|  |  |
| --- | --- |
| **TEXAS CTE LESSON PLAN**  [www.txcte.org](http://www.txcte.org) | |
| **Lesson Identification and TEKS Addressed** | |
| **Career Cluster** | Law, Public Safety, Corrections, and Security |
| **Course Name** | Federal Law Enforcement and Protective Services |
| **Lesson/Unit Title** | Overall Role of Security Systems |
| **TEKS Student Expectations** | 130.341. (c) **Knowledge and Skills**  (6) The student explains risk management principles as they apply to security functions for the protection of assets.  (A) The student is expected to describe the sources of natural, intentional, and unintentional threats such as information assurance, computer security, cybercrime, human trafficking, border security, and domestic and foreign terrorism  (B) The student is expected to present examples that depict potential physical, electronic, procedural, and personnel vulnerabilities  (C) The student is expected to summarize the concept of risk management from a local, state, federal, and national security perspective, including the importance of knowing what to protect and the consequences of loss and  (D) The student is expected to explain how security operations and the criminal justice field interface and rely upon each other |
| **Basic Direct Teach Lesson**  (Includes Special Education Modifications/Accommodations and  one English Language Proficiency Standards (ELPS) Strategy) | |
| **Instructional Objectives** | The students will be able to:   * Describe the sources of natural, intentional, and unintentional threats * Present examples that depict potential physical, electronic, procedural, and personnel vulnerabilities * Summarize the concept of risk management from a security perspective, including the importance of knowing what to protect and the consequences of loss * Explain how security operations and the criminal justice field interface and rely upon each other |
| **Rationale** | Risk management is the most common method used for security control and appropriate organizational spending. Security risk analysis/assessment is fundamental to the security of any organization. It is essential to ensuring that controls and expenditures are fully commensurate with the risks to which the organization is exposed. In other words, it must be determined which security controls are appropriate and cost effective. |
| **Duration of Lesson** | 5 to 6 hours |
| **Word Wall/Key Vocabulary**  *(ELPS c1a,c,f; c2b; c3a,b,d; c4c; c5b) PDAS II(5)* |  |
| **Materials/Specialized Equipment Needed** | **Materials**   * Overall Role of Security Systems computer-based presentation * Overall Role of Security Systems Key Terms * Risk/Threat Analysis Map * Risk/Threat Analysis Map Activity Handout * White board/chalk board * Computers with Internet Access * Discussion Rubric * Group Evaluation Rubric * Individual Work Rubric * Presentation Rubric |
| **Anticipatory Set**  (May include pre-assessment for prior knowledge) | Have the class break into several small groups and brainstorm and discuss the following questions:   * What do you believe the term operational audit means? * Why should accounting procedures be a part of a security survey? * Why are employee/company files significant in security protection planning? * If a security countermeasure costs as much as, or more than, the loss being protected against, does it follow that the security measure   should be discontinued because it is not cost effective?  Use the Discussion Rubric for assessment. |
| **Direct Instruction \*** | 1. Risk Analysis    1. The overall role of security management that includes identifying potential areas of loss and developing/instilling appropriate security countermeasures    2. One part of this process is the security survey, which is used to identify potential problem areas    3. Security services methodologies include       1. One-Dimensional Security – relies on a single deterring factor (i.e. guards)       2. Piecemeal Security – security systems that have individual pieces added to the loss prevention function as the need arises without a comprehensive plan       3. Reactive Security- security systems that respond only to specific events of loss       4. Packaged Security- standard security systems (equipment, personnel, or both) without a connection to any specific threats and with the assumption that packaged systems will take care of all problems    4. There is a range of needs in security services       1. A small business with minimal loss potential or relative ease of defense might adequately be served by one-dimensional security (i.e. a good lock on the door and an alarm system, or a contract guard patrol)       2. As risks increase and become more complex, the effectiveness of the one-dimensional approach decreases, and a more comprehensive security program becomes necessary    5. Security must be based on the analysis of the total risk potential    6. In order to set up defenses against losses from crime, accidents, or natural disasters, there must first be a means of identification of the risks   II. Risk Management   * 1. Management techniques that identify, analyze, and assess risks/threats; if a risk/threat is detected, methods are employed to manage it   2. Begins with threat assessment (identifying vulnerabilities)      1. Many threats to businesses are important to security      2. Specific threats are not always obvious      3. The key is to consider the specific vulnerabilities in a given situation      4. Characteristics of a good security manager are         1. Awareness of all possible risks         2. The ability to assess the system and policies from the perspective of a criminal in order to accurately reduce the vulnerability of company property      5. A thorough threat assessment is comprehensive and accurate, and leads to effective countermeasures      6. After a threat assessment is complete, a vulnerability analysis (aka a security survey or an audit) should be repeated on a regular basis      7. Threats to information systems are divided into three categories         1. Natural Threats – global and environmental; these threats include natural disasters such as floods, earthquakes, tornadoes, hurricanes, and storms         2. Intentional Threats – purposeful and deliberate crimes by an unknown person or group that results in some form of damage; these crimes include espionage, identity theft, computer hacking, and terrorism         3. Unintentional Threats – occur accidentally