San Luis Rey

Case #3 - Scenario Based City Risk Assessment
For Approval by, Professor Randall Nichols – Utica College
Team - The Warriors

Leia Scime’-Stickles (TL)

Ian Malloy (XO)
Stephen Krater
John Ata
Francis Sullivan
Enzi Jauregui

Fallou Thiobane (XO)
Stanley Noneze
John Stechyshyn
Ki Choi
Celenia Santos

Erin Toombs (XO)
Jonathan Calvo
Kagan Helm
Tiffany Washington
Agenda

Executive Summary
City Facts
Existing Security Policies and Procedures
Terrorist Profile
Threat Analysis
Vulnerability Analysis
Initial Risk Assessment
City Disaster Plan
Risk Assessment after Disaster Plan Recommendation
Conclusions
References
Executive Summary
(1 of 2)

• Scenario Based City Risk Assessment of San Luis Rey
• AnonSovereign and AAACU Terrorist Group formed from Syrian Electronic Army (SEA), Anonymous, Sovereign Citizens, Al Asaam Alaikum Cyber Unit (AAACU)
• The CARVER Method is used to rate the Threat targets
• A Vulnerability Assessment Worksheet from the U.S. Department of Homeland Security is used to rate Vulnerability Analysis targets
• The Risk Assessment Probability of San Luis Rey = 30%
Executive Summary
(2 of 2)

• A separate Emergency Response/Disaster Plan Document outlines the Short-Term and Long-Term Procedures and Recommendations of the top Threats and Vulnerabilities as laid out in this Risk Assessment.

• The Disaster Plan also outlines Communication Procedures, Priorities for Response, and Goals for Response.

• The Risk Assessment of San Luis Rey after the Disaster Plan Recommendations = 17 %
City Facts
(1 of 5)

• Founded - 1706
• Location - On a Rocky Bluff above Surco River and Estaban Bay
• Population in 2000: 1,178,340; Metropolitan area: 2,432,680
• Urban Residential Areas and Suburbs - Extend North and West
• City Industries lie along Surco River and South of Estaban Bay
• Four Bridges Connect San Luis Rey to Neighboring city, Thornton, Franklin
City Facts
(2 of 5)

• Economy: Some estimates place Estaban Deep Water Port imports/exports at 70%  
  o Top Ten in US and has a Unique Free Trade Zone
• Tourism also important to San Luis Rey and surrounding area
• New Grand Trunk Telecommunications grown to become top ten telecom and digital service firm in the world
• Net exporter of electricity to a multi-state region
Robert Muller Dam formed Lake Juniper
Lake Juniper Water Station operates one nuclear power station and two hydraulic generators
The San Luis Rey International Airport is served by three international, one national, and three regional carriers
Subway-light rail connects Uptown with Crusader Coliseum, the Cottonland Campus of San Luis Rey State University, the International Airport, and points in between.
City Facts
(4 of 5)

Map of San Luis Rey

Metro Overview
San Luis Rey Police Department - neither trained nor organized for their role in the prevention of terrorist attack

Poor cooperation between local Law Enforcement Agencies and Federal Law Enforcement

Dissemination of information to front line officers - lacking
  ○ No speedy chain of command for intelligence on possible terrorist cells

San Luis Rey’s AirSpace - Temporary security restrictions after 9/11/01, but not permanent
  ○ Lack Standard Operating Procedure between aeronautical agencies
Existing Security Policies and Procedures
(2 of 4)

• Relationship between Law Enforcements and media press is poor - slightly hostile
  o Proactive public information program regarding the threat of terrorism is also poor

• There has not been a full account of all elements of the critical infrastructure nor a written understanding of the interdependencies between these critical asset holders
  o Depth of independent security needs unknown
  o City does not inspect or verify the security procedures of private critical asset holders
  o There is a lack of trust that the confidentiality of such reports will be maintained
Existing Security Policies and Procedures
(3 of 4)

• Significant regional resistance continues to exist within the city’s law enforcement and emergency management divisions
  ○ City is more favorably disposed to working with bordering localities (Surco River Corporation)
• No equipment interoperability, protocol integration, volunteer screening or regular training across jurisdictional boundaries (local, state and federal)
• Building, safety, and zoning ordinances do not require disaster sustainability or regular multiple building evacuation drills
Existing Security Policies and Procedures
(4 of 4)

