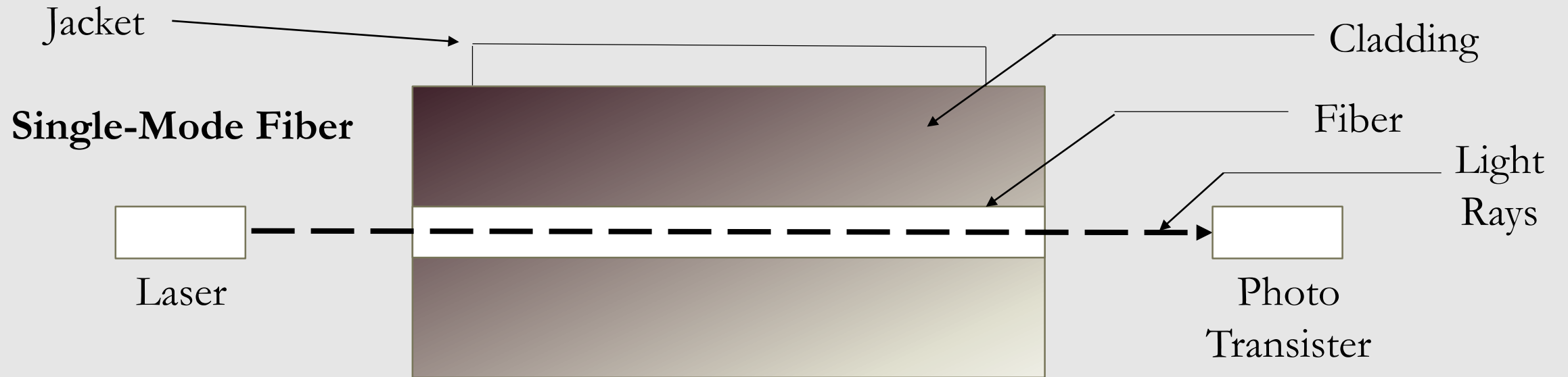
- Fiber Optic: (Communication Media)
 - **Single mode:** based on laser; single-mode fiber is made of glass.
 - It pipes the laser directly down **the middle of the glass tube** like a waveguide. single-mode fiber has a small cross-sectional area (8 or 9 μm) relative to the frequency of the light transmitted through.
 - The laser can carry multiple signals on its carrier. 1550 and 1310 nm frequencies are very common to single-mode fiber. (**Note: 1550 and 1310 are exclusively transmitted in laser**)
 - 43 - 62 miles with economical equipment, high end converters up to 500 mi.



Network Devices Overview

- **Multimode:** use either a laser or a light-emitting diode (LED).
 - Multimode fiber is typically plastic, it has a large cross-sectional area relative to the wavelength of the light transmitted through it, typically either 50 or 62.5 μm (micron) fiber diameter. **It bounces laser or light of the sides of tube.**
 - It has limited distance because the signal is softened or rounded. 850 nm is most used in multimode fiber. **(Note: 850 nm exclusively transmitted in LED)**
 - Limited to 1640 ft for fast Ethernet connections





Network Device Overview

- TCP/IP signals can also be communicated via radio, microwave, or laser. The most common type of radio communication network is in the 802.11 band.
 - **Backhaul:** delivered by 802.11a, 10 channels available and they can all be used in the same airspace.
 - **Client service:** provided by 802.11b/g/i. 802.11b provides 11 Mbps maximum, whereas 802.11g/i provide 54 Mbps. 802.11b/g/i have 13 available channels, but cross traffic is a problem Do not plan to use more than six channels in a single airspace.



Network Infrastructure Devices

- Network infrastructure devices comprise those devices that facilitate the movement of data along the communications media.
 - **Hubs** - A hub is simply a device with Ethernet connectors, which connects all devices together in parallel with no processing.
 - **Switches** - Can read the TCP/IP packet header and direct the signal to the appropriate port(s). Switches are OSI level 2 devices and control where data may go.
 - **Routers** - In addition to directing the traffic of individual ports, they can in fact make decisions about data that is presented to them and can decide if that data belongs on that section of the network
 - **Firewalls**- Firewalls are used with routers to deny inappropriate data traffic from another network
 - **Intrusion Detection Systems** - They continuously monitor the traffic into and out of the network to detect any unauthorized attempt to gain access to the network.



Servers

- Servers process and store data for use by workstations. For security systems, there are several possible types of servers. These may be combined on a single machine or may be distributed across several physical servers.
 - **Directory service server:** Is an index for all workstations to use to find the data for which they are searching.
 - **Archive service server:** stores data for future reference
 - **Program service server:** Allows programs to reside on the server rather than on the workstation.
 - **FTP or HTTP server:** Useful for remote monitoring and retrieval of data from a remote site to a central monitoring station
 - **Email server:** send and receive email



Servers

- **Broadcast server:** Broadcast alerts or alarms to pagers, cell phones, loudspeakers, printers, and so forth
- **Workstations:** Provide a human interface to the network. Workstations can be single purpose or multiuse, serving other types of programs and other networks.
- **Printers:** can be connected to a workstation or directly to the network, where they can serve multiple workstations



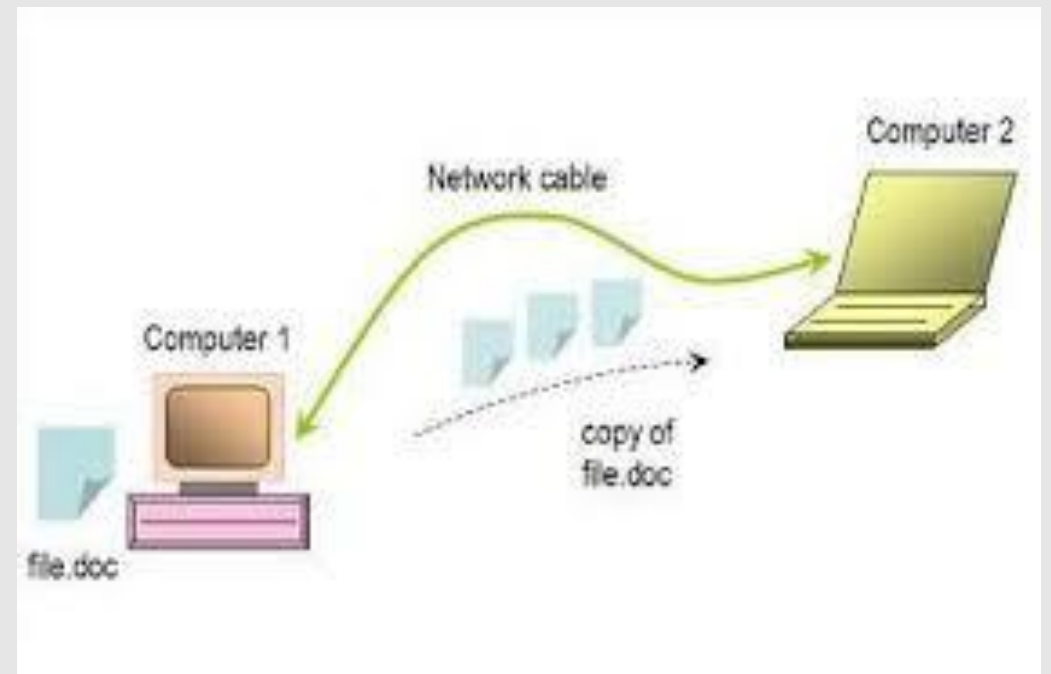
Servers

- **Mass Storage:** Digital video systems can store a lot of data—much more data than any other type of system. It is not unusual to design systems with many terabytes of video storage. Two ways of extending the storage:
 - **Network-attached storage (NAS)** - units include a processor and many disk or tape drives (or a combination of both). They are typically configured to “look” like a disk drive to the system, and **they connect directly to the network**, just like a server or a workstation. This means that a large volume of data traffic is on the network to feed the NAS.
 - **Storage area networks (SANs)** - **is on its own network** in order to separate the vast amount of traffic it generates away from the common network.