or by chance (i.e. a person accidentally unplugging a computer cord or reformatting a computer hard disk drive)      8. No system can be truly safe from all threats, but knowing the risks and methods for prevention increases the chance of protection   3. Requires procedures and research to help businesses avoid taking security risks   4. Includes two alternative solutions, which should be complementary      1. Investment in loss-prevention techniques      2. Insurance/Insurance companies         1. Cannot meet the security challenges faced by major corporations alone         2. Have found loss-prevention techniques and programs invaluable   5. Allows risk to be handled in a logical manner by using long-held management principles   6. Requires a good risk-management program that involves four basic steps      1. Identification of risks or specific vulnerabilities      2. Analysis and study of the risks/vulnerabilities      3. Optimization of risk management alternatives (see Section X)         1. Risk Avoidance – a technique used to avoid or eliminate a risk, problem, threat, or hazard         2. Risk Reduction – decreasing the threats to safety and security whenever possible         3. Risk Spreading – decentralizing a procedure or operation so that a security or safety problem at one location will not cause a complete loss (Fischer and Green, 1998)         4. Risk Transfer – removing the risk to the company by paying for the protection of an insurance policy (Fischer and Green, 1998)         5. Self-assumption of risk – planning for the worse by creating a plan for an eventual loss without insurance   4. Ongoing study of security  III. Security Survey   * 1. An exhaustive physical examination of the premises and a thorough inspection of all operational systems and procedures      1. To analyze a facility to determine the existing state of its security      2. To locate weaknesses in its defenses      3. To determine the degree of protection required      4. To lead to recommendations for establishing a total security program   2. Requires an examination of the procedures and routines in regular operation   3. Requires an inspection of the physical plant and its environs   4. Can be conducted by      1. Staff security personnel currently employed by the company      2. Qualified security specialists employed from outside of the company for this specific purpose   5. Some experts suggest that outside security personnel can provide a more complete appraisal because they are more objective and less likely to be blinded by routine  1. Should be completed by persons who    1. Have training in the field    2. Have achieved a high level of ability    3. Are totally familiar with the facility and its operations 2. Includes a checklist created by the survey team in preparation for the actual inspection    1. Serves as a guide for the areas that must be examined    2. Includes locations and departments to be surveyed including       1. Physical location       2. Personnel department       3. Accounting department       4. Data processing department       5. Purchasing department       6. Shipping and receiving department   IV. Report of the Survey   * 1. After the survey is complete a report should be written indicating the areas that have weak security and recommending solutions   2. After the report is complete, a security plan may be created using it as a resource   3. The plan must be revised to find the best approach for achieving acceptable security standards within the indicated limitations; compromise will be necessary in some cases   4. When security directors do not receive their requests, they must work within the framework as best they can   5. When security directors are denied extra personnel, they must find hardware that will compensate   6. Security directors must exhaust every alternative method of coverage before going to management with an opinion that requires this kind of decision   V. Operational Audits and Programmed Supervision   * 1. An operational audit (OA)      1. Considers all aspects of the security operation on a continuing basis      2. A methodical examination, or audit, of operations      3. Threefold purpose         1. To find deviations from established security standards and practices         2. To find loopholes in security controls         3. To consider means of improving the efficiency or control of the operation without reducing security      4. Relatively inexpensive and builds on the security survey      5. Based on the concept of programmed supervision without which the audit would become nothing more than a simple security survey      6. Programmed Supervision (PS) – making sure that a supervisor or other employees go through a prescribed series of inspections that will determine whether the functions or procedures for which they are responsible are being properly executed (Fischer and Green, 1998)   2. Conducted by supervisors who are evaluating their areas of responsibility on an ongoing basis   3. Differs from a security survey which begins by developing a checklist of items that the security team believes are important   4. Conducted regularly and frequently, and once the OA begins, it continues until someone in a position of authority decides that it is no longer necessary   5. Requires supervisors to report physical conditions regularly, as opposed to the security survey which relies heavily on either the proprietary security force or a contractor   6. Uses the management resources of the company  1. The security manager can develop a comprehensive security plan using the information gained from vulnerability analysis, security surveys, and OAs   VI. Probability   1. Involves the chance that something will happen and typically involves the use of mathematics 2. After vulnerabilities are identified by the security survey or the OA, it is essential to determine the probability of loss, even though probability is subjective 3. Then decisions must be made based on    1. How quickly a problem needs to be addressed    2. Data, such as the physical aspects of the vulnerability being assessed    3. Procedural considerations    4. History of the industry’s vulnerabilities   VII. Criticality   1. A term used to help separate vulnerabilities into smaller, specific categories; also means the impact of a loss as measured in dollars 2. Determines how important the area, practice, or issue is to the existence of the organization 3. Measures the impact of dollar