- Public and private security perimeters of many buildings too small
- Measures to protect first responders, municipal employees, buildings, and food and water supply from bio-chemical attack inadequate
- Security screening procedures for city employment and continuing security assessment of municipal employees inadequate
- Only one level of off-site redundancy exists for critical data resources, computer systems as well as the critical computer requirements of the Lake Juniper Water Authority
  - Inadequate to protect against terrorist attack
Terrorist Profile

- Syrian Electronic Army (SEA)
- Anonymous
- Sovereign Citizens
- Al Asaam Alaikum Cyber Unit (AAACU)
Terrorist Profile
Syrian Electronic Army (SEA)

- Most noted for their damage on financial sectors as well as hijacking websites and defacing them to promote their cause
- Technologically sophisticated though possibly identified
- Their exact location is unknown
Terrorist Profile
Anonymous

- Formerly ‘led’ by Hector Monseguire, aka AnynmoSabu, they have performed countless cyber operations for nearly as many causes.
- The Anonymous group says they are everyone and no one, quoting as a collective that they have nothing in common and anyone can be Anonymous.
- Making it very easy for terrorists to infiltrate their ranks.
Terrorist Profile
Sovereign Citizens

- Known for forging documents, disregarding rule of constitutional law and denouncing their given names
- Have been known to commit ‘paper terrorism’
- Have been known to kill law enforcement officers.
Terrorist Profile
Al Asaam Alaikum Cyber Unit (AAACU)

- كل ما تبذلونه من اسم
- ‘All your name’
- Right-Wing Radicals
- Fundamentalists
Terrorist Profile Survey
(1 of 10)

• Age - **Varies from 18-40**
• Education - **Varies from uneducated to very educated**
• Special Skills:
  o **Cybercrime**
  o **Cyberterrorism**
  o **Terrorism**
  o **Programming**
  o **Weapons Training**
Terrorist Profile Survey
(2 of 10)

• Personal Motivation (Why are you ready to cause harm to others)
  o Politically Motivated
  o To produce change
  o To cause fear

• Organizations Motivation (Why does the organization perceive that causing harm to others is justified and/or effective)
  o The organization is a diverse group of Anti-US, right wing radicals, Muslim fundamentalists, Citizens disregarding the rule of law and the constitution.
Terrorist Profile Survey
(3 of 10)

• Organizations Strategic Objectives:
  o Through the use of cyber-attack and convention attack:
    ▪ Create chaos
    ▪ Destruction
    ▪ Long lasting effects
    ▪ Death

• Does your organization seek to undertake a catastrophic attack?
  o YES

• Does your organization have a reasonable capacity to undertake a catastrophic attack?
  o YES
Terrorist Profile Survey
Target and Attack Modalities (4 of 10)

- Given the motivation, intention, and track record of your terrorist group, what do you consider the most likely target in your community? (These Categories are based on the Department of Homeland Security’s Strategy and Assessment toolkit and are organized most likely to least likely)
  - Information/Communications (Including telecommunication and computers): EMP
  - Other: Panic, Chaos and Long Lasting Fear
  - Public Health: Nuclear Fallout
  - Agricultural Sector: Nuclear Fallout
  - Commercial/Industrial Facilities: Nuclear Plant
Terrorist Profile Survey
Target and Attack Modalities (5 of 10)

- Electric Power System: **Nuclear Plant**
- Banking and Financial System: **ZEUS bot**
- Transportation Centers: **Mass Shootings**
- Water Supply: **gate closure**
- Civic and Social Institutions (including public symbols): **None**
- Emergency Services: **None**
- Government Services: **None**
- Recreational Facilities: **None**

* Is your above selection different if, instead of asking “most likely,” you ask yourself what target when successfully attacked results in the most devastation
  - **NO**
• If a catastrophe is an event that “changes everything for always,” would an effective attack on any particular target result in catastrophic damage
  o Public health as a result of nuclear fallout or radiation poisoning, long term psychological problems due to fear, Information/Communication, Power and electronic devices may never be the same as a result of the EMP attack.