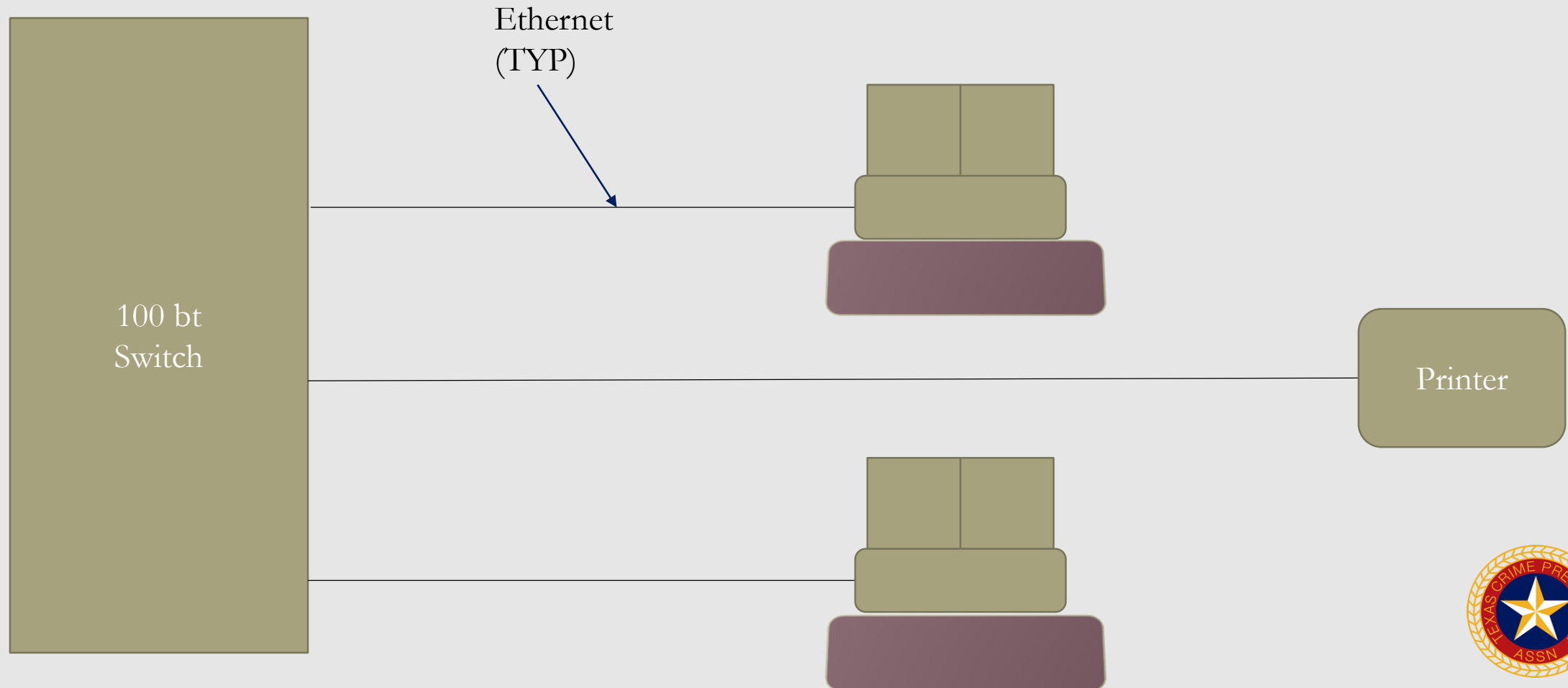
Network Architecture

- **Simple Networks:** The simplest networks connect two devices together on a cable.
 - May connect several devices together on a single switch. This creates a local area network (LAN).
 - May be a single workstation/server (one computer serving both purposes) that is connected through one or more switches to several cameras, intercoms, codecs, access control panels, etc.