loss, which includes    1. Cost of the item lost    2. Replacement cost    3. Temporary replacement    4. Downtime    5. Discounted cash    6. Insurance rate changes    7. Loss of marketplace advantage 4. The expense of security services must be greater than the potential loss of money for a viable cost-benefit analysis   VIII. The Probability/Criticality/Vulnerability Matrix   1. Criticality, like probability, is a subjective measure, but it can be placed on a continuum 2. By using the ranking generated for probability and criticality, and by devising a matrix system for the various vulnerabilities, it is possible to quantify security risks and determine which vulnerabilities merit immediate attention 3. Although some areas of importance may be obvious, some security executives may be surprised to find that other areas are more critical than they first surmised 4. By considering the history of loss and the number and quality of security devices present, it is possible to estimate the probability of a cash theft 5. Criticality should take precedence over probability 6. The security director should implement measures to reduce the threat to the improbable level whenever the measures are cost-effective   IX. Alternatives for optimizing risk management   1. After the security probability and criticality analysis is completed, and the security problems are identified and ranked in importance, the security manager in cooperation with company executives must decide how to proceed 2. There are many risk management alternatives (see Section III, F, 3)    1. Risk avoidance    2. Risk reduction    3. Risk spreading    4. Risk transfer    5. Self-assumption of risk 3. It is unlikely that any evaluation can absolutely determine the cost effectiveness of any security operation 4. A low crime rate can indicate that the security department is performing effectively 5. Security services can also be considered insurance against unacceptable risks 6. Effective security services must be adaptable, changing regularly to accommodate changing circumstances in a given facility 7. Compiling pertinent information is a useful tool for keeping security services current and effective    1. The survey and the report provide a valuable evaluation that shows a detailed and current profile of the firm’s regular activities    2. Texts, periodicals, official papers, and articles in the general press related to security matters especially those with local significance       1. May have immediate importance       2. May eventually reveal and predict risk patterns (i.e. seasonal shifts, economic trends)   3. Litigation, particularly with issues about no or I f inefficient security  *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  none |
| **Guided Practice \*** | *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  none |
| **Independent Practice/Laboratory Experience/Differentiated Activities \*** | 1. Have the students design the standard operating procedures for a business (existing or created) of their own choice. Then have the students exchange their work with another group and develop a list of possible threats or vulnerabilities to their business. This activity can be completed either individually or in small work groups. Use the Individual Work Rubric and/or the Group Evaluation Rubric for assessment. 2. Have students select a location and complete a security survey. This activity can be completed either individually or in small work groups. Use the Individual Work Rubric and/or the Group Evaluation Rubric for assessment. 3. Divide the class into small groups. Give each student a copy of the Risk/Threat Analysis Map Activity Handout and the Risk/Threat Analysis Map. Have students follow the instructions on the Risk/Threat Analysis Map Activity Handout to analyze the Risk/Threat Analysis Map and identify ways the property can be altered to harden security and protect it from potential criminal activities. Students may make a list and/or sketch their ideas. Have the students present their suggested changes to the class. Use the Presentation Rubric for assessment.   *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  none |
| **Lesson Closure** |  |
| **Summative/End of Lesson Assessment \*** | Overall Role of Security Systems Exam and Key  *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*  Accommodations for Learning Differences For reinforcement, the students will create a Main Idea Web illustrating the threats that are possible to a large urban shopping center. Use the Individual Work Rubric for assessment. |
| **References/Resources/**  **Teacher Preparation** | 012382012X, Effective Security Management, Charles A. Sennewald, Security World Publishing, 2011  0205592406, *Introduction to Private Security: Theory Meets Practice,* Cliff Roberson and Michael L. Birzer, Prentice Hall, 2009  0750684321, *Introduction to Security,* Robert J. Fischer and Gion Green, Butterworth-Heinemann, 2008  Threats to Security: In Information Assurance and Security, Purdue University, The Center of Educational Research  Investigator/Officer’s Personal Experience |
| **Additional Required Components** | |
| **English Language Proficiency Standards (ELPS) Strategies** |  |
| **College and Career Readiness Connection[[1]](#footnote-1)** | **Cross-Disciplinary Standards**  I. Key Cognitive Skills   1. Reasoning    1. Consider arguments and conclusions of self and others.    2. Construct well-reasoned arguments to explain phenomena, validate conjectures, or support positions. |
| **Recommended Strategies** | |
| **Reading Strategies** |  |
| **Quotes** |  |
| **Multimedia/Visual Strategy**  **Presentation Slides + One Additional Technology Connection** |  |
| **Graphic Organizers/Handout** |  |
| **Writing Strategies**  **Journal Entries + 1 Additional Writing Strategy** |  |
| **Communication**  **90 Second Speech Topics** |  |
| **Other Essential Lesson Components** | |
| **Enrichment Activity**  (e.g., homework assignment) | For enrichment, the students will research, explain, and present examples of natural, intentional, and unintentional threats. Use the Presentation Rubric for assessment. |
| **Family/Community Connection** |  |
| **CTSO connection(s)** | SkillsUSA |
| **Service Learning Projects** |  |
| **Lesson Notes** |  |

1. Visit the Texas College and Career Readiness Standards at <http://www.thecb.state.tx.us/collegereadiness/CRS.pdf>, Texas Higher Education Coordinating Board (THECB), 2009. [↑](#footnote-ref-1)