• Even if you consider such an attack unlikely, where would a successful attack produce the broadest and longest-term impact
  o Public health, Electric Power System, Commercial/Industrial Facilities, Information/Communications, Psychological
Terrorist Profile Survey
(7 of 10)

• Which target, if successfully attacked, would make recovery the most difficult
  ○ Electric Power System, Information/communications, Commercial/Industrial Facilities
Terrorist Profile Survey
(8 of 10)

• Given the motivation, intention, and track record of your terrorist group, what do you consider the most likely method of attack in your community? (The following attack methods are based on several chapters in Homeland Security, by Sauter and Carafano. Attack methods are listed most likely to least likely).

  o Attack on Nuclear Power Infrastructure
  o Bombings
  o Sabotage
  o Cyber Attack
  o Drive-by-shooting
  o Hoax
  o Radiological Attack (Dirty Bomb)
  o Industrial Chemical Attack
  o Suicide Attacks
  o High Yield Explosives (i.e. Murrah Federal Building and WTC 1993)
  o Chemical Weapons
  o Biological Attack on Food Supply
Terrorist Profile Survey
(9 of 10)

- Biological Attack using Human Disease
- Ambush
- Assassination
- Kidnapping
- Hostage Taking
- Antiaircraft Missiles
- Hijackings
- Siege
- Nuclear Attack (Stolen Weapon)
Terrorist Profile Survey
(10 of 10)

• Is your selection different if, instead of asking “most likely” you ask yourself what method of attack results in the most devastation? Which of these methods strike you as most catastrophic
  o Nuclear Attack (stolen Weapon) Radiological Attack (Dirty Bomb) Attack on Nuclear Power Infrastructure, Biological on Food Supply, Biological using Human Disease, Chemical Weapons

• Which method, if successfully actualized makes recovery the most difficult
  o Nuclear Attack (stolen Weapon) Radiological Attack (Dirty Bomb), Attack on Nuclear Power Infrastructure, Biological on Food Supply, Biological using Human Disease, Chemical Weapons, Electromagnetic Pulse device
As Alaam Alaikum Cyber Unit (AAACU) is formed based upon segments of the Syrian Electronic Army’s Anti-US and cyber attack sentiments and methods respectively.

AAACU infiltrates the hacktivist Collective ‘Anonymous.’

AAACU begins frequenting Sovereign Citizen (SC) message boards and, using sock puppets and Virtual Private Networks (VPN’s), shares the SC content.

Members of AAACU learn cryptocurrency mining and create a revenue stream.
Gaining popularity in Anonymous by DoX’ing US Federal Agents, members of AAACU begin creating their own Ops. under the title of Anonymous.

By sharing information and hate-speech regarding homosexuals and those who ‘go against god,’ AAACU begins having leverage with Sovereign Citizen’s (SC).

With an increased revenue stream created by mining bitcoin, litecoin, and ppcoins they begin purchasing needed materials to infiltrate and attack the US.
Attack Taxonomy
Cyber and Kinetic threats as posed by AnonSovereign & AAACU (3 of 7)

- Now actively teaching SC’s Anonymous tactics, the AAACU starts infiltrating America’s border. Coming through long routes and taking their time, the AAACU make their way.
- The city of San Luis Rey is chosen as their target.
- SC’s begin receiving materials from AAACU for assembling EMP’s, which are the primary attack against San Luis Rey.
Attack Taxonomy
Cyber and Kinetic threats as posed by AnonSovereign & AAACU (4 of 7)

- All players are on the field, though members of AAACU have not met with anyone yet.
- With everyone in the US, Sovereign Citizens arrive in San Luis Rey under the impression that the AAACU is also spread through San Luis Rey.
- AAACU purchases numerous, high value prepaid cards and delivers them to the SC’s.
- SC’s begin mail ordering shotguns from Texas, US
- SC’s modify the semi-automatic shotguns
AAACU officially releases a video through Anonymous sock puppets to claim the birth of AnonSovereign, spewing forth propaganda and SC sentiments about the US-Constitution.

AnonSovereign (AS) meets in San Luis Rey.

AS purchases its first high-altitude balloon using a dummy-company created with forged documents.

AS tests balloon.

AS begins frequenting chats to learn about Supervisory Control And Data Acquisition (SCADA).
● AS finds a pastebin of code reportedly from stuxnet.
● AS begins sharing this code with Anonymous Members to learn how to use scripts to make the code operational.
● AS advertises how much it owns in cryptocurrency and Anonymous members flock to help with developing the code.
● US-FBI begins finding pieces of a potential threat, DHS is notified.
AS begins testing small EMP devices after choosing a balloon for the SLR attack.