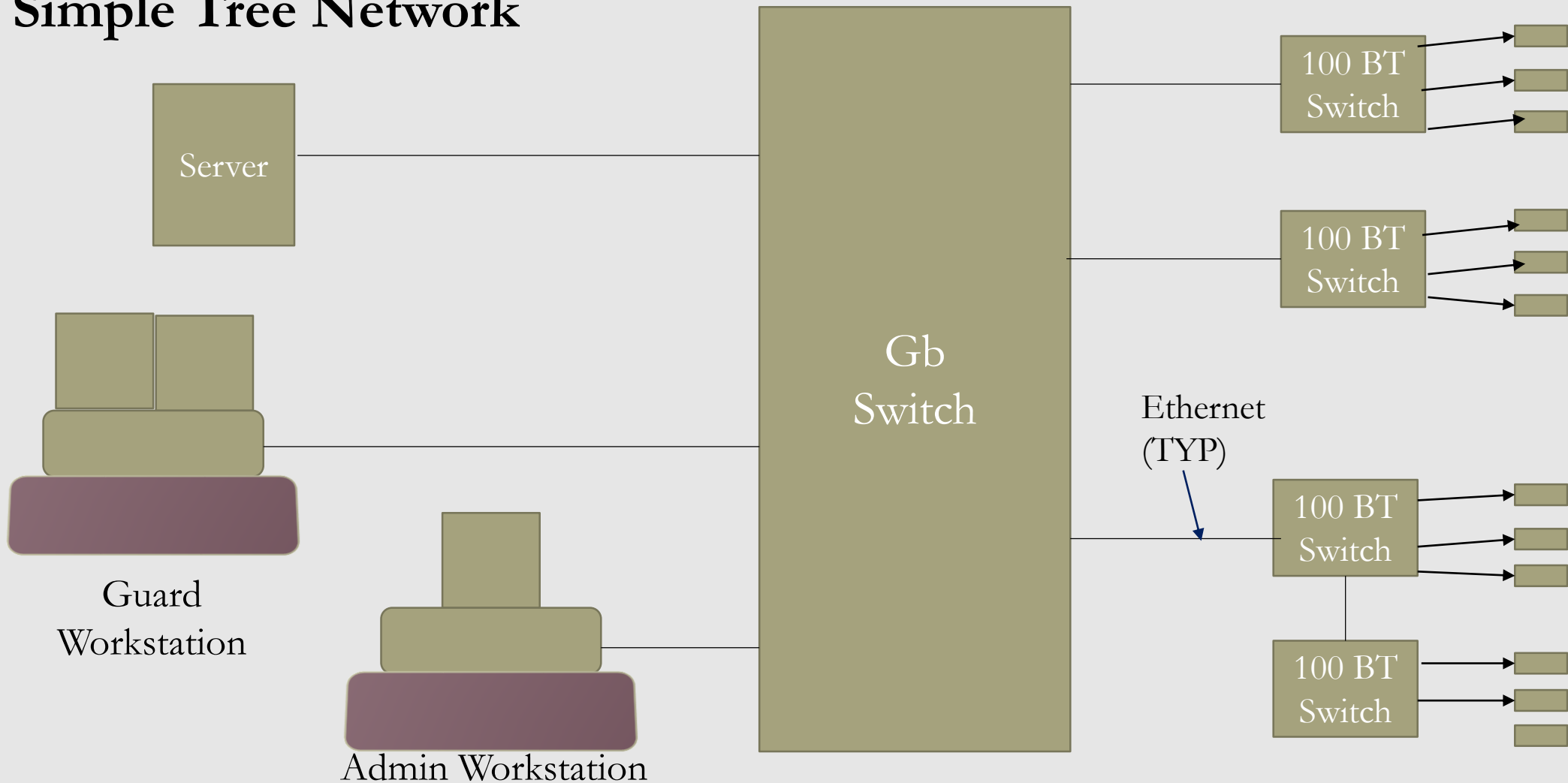
Advanced Networks Architecture

Switch-Connected Network



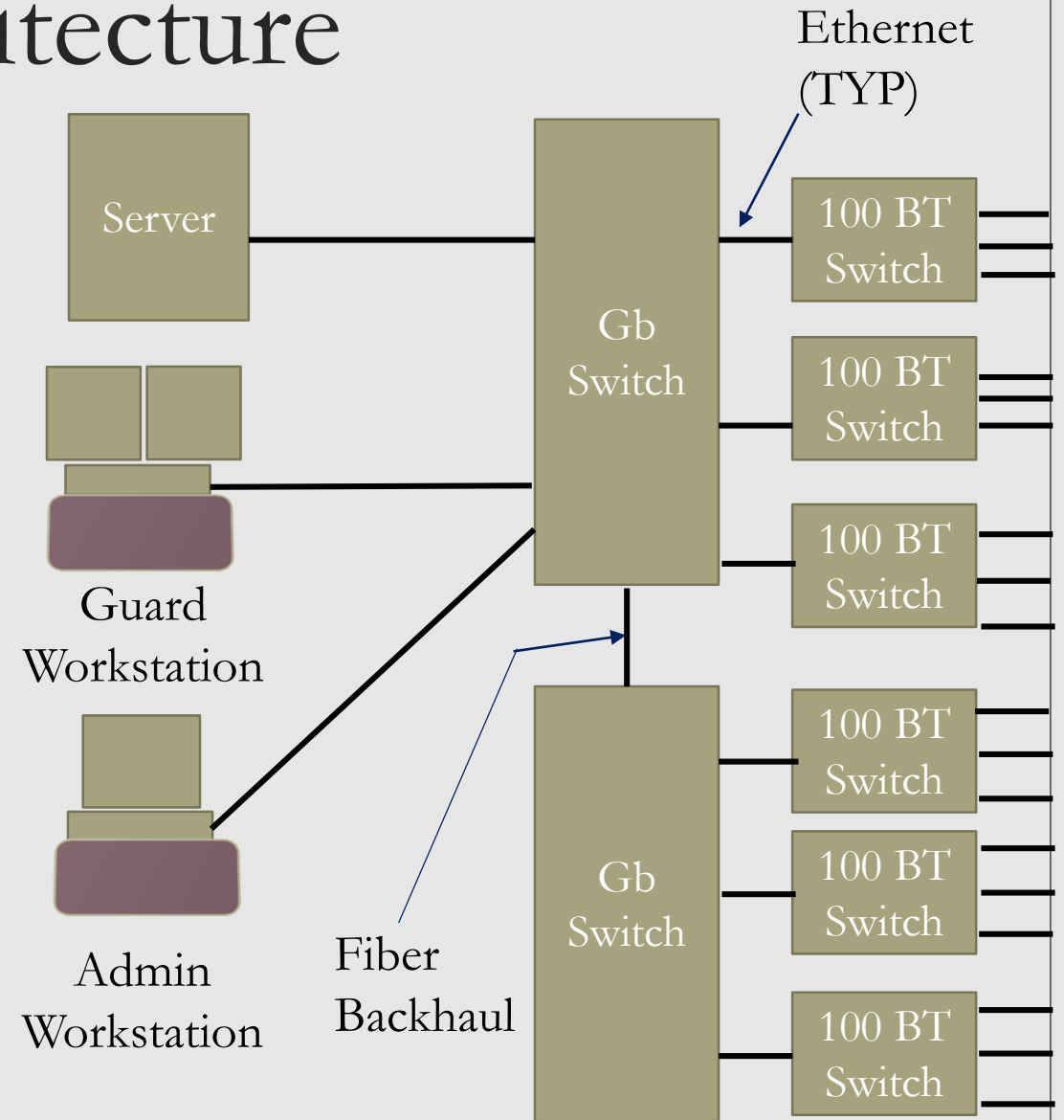
Advanced Network Architecture

Simple Tree Network



Advanced Network Architecture

- **Backhaul Networks:** Beyond simple tree architecture, as network size grows, it is common to create a backhaul network and a client network.
 - A simple gigabit switch is equipped with several fast Ethernet (100 Mbps) ports to connect edge devices, such as cameras, codecs, intercoms, or access control panels, and a backhaul connection that supports gigabit (100 Mbps) speeds.