A ballpark is set for a date of attack.
Attack Timeline: AnonSovereign and AAACU

(1 of 5)

0000
- As release EMP balloon outside of town and launches dirty bomb down river into dam

0847
- AAACU & SEA activate ZEUS/ZBOT in infected SLR citizens computers

0913
- Traffic lights shift to the opposite pattern, establishing AAACU’s connection to the system
Attack Timeline: AnonSovereign and AAACU

1000
- ZEUS/ZBOT provides access to bank systems, all accounts are set to $0.00

1015
- Traffic lights start changing sporadically, causing gridlock at major intersections
- DHS & FBI in SLR & SLR Sheriff’s Department are debriefed

1017
- An attempt is made to access SCADA systems of the Dam and Sewage System, city placed on high alert
Attack Timeline: AnonSovereign and AAACU
(3 of 5)

1025
- Agents and Officers move to contain the incidents, placing public on alert

1029
- An EMP device is activated, but detonates over a residential area

1030
- AAACU launch the modified ‘stuxnet’ against the nuclear plant.
Attack Timeline: AnonSovereign and AAACU
(4 of 5)

1040
- An Advanced Persistent Threat is detected in the city computer systems and proactive measures to begin to counter the threat.

1050
- Attempt to destroy cooling systems.

1100
- City placed on lockdown.
Attack Timeline: AnonSovereign and AAACU

1123
- AAACU ceases cyber attack

1730
- Gunmen open fire on motorists at gridlocked intersections.

1748
- Gunmen are shot in a police confrontation.
Threat Analysis
City of San Luis Rey Top Threats

• Cyber - ZEUS/ZBOT and STUXNET
• Nuclear - Dirty Bomb
• Water - Sewage Gate Closings
• Electric - EMP
• Transit - Mass Shootings
CARVER Method

**Criticality** - What are your key node, choke points, and potential causes of cascading failure?

**Accessibility** - How easy is it to access or impact the critical asset?

**Recoverability** - How much time and money would be required to replace or restore a critical asset?

**Vulnerability** - Are there effective methods for securing the critical asset?

**Effect** - What are the adverse consequences that would result from a successful natural or accidental or intentional threat aimed at the critical asset?

**Recognizability** - What is the likelihood that terrorists will recognize the critical nature of the asset?
<table>
<thead>
<tr>
<th>VALUE</th>
<th>C</th>
<th>A</th>
<th>R</th>
<th>V</th>
<th>E</th>
<th>R</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Loss would be mission stopper</td>
<td>Easily accessible. Away from security</td>
<td>Extremely difficult to replace. Long down time (1 year)</td>
<td>Special operations forces definitely have the means and expertise to attack</td>
<td>Favorable sociological impact. OK impact on civilians</td>
<td>Easily recognized by all with no confusion</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Loss would reduce mission performance considerably</td>
<td>Easily accessible outside</td>
<td>Difficult to replace with long down (&lt;1 year)</td>
<td>Special operations forces probably have the means and expertise</td>
<td>Favorable impact; no adverse impact on civilians</td>
<td>Easily recognized by most, with little confusion</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Loss would reduce mission performance</td>
<td>Accessible</td>
<td>Can be replaced in a relatively short time (months)</td>
<td>Special operations forces may have the means and expertise to attack</td>
<td>Favorable impact; some adverse impact on civilians</td>
<td>Recognized with some training</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Loss may reduce mission performances</td>
<td>Difficult to gain access</td>
<td>Easily replaced in a short time (weeks)</td>
<td>Special operations forces probably have no impact</td>
<td>No impact. Adverse impact on civilians</td>
<td>Hard to recognize. Confusion probable</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>Loss would not affect mission performance</td>
<td>Very difficult to gain access</td>
<td>Easily replaced in short time (days)</td>
<td>Special operations forces do not have much capability to attack</td>
<td>Unfavorable impact. Assured adverse impact on civilians</td>
<td>Extremely difficult to recognize without extensive orientation</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: For specific targets, more precise, target-related data can be developed for each element in the matrix.
CARVER
Criticality Targets

- What is it?
  - Target is critical when it’s destruction or damage results in a significant impact on its military, political or economic operations.
  - Factors to consider include Time, Quality, Surrogates and Relativity.
  - These then can be mapped to the Carver Value Rating Scale and its associated impact.
  - Key nodes, choke points, and potential causes of cascading failure are evaluated
CARVER
Criticality Factors