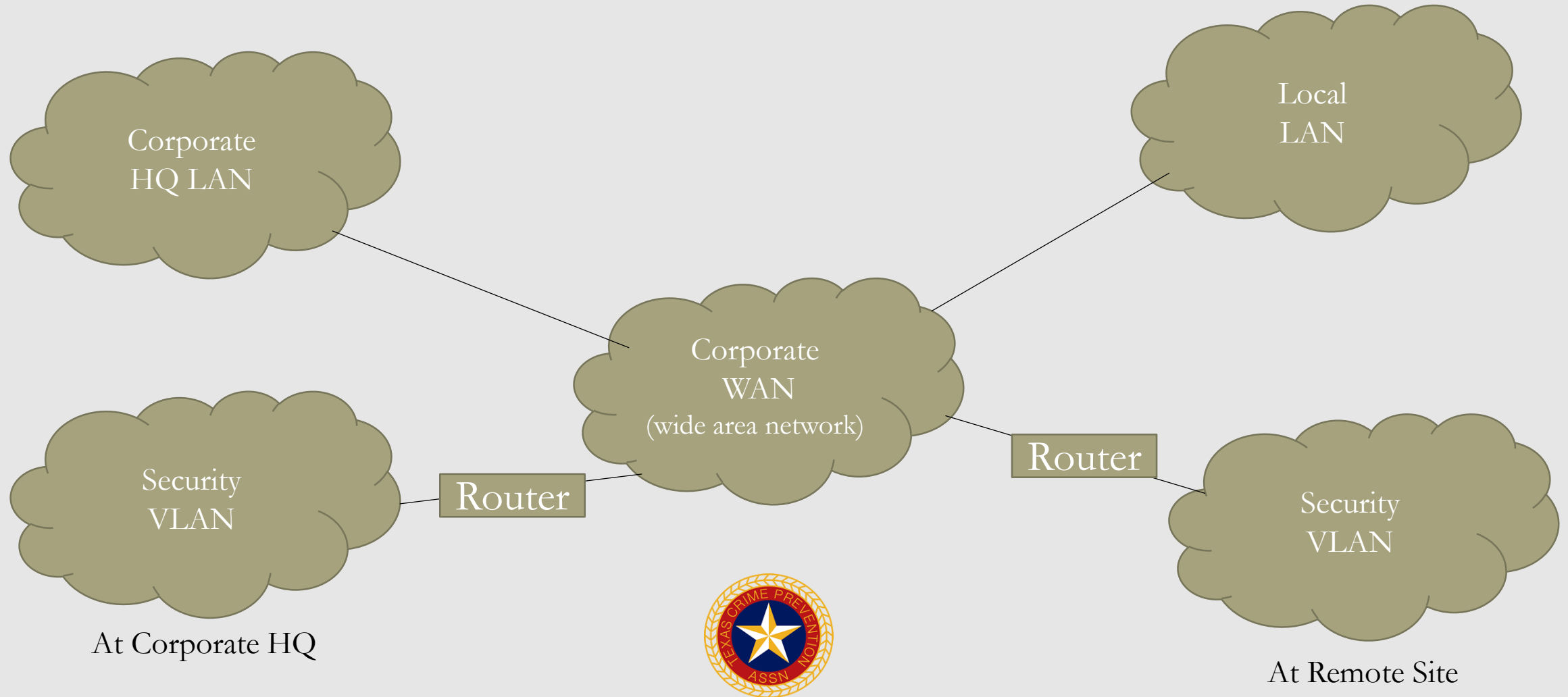
Advance Network Structure

- **Subnets:** Basically a Virtual LAN (VLAN) that is a logical subset of the overall LAN.
 - Subnets limit network bandwidth to manageable levels or minimize traffic that is not appropriate for certain devices.
 - Subnets also limit network traffic
 - **It is recommended that companies do not pipe more than 45% of the rated bandwidth of any device.** Example of why: Because the rated bandwidths are based on normal network traffic and not on streaming data, such as video.
 - A VLAN is created by joining two or more networks by routers. VLAN's are global subnets. VLAN can coexist across the mother LAN



Example

Subnet to segregate network traffic



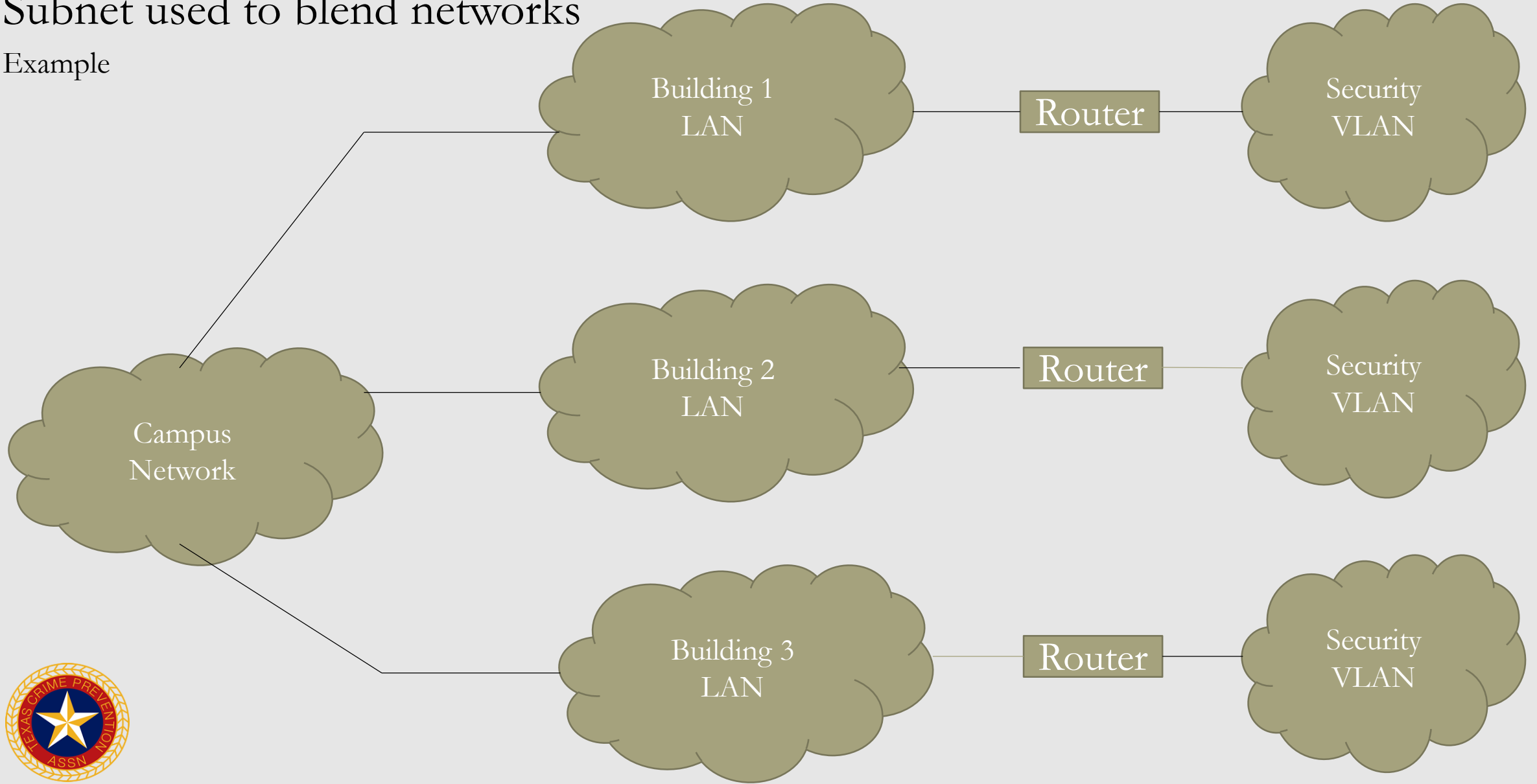
Virtual Local Area Network

- VLANs are global subnets.
- VLAN segregates a data channel for a specific purpose or group.
- Unlike a subnet, which is a hierarchical daughter of a physical LAN, a VLAN can coexist across the mother LAN as a VLAN though there were two separate sets of hardware infrastructure.
- A VLAN operates on a dedicated port to which only the VLAN has privileges.
- Cameras, intercoms, and access control system controllers can be plugged into the same managed switch with workstations and printers of the organization's business LAN.
- When the security devices' ports are dedicated to a security VLAN, those devices will not be apparent or accessible to the users or the LAN.