**Time:** How rapidly will the impact of the target attack affect operations?

**Quality:** What percentage of output, production, or service will be curtailed by target damage?

**Surrogates:** What will be the effect on the output, production, and service?

**Relativity:** What is the number of targets and their position in the system or complex flow diagram?
## CARVER

**Criticality Definitions and values**

<table>
<thead>
<tr>
<th>Criticality Criteria</th>
<th>Criticality Scale</th>
<th>Carver Value</th>
<th>Carver Value Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate halt in output, production, or service; target cannot function without it</td>
<td>9-10 “Omega”</td>
<td>5</td>
<td>Loss would be mission stopper</td>
</tr>
<tr>
<td>Halt within 1 day, or 66% curtailment in output, production, or service</td>
<td>7-8 “Alpha”</td>
<td>4</td>
<td>Loss would reduce mission performance considerably</td>
</tr>
<tr>
<td>Halt within 1 week, or 33% curtailment in output, production, or service</td>
<td>5-6 “Bravo”</td>
<td>3</td>
<td>Loss would reduce mission performance</td>
</tr>
<tr>
<td>Halt within 10 days, or 10% curtailment in output, production, or service</td>
<td>3-4 “Charlie”</td>
<td>2</td>
<td>Loss may reduce mission performance</td>
</tr>
<tr>
<td>No significant effect on output, production, or service</td>
<td>1-2 “Delta”</td>
<td>1</td>
<td>Loss would not affect mission performance</td>
</tr>
</tbody>
</table>
## CARVER

### Criticality Assignments

<table>
<thead>
<tr>
<th>Threat</th>
<th>CARVER Value (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - ZEUS/ZBOT &amp; STUXNET</td>
<td>5</td>
</tr>
<tr>
<td>Nuclear - Dirty Bombs</td>
<td>5</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>2</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>5</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>3</td>
</tr>
</tbody>
</table>
• Cyber - ZEUS/ZBOT & STUXNET
  o Unauthorized access to a control system device or network using a data communication pathway
  o can affect critical infrastructure such as nuclear, power, water or financial
  o two specific top cyber threats examined
  o Highest criticality will be used for the overall cyber criticality value
• ZEUS/ZBOT
  o Used to capture sensitive information as it is input by the user and sent to the control center located elsewhere
  o Sensitive financial information such as credit card numbers, expiration dates, login to financial sites, etc. can be intercepted.
  o Compromise of selected targets such as sites that issue security certificates can undermine the financial sector
  o An example of this is the DigiNotar Certificate breach which pretty effectively ended with a temporary shutdown of the e-government in the Netherlands
  o Impact of loss would reduce mission performance
ZEUS/ZBOT - Spam Method

**Typical infection flow**
1. Spam emails supposedly from legitimate websites arrive in a user’s inbox.
2. Clicking the link in the message leads to a phishing site.
3. The phishing website requests users to fill in some required information. Once logged in, the site will direct users to a download link.

**Other infection flow found**
1. Users unknowingly download the file from malicious websites.
2. Users download a ZBOT variant that installs itself on the affected system.

**ZBOT logs keystrokes and steals personally-identifiable information, particularly personal financial information. The gathered information are sent to remote URLs via HTTP.**

The Trend Micro Smart Protection Network delivers security that’s smarter than conventional approaches by blocking the latest threats before they reach you.
ZEUS/ZBOT - Malicious Site Download

TSPY_ZBOT.BYZ is downloaded from a malicious site.

TSPY_ZBOT.BYZ decrypts and executes PE_LICAT.A-O in the infected system’s memory.

PE_LICAT.A-O inserts its code into unused file spaces, turning infected files into PE_LICAT.A.

ZBOT variants steal sensitive information such as user names and passwords to banking and other sites, which may lead to unauthorized use of the stolen data for malicious purposes.

PE_LICAT.A-O generates and connects to random URLs to download TSPY_ZBOT.BYZ.
• **STUXNET**
  
  o Computer worm that was designed to attack specifically Siemens programmable logic controllers (PLC) that are controlled by Windows based industrial software.
  
  o Stuxnet is noted for its attack on Iran’s nuclear enrichment plants causing some of its centrifuges to overspin. It accomplishes this through a Supervisory Control and Data Acquisition (SCADA) attack.
  
  o SCADA systems are used in various processes such as nuclear power, electric generating and water plants.
  
  o In nuclear power plants, SCADA is used to control many aspects including cooling which is critical in preventing a meltdown.
A successful attack by a modified Stuxnet worm on such a critical system could result in a nuclear meltdown.