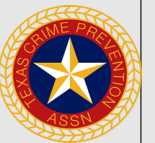
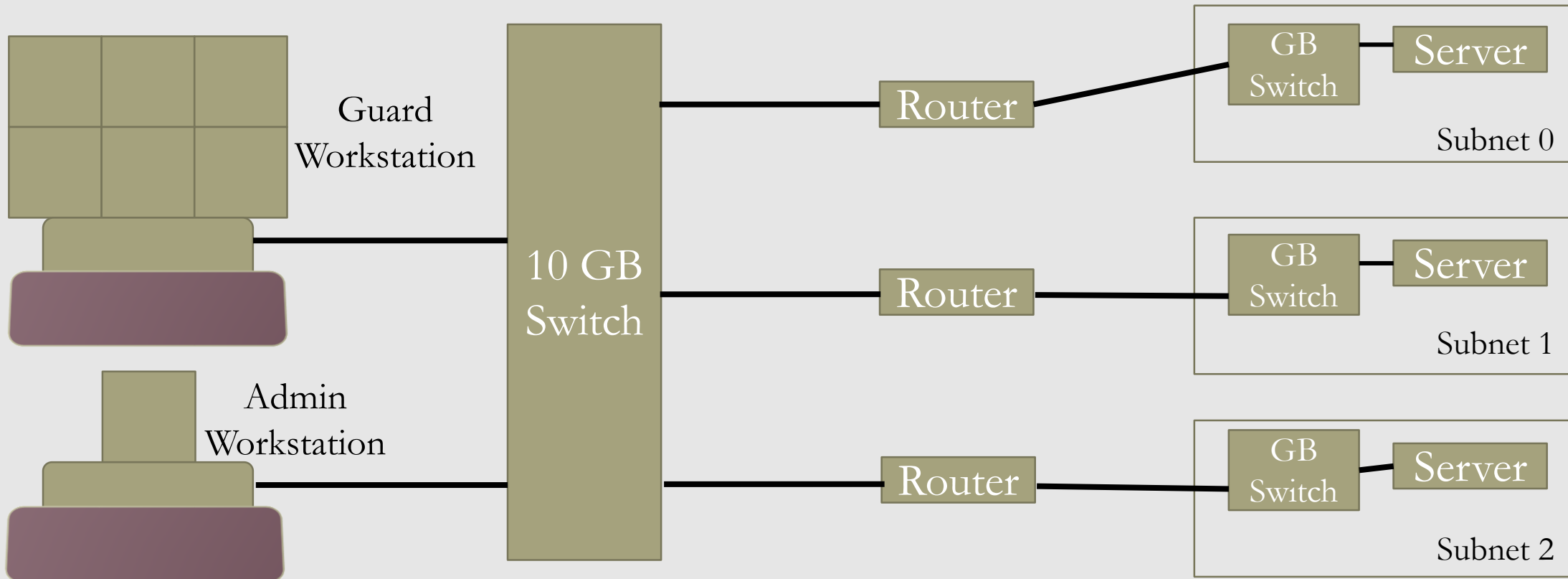
Subnet used to blend networks

Example



Advanced Network Structure

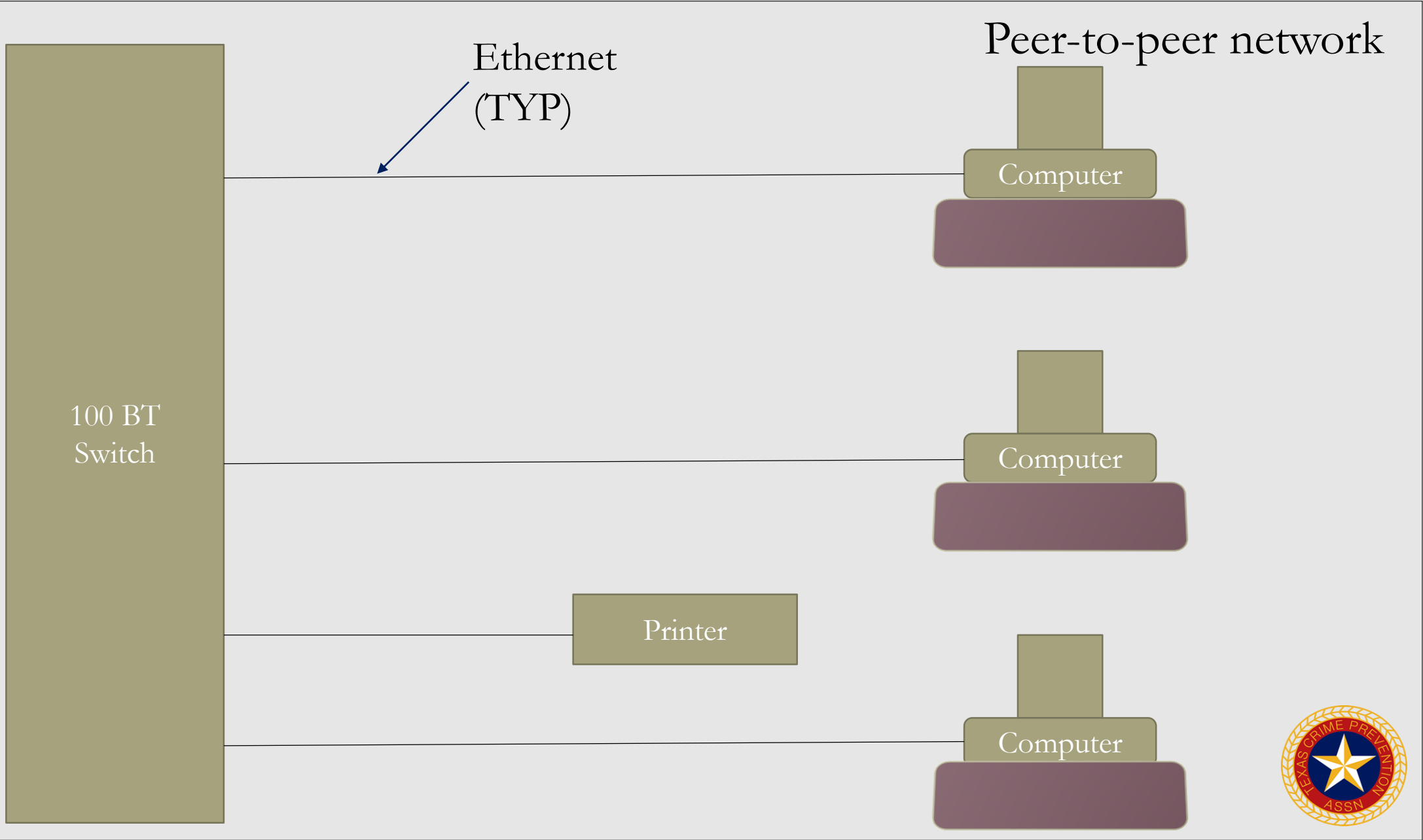
- **Subnets to segregate network traffic:** When a security system serves many buildings on a campus, it is not useful to have the traffic of one building on the network of others.



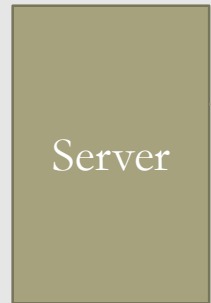
Network Configurations

- **A network is composed of a series of TCP/IP devices connected together.**
 - **Peer to Peer Network:** Peer-to-peer networks are created by connecting each device together through a hub or switch. Each computer, codec, or access control panel is equal in the eyes of the switch.
 - **Client Sever Network:** Major processing is performed in one or more servers, and the human interface is accommodated with client devices or workstations.
 - Cameras, intercoms, access control readers, locks, door position switches, request-to-exit devices, alarm-triggering devices, and so forth are all human interface devices, as are guard and lobby workstations, intercom master stations, and so forth.
 - Human interface devices are connected to processing devices that interface to the network via TCP/IP connection, usually Ethernet. These may include codecs and alarm/access control panels.