Such a nuclear meltdown would be disastrous, causing a total shutdown of the plant as well as casualties on-site, serious ramifications for the surrounding region, and the necessity of mandating a massive cleanup effort.

Impact of loss would be a mission stopper.
**Stuxnet Details (1/2)**

**HOW STUXNET WORKED**

1. **Infection**
   Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. **Search**
   Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. **Update**
   If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. **Compromise**
   The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. **Control**
   In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. **Deceive and Destroy**
   Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.
CARVER
Criticality - Nuclear

- Nuclear - Dirty Bomb
  - Designed to disperse radiation - radiological dispersal device (RDD)
  - Is actually a weapon of mass disruption rather than destruction
  - Resulting radiation would be immediately noticeable
  - Strategically placed in populated areas, radiation persists for a period of time with larger cumulative effect compared to the original blast
  - Affected areas would have limited access during the substantial decontamination effort effectively shutting target down.
  - Decontamination/cleanup makes it an ideal economic weapon
  - Panic could increase the casualty count higher than the blast
  - Impact of loss would be a mission stopper
CARVER
Criticality - Water

- Water - Sewage Gate Closings
  - Sluice gates keep raw sewage from drinking water
  - Contamination of water supply could result from gate sabotage
  - Effect is not immediate, could take 3-7 days
  - Cleanup could take 3-6 months e.g. WVA contamination - (10 day ban on drinking water and still have questions two months later)
  - Alternatives exist to tap water - also, other uses such as putting out fires or cooling nuclear reactors are still viable.
  - Impact of loss may reduce mission performance
# Sewage Gates: Target Timetable for Recovery

<table>
<thead>
<tr>
<th>Event occurs</th>
<th>0–24 hours</th>
<th>1–3 days</th>
<th>3–7 days</th>
<th>1–2 weeks</th>
<th>2 weeks – 1 month</th>
<th>1–3 months</th>
<th>3–6 months</th>
<th>6 months–1 year</th>
<th>1–3 years</th>
<th>3+ years</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wastewater Systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threats to public health &amp; safety controlled</td>
<td>R</td>
<td>Y</td>
<td>G</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raw sewage contained &amp; routed away from population</td>
<td>R</td>
<td>Y</td>
<td>G</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treatment plants operational to meet regulatory requirements</td>
<td>R</td>
<td>Y</td>
<td>G</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major trunk lines and pump stations operational</td>
<td>R</td>
<td>Y</td>
<td>G</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection system operational</td>
<td>R</td>
<td>Y</td>
<td>G</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key to the Table**

- **R**: Required action within specified time frame.
- **Y**: Action to be completed within specified time frame.
- **G**: Goal to be achieved within specified time frame.
- **X**: No action required within specified time frame.
Electric – EMP

- Electromagnetic Pulse (EMP) attack uses a device generating such a pulse that could have the effect of permanently crippling electronic components in the susceptible area.

- Most likely scenario: explosion by a relatively sophisticated nuclear warhead in the megaton range at 30 miles above the target.

- Today, smaller non-nuclear devices such as high power microwave (HPM) devices are considered as viable threats.

- These cannot currently create a pulse big enough to even affect an entire city.
Electric – EMP

• They could theoretically create a blackout in a strategically chosen localized target area lasting until the electronic equipment can be relocated and replaced.

• Impact of loss would be mission stopper

Note: while this has been given a high criticality rating, the effects of EMP are currently disputed. See the cited paper by Nobel Prize (Physics, 1988) laureate Jack Steinberger who thinks the case for EMP is overstated and does not recommend spending vast sums of money to harden the critical infrastructure.
Transit - Mass Shootings

- Typically involve the slaughter of 4 or more victims.
- In a public transit system, could have the effect of temporarily halting the transit line in the vicinity.
- It would be most effective when combined with another vector.
- For example, a successful EMP attack would necessitate bringing in replacement electronic devices. However, if the transportation is clogged, this may hamper the timeliness of this remedy.
- Impact of loss would reduce mission performance
Accessibility - How easy is it to access or impact the critical asset?
## CARVER
Accessibility Assignments