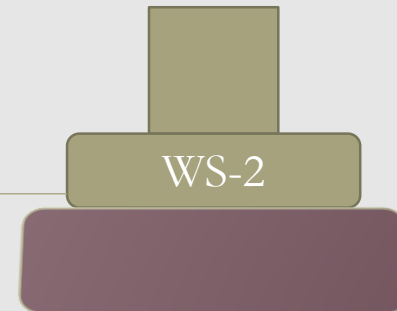
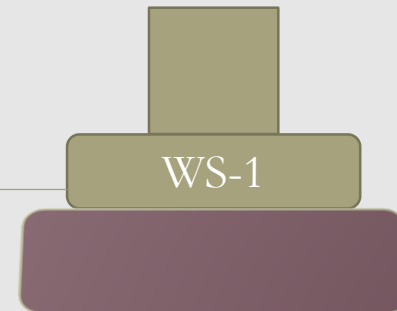
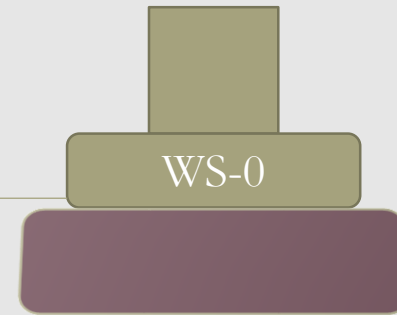
Client/Server Network



Ethernet
(TYP)



Clients

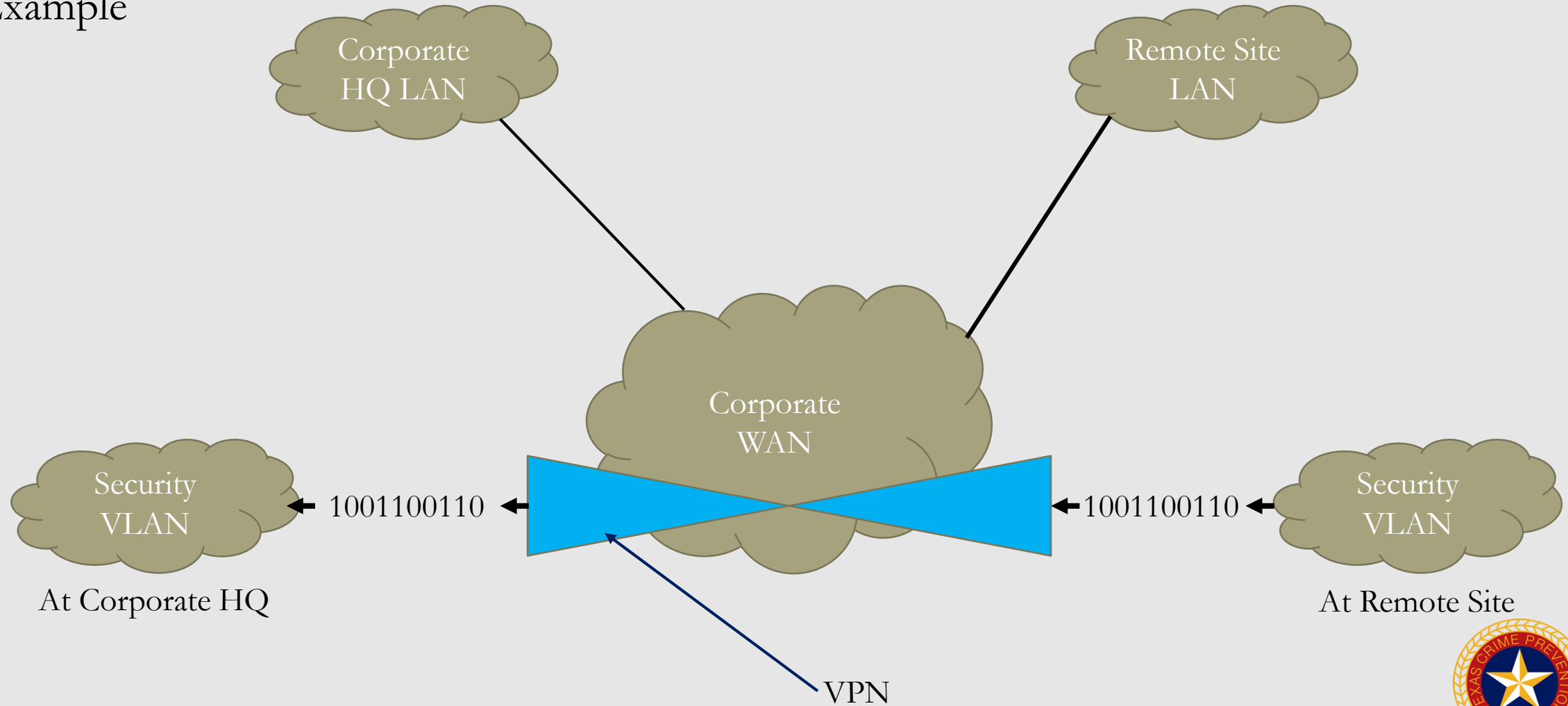


Creating Network Efficiencies

- Two Efficient ways to remotely monitor over a business network:
 - **Browser:**
 - A browser connection is quick, easy, and does not consume any bandwidth when it is not sending data.
 - It consumes only what it displays.
 - They consume data even when minimized, and consume both network bandwidth and workstation processing power
 - Browsers should be run under https rather than http (https is a higher security environment), and secure socket layer encryption is often advisable to ensure the security of the system being monitored.
 - **Virtual Private Network:**
 - A VPN is a tunnel between the server being monitored and the server that is requesting its data. That tunnel is firewalled and encrypted.
 - disadvantage of VPNs is that they utilize a fixed bandwidth



Virtual Private Network Example



System Architecture

- Servers: Servers provide the guidance and direction for the entire system and store its activities and history.
 - Directory Service: directory service provides the routing information to locate cameras, intercoms, and archived video on demand. It also maintains the necessary information for all system devices to communicate effectively.
 - Archiving: Server will typically archive alarm/access control, video, and intercom activity, indexing it by date and time and often correlating video and voice data to alarm and security events so that the operator has immediate access to appropriate video and voice as he or she views alarm activity.



System Architecture

- **Remote Access Services:**

- **Web Access:** A VPN helps ensure data integrity for off-site Web service connections. Remote access from within the domain is often accommodated by use of a VLAN.
- **Email:** These will require exchange server or similar software or a dial-up or Web connection for a pager.

- **Hardware:**

- CPU – Central Processing Unit
- Memory – More is better



System Architecture

- **Disk Storage:**

- **Operating Systems and Programs:** All system servers should be equipped with multiple disks, including two mirrored automatic fail-over drives for operating systems and programs, complete with current configurations.
 - Additional disk slots should be dedicated to data archive up to the server's capacity.
 - External storage capacity should be considered. Tape, Disk, Network Attached Storage, Storage Area Network

- **Workstations:**

- A workstation is a computer used by a person who operates the system
 - Security monitoring/command, guard or lobby, administrative, photo ID, access verification



System Architecture

- **Edge Devices:**

- Edge devices include cameras, intercoms, card readers, alarm detection devices, electrified door locks, and request-to exit detectors.
- These are the devices that interface with the user.
- On a typical integrated security system the edge device connects with a data controller or codec, which converts its native signal (audio/video, dry contact, or data) to a uniform TCP/IP standard.
- The edge devices typically connect to the system through a data switch.



System Architecture

- **Infrastructure Devices:** Between edge devices and servers/workstations is the digital infrastructure, which connects the system together and manages its communication rules.
 - **Switches:**
 - Digital switches are the connection points for almost all system devices.
 - A digital switch is a device that not only provides a connection point but also can manage how each device communicates with the system.
 - Switches are OSI layer 2 devices, but better switches can also perform OSI layer 3 management functions.
 - **Routers:**
 - Routers manage data traffic at a more global level and are OSI level 3 devices.
 - capable of segregating traffic into subnets and VLANs, creating logical separations of data and making communications within the network much more efficient and secure.



System Architecture

- **Firewalls:** A network firewall is a computing device that is designed to prevent communications from and to some devices in support of an organization's network security policy.
- **Wireless nodes:** Wireless nodes are radio-frequency transceivers that support network communications. Often, they also incorporate network switches, and sometimes they can incorporate routers and even firewalls. They also commonly encrypt data placed on the wireless link.
- There are four common speeds of network communications:
 - 10Base-T: 10 Mbps
 - 100Base-T: 100 Mbps
 - 1000Base-T: 1 Gbps
 - 10000Base-T: 10 Gbps



System Architecture

- **Cabling:** Network cabling can be wired or fiber optic. Fiber optic cabling types include single mode and multimode
 - **Wired Cabling:** Cat5E and Cat6 cables are used for network cabling. Both have a native distance limit of 300 ft. Cat5E and Cat6 cables can support 10Base-T, 100Base-T, and 1000Base-T connections, with distance decreasing as the speed increases.
 - **Fiber Optic:** Fiber optic cabling can support faster speeds, longer distances, and simultaneous communications. Unlike wired cable, fiber only supports a single communication on a single frequency at one time.
 - **Multimode:** Multimode fiber uses inexpensive LEDs operating at 850 or 1500 nm to transmit data. Multimode fiber is made of inexpensive plastic.
 - **Single mode:** Single-mode fiber uses more expensive lasers and optical glass. Single-mode communication is right down the center of the glass fiber, never bouncing (thus single mode). Single-mode fiber can stand higher power and thus yields longer distances.



System Architecture

- **Scaling Designs:** Systems can be scaled by creating **subnets**, which can segregate the system based on function or location. This approach allows the master system to have oversight and observation of the activities of all of its subsystems while not allowing the subsystems to see or affect each other.



Process Control Networks

- **Integrated security systems are classified as process-control network**
- Differs from a business network in that it is a closed network, dedicated to a special purpose, and is segregated from the business network.
- The integrated security system may integrate with other types of process-control networks, including building automation systems (BASs), elevators, telephony systems, fire-alarm systems, parking management systems, and vending systems.



More Protocol Factors

- **Unicast Protocols:** commonly TCP/IP, are meant to communicate a signal from one device to another. Verifies receipt of packet data. Used for pure data, such as alarm and access control data.
- **Multicast Protocols:** Such as UDP/IP (*UDP - User Datagram Protocol*) and RTP/IP, (*RTP - Real-time transit protocol*) are used to broadcast data to any number of receiving devices. Does NOT verify packet of data sent. Multicast is widely used for video and audio data.
 - It was designed to support a single source transmitting data to many destination devices
- **Warning!!! Do not confuse multicast protocol with multipath.**
 - Multipath is the phenomenon caused by radio-frequency reflections, and multicast is the distribution of a single digital signal to more than one destination using a single signal to which each receiving device signs up on a subscription.



Summary

- Understanding information technology infrastructure is the basis for a successful integrated security system design
- The TCP/IP suite of protocols is the basis for information technology network systems.
- TCP/IP operates on levels 3 and 4 of the OSI networking model. Data are encapsulated from the application program through the seven layers down to the network wire, sent across the network, and then de-capsulated backup the seven layers to the application on the other end.
- TCP protocol is able to fix bad communications
- TCP/IP is also an addressing scheme. Each network-connected device is assigned a TCP/IP address that identifies its location on the network. Addresses can be assigned automatically or manually.
- Edge devices include IP video cameras, IP intercoms, and codecs.
- Network infrastructure and wiring is connected using hubs, switches, routers, and firewalls.



Summary

- Common wiring schemes include Ethernet and fiber optic cables
- Ethernet is available on Cat5, Cat5E, and Cat6 cable at speeds of 10, 100, and 1000 Mbps or 10Base-T, 100Base-T, or 1000Base-T (gigabit Ethernet).
- Fiber optic runs can be on either single-mode or multimode fiber.
- Single-mode fiber can carry more data farther
- Gigabit switches are often available with fiber connectors to link switches together over long distances, and RJ-45 connectors are used for short runs of Ethernet cables to local devices.
- Edge devices include IP video cameras, IP intercoms, and codecs
- Hubs are rarely used today, because they simply connect wires together and do nothing to handle network contention.



Summary

- Switches handle the connection of local devices.
- Routers control where network communications can go.
- Firewalls exclude unauthorized devices from gaining access to the network. IDSs monitor the network firewall to detect any attempt to intrude into the network.
- Integrated security system network computers include servers and workstations.
- Servers can include directory service servers (Windows directory service), IISs, DNS, and other network management services.
- Other services may include archiving, application program service, ftp, http, e-mail, and broadcast services.
- Workstations provide the interface between users and the network.
- Printers and mass storage systems round out the network-attached devices



Summary

- Network architecture includes simple networks, LANs, and WANs
- Advanced network architecture includes backhaul networks, subnets, and VLANs.
- Network connection types include peer-to-peer and client/server configurations.
- Systems can be monitored remotely and safely using browser (http) or VPNs.
- Digital cameras can link directly to the network, whereas analog video cameras require a codec interface.
- Workstation types include security-monitoring centers, guard or lobby-desk workstations, administrative workstations, photo ID workstations, and access-verification workstations



Summary

- Integrated security systems can interface to many other types of systems, including process-control networks, BASs, elevators, PABXs, VoIP systems, fire-alarm systems, public address systems, parking-control systems, and vending systems.
- Multicast protocol is sometimes used in digital video systems, but it is fraught with many nuances requiring special skills and knowledge.





MULTI-RESIDENTIAL SECURITY

Apartments / Hotel and Motels



Common Characteristics of Multi-Residential Communities

- **Planned Communities:** Central Parks, Jogging paths, swimming pools, club houses, golf courses, tennis court, multi-use facility with retail, dining, and night-life...etc.
- **Common selling points:** Luxury, 24-hour security, access control, state-of-the-art security, safe for professional women...etc.
- **Issues to look for during a survey:** poor lighting, lack of no trespassing signs, poor or broken gates, defective pedestrian gates, overall poor maintenance.
- **Common Complaints:** Centering on noise, pets, children, and parking. Depending on area criminal intrusion is a big problem.



Apartments

- **Texas Apartment Association (TAA):**

- Been advising its membership (apartment owner/operators) of tenant security needs. TAA created “Security Guidelines for Residents” (Form 87-M) to be attached to tenant leases which provides 30 crime prevention tips.

- TAA also created a “red book,” which has an extensive section on security with useful security recommendations:

- **“Red Book” Recommendation:**

- educate tenants,

- check exterior lighting weekly,

- keep vacant units locked,

- install dead bolts and peepholes and strengthen striker plates,

- protect master keys,

- screen employees.



Apartments

- Failure to warn tenants of criminal activity is considered negligence in many jurisdictions.
- Apartment leases alerts tenants to their “**security rights**” under **Section 92.151, and following sections, of the Texas Property Code.**
- TAA provides a sample form for notifying Texas tenants of crime. This form calls for identification of the type of crime, such as rape, murder, robbery, or burglary.
 - **Note:** *The TAA form uses the phrase “in the immediate area of the apartment[s]. This notice concludes, “Please remember that your security is the responsibility of yourself [sic] and the local law enforcement agencies.”*
- You must consider low-income housing (Section 8)



Condominiums

- Unlike apartments Condo / Townhomes are owned not rented
- The Community Associations Institute (CAI) is the major organization serving the condominium community.
- **Common Issues:** Poor Lighting, overgrown shrubs/trees, broken access control devices
- Probably nothing causes more hostility in condominium projects than parking regulations.
 - **Recommendations:**
 - Add visitor parking spaces
 - Issue parking cards to residents / window stickers
 - Offer visitor passes
 - Clearly mark fire lanes and loading zones



Levels of Security for Multi-Residential

- Three Lines of Defense:
- Outer Perimeter:
 - Entrances and exits, bordering green belts, undeveloped property, woods, roadways etc.
 - Special Hazard: two, three, or four different types of property, located on various sides, may have to be considered.
- Common Areas:
 - roadways, / parking lots,
 - marinas,
 - Lawns / walkways
 - recreational areas
- Building / Units:
 - Windows, balconies, doors



Involving Tenants and Owners

- It is incumbent on all citizens to report problems and become our “eyes and ears”
- Recommend apartment / condo watch and encourage regular personal safety and crime prevention meetings for residents.
- Tenant Screening: Recommend a service company willing to check on applicants for a fee. Subscribers are urged to provide regular information on “tenant performance” and any lease violations.



Physical Security and Hardware

- **Recommendations:**
 - See Through Fencing which encloses the perimeter at 8' high.
 - Limit vehicle traffic with working gates
 - 3 common gates:
 - Barrier arm
 - Metal slide / metal swing
 - Pop-up gates
 - Control Pedestrian gates code locks, access control cards, or keys
 - Lock and Doors (same as residential)





Pedestrian Gate



Sliding Metal Gate



Pop-Up Gate



Metal Swing



Barrier Arm



Physical Security and Hardware

- **Recommendations:**

- **Key Control:**

- An adequate key control system requires an overall plan and the proper selection of locks and key blanks, blind key codes, and comprehensive records
 - Locks should be changed or rekeyed when a new party moves in or if a door key is lost.
 - Records of key changes or lock swaps, from one door to another, must be accurate and up to date
 - Key machines and blanks and key lockers require close control
 - If management requires an extra key to open units in an emergency, keys should be kept in a sealed packet or special onetime plastic key box. This way a key cannot be removed without clear evidence of the action.



Physical Security and Hardware

- **Recommendations:**

- **Windows / Sliding Glass Doors:**

- Auxiliary locks for windows / sliding glass doors

- **Visitor Intercoms:**

- May be audio (voice only) or audio and video, electric door strike to allow remote access

- **Video Intercom System:**

- A video intercom system, including a telephone for verbal communication, allows the resident to see who requests entry and to speak with that person



Traffic Calming

- **Speed Bumps**

- **Recommendations:**

- design discourages speeding but minimizes vehicle damage. It is not necessary to use narrow, steep bumps
 - Speed bumps should have a gradual slope and at least one-foot width (at the top)
 - Notice of their presence should be posted at each vehicular entrance
 - Speed bumps should be painted, or striped, in yellow or international orange,
 - Openings for bicycles are recommended.





Special Areas of Vulnerability

- **Day Care Centers**

- **Considerations / Recommendations:**

- Access control is critical as well as panic buttons in staff areas.
 - No one should be able to walk into the facility without prior approval
 - Children be released only to approved persons

- **Elevators and Lobbies**

- **Considerations / Recommendations:**

- Elevator lobbies should be in plain view and not screened by vegetation
 - Elevators and lobbies should be well lit, day and night
 - Mirrors should be placed in each elevator so that a user can see if anyone suspicious is already in the elevator
 - Alarm buttons connected to the resident manager's unit



Special Area of Vulnerability

- **Laundry Room**

- **Considerations / Recommendations:**

- Location is too in a remote part of the complex: Ensure proper lighting add security cameras
 - Laundry room lack Access Control: Key code or allow access only through a resident key, key card or fob.
 - Laundry room door has no window; Replace the door adding a window lite.

- **Pools / Outdoor Water**

- **Considerations / Recommendations:**

- All residents must be warned about water dangers
 - Local ordinances usually require that pools be fenced. (Minimum 8’)
 - In the case of units adjacent to water, it is prudent to install a fence, at least around the back of such units.



Basic Step in Mutli-Residential Security

- Physical security survey (including measurement of lighting)
- Tenant attitude survey on security and crime
- Recognition of vulnerable populations and places (such as women living alone and laundry rooms)
- Analysis of area and on-site crime types and patterns
- Analysis of tenant/owner's complaints about crime and security
- Honest reporting of crime problems and what security is provided tenants/owners
- Honest reporting of crime and changes in provided security to tenants/owners
- Written security program, including use of personnel, physical (hardware), and procedures—perimeter and interior control
- Scheduled regular evaluation of crime risks and the state of provided security
- Good local police liaison,
- Daily evaluation of security/courtesy logs and reports



Hotel / Motel Guest Security

- **Update Locks:**
 - Have Locks that can track who goes in and out of rooms can serve as a deterrent to theft. (internal theft)
 - include automatic deadbolts, which can better prevent external threats from thieves, or systems that eliminate the need for master keys.
- **Safety Meetings:**
 - Have regular safety meeting
 - Schedule time to talk about guest safety.
 - Watching training videos, such as those produced by Safety Source Productions.
- **Monitor Activity with Cameras:**
 - Have cameras being watched 24 /7 if possible
 - Coupled with software, video cameras can now recognize activity in an area and provide an alert.
 - Add third party monitoring



Hotel / Motel Guest Security

- **Evaluate and Improve:**

- Conducts weekly reviews of the property and have checklists for staff to ensure areas, such as stairwells, are clean, safe, and well lit
- Act swiftly to address issues found don't wait

- **Meet and greet:**

- Most effective, ways of securing a property is to provide excellent customer service. “Engage customers you encounter,”
- Educate employees about safety
- Employees should also look out for people who don't fit the profile of the hotel's typical guest.



Theft & Fraud: Monitoring Employees

- **Provide a sense of ownership:**
 - One method to promote such ownership is instituting some form of profit sharing.
- **Boost employee empowerment:**
 - Have an anonymous tip line, where employees can report theft or threats to guest or staff safety
 - When an employee sees anything unsafe or unsecure on the property, have a work order system in place that treats these reports with priority.
- **Smart Staff:**
 - During the hiring process, conduct drug screening and criminal background checks.
 - Explain that there are controls in place to monitor theft and fraud
 - When handling cash have two employees
 - Add active monitoring to employee only areas



Cybersecurity: Protecting Electronic Borders

- **Connect IT and Security Departments:**

- information technology and security departments of any property should work together
- place the two departments under the same manager and same budget.
- the two departments should conduct regular security meetings, perhaps as often as once a week.

- **Upgrade to VLAN:**

- WiFi that's directly connected to your property's servers can pose a risk and provide easy access for savvy hackers.
- Install a VLAN with one wireless network for guest and another for staff

- **Beware of social engineering:**

- Social engineering and physical hacking of hotel computers pose a significant risk. Example: Employee gives up a security code.
- Change passwords every three months.



CPTED Considerations for Hotels

- Ability to see persons on an elevator at lobby level from the front desk.
- Entrances well-lit and designed to eliminate hiding spots
- Guest room corridors well-lit and without areas in which a person might hide.
- Lighting on the exterior of the structure that will not be screened-out by landscaping or building features.
- Pathways / Walkways well marked and lighted using Territorial Reinforcement.





Thank you
For
Attending