<table>
<thead>
<tr>
<th>Threat</th>
<th>CARVER Value (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - ZEUS/ZBOT &amp; STUXNET</td>
<td>5</td>
</tr>
<tr>
<td>Nuclear - Dirty Bombs</td>
<td>3</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>3</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>4</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>4</td>
</tr>
</tbody>
</table>
Carver
Accessibility - Cyber (1 of 3)
• ZEUS/ZBOT & STUXNET = 5
  o Cyber attacks using the computer programs of ZEUS/ZBOT & STUXNET is easily accessible away from Security.
  o Because a Trojan built with a ZEUS toolkit is adaptable, variations of ZEUS Trojan are often missed by anti-virus software applications.
  o Once infected, a PC can be recruited to become part of a botnet. Also the ZEUS Trojan lays dormant until the end user visits a Web page with a form to fill out.
**CARVER**

**Accessibility - Cyber (2 of 3)**

- Cyber- ZEUS/ZBOT & STUXNET = 5
- STUXNET
  - Computer worm that target industrial control systems (ICS) that are commonly used in infrastructure supporting facilities. (i.e. power plants, water treatment facilities, gas lines, etc.)
  - This computer worm is designed to programmatically alter Program Logic Controllers (PLC)
  - Many of the hardware devices used in industrial control systems (ICS) are not Internet-connected (and often not network connected).
  - Stuxnet worm incorporates several sophisticated means of propagation with the goal of eventually reaching and infecting STEP 7 project files used to program the PLC devices.
• Cyber - ZEUS/ZBOT & STUXNET= 5
  o The worm targets computers running Windows operating systems.
  o PLC is not a Window operating systems device, but more of a proprietary machine-language device.
  o STUXNET simply traverses Windows computers in order to get to the systems that manage the PLCs, upon which it renders its payload.
  o The worm infects USB drives or other removable storage devices that are subsequently connected to the infected machine.
    ▪ Those USB drives then infect other machines much like the common cold.
• Nuclear - Dirty Bomb = 3
  
  o Some radioactive materials are accessible to terrorists just by common theft from an individual or company.
  
  o Radioactive materials are routinely used at hospitals, research facilities, industrial activities, and construction sites. These radioactive materials are used for such purposes as diagnosing and treating illnesses, sterilizing equipment, inspecting welding seams.
• Water - Sewage Gate Closings = 3
  o The Water Sewage SCADA is accessible to the point where one that is controlled by a powering door (so to speak) can be influenced to be shut down. This could allow too much water to remain in the system or, worse, not enough water rendering the system inoperable.
  o Better to access from a computer system than manually
  o There are however some that are manually opened and closed, which present a problem for the attackers that want to cause damage to the water system.
The threat of using an EMP (electromagnetic pulse) device is easily accessible outside.

A weaponized EMP would be ideal for the destruction of communication devices in a large area.

Defence experts believe detonating a nuclear device above the earth could cripple electronic systems, knock out water and electricity supplies and bring civilisation to a halt.

The strength of the pulse depends on the distance of the explosion from the earth's equator.

The discovery of the weapon would be after the fact because it can be hidden in secret, possibility of detection is slim if documentation was to be falsified by Sovereign Citizens or a possible decoy that could be deployed.
CARVER
Accessibility - Transit

- Transit- Mass Shootings = 4
  - Mass shootings are easily accessible outside.
  - These shootings can occur at any mass transit area and at any time.
  - The AAACU can manipulate transit computer systems, leaving the law enforcement scrambling to figure out routes to get around wasting valuable time for responding to the incidents.
  - Emergency services would not know what happened until someone called the incident and explained what was happening.
  - There would be no proactive strategies.
  - Not many people would be prepared for this threat and would be in a panic
CARVER
Recoverability

**Recoverability** - How much time and money would be required to replace or restore a critical asset?
## CARVER

### Recoverability Assignments

<table>
<thead>
<tr>
<th>Threat</th>
<th>CARVER Value (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - ZEUS/ZBOT &amp; STUXNET</td>
<td>5</td>
</tr>
<tr>
<td>Nuclear - Dirty Bombs</td>
<td>5</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>1</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>5</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>5</td>
</tr>
</tbody>
</table>
CARVER
Recoverability

- Recoverability
  - Recoverability is measured by how much time and money would be required to replace or restore a critical asset.
  - Recoverability varies by the type and source of the target and the availability of spare parts and other resources.

- Determining Factors are:
  - Onhand equipment i.e. railroads, cranes, drydocks, and cannibalization
  - Restoration and substitution through redundancies
  - Onhand spares
CARVER
Recoverability - Cyber

- Cyber - ZEUS/ZBOT = 1
  - ZEUS/ZBOT Uses stealth techniques and can be hard to find.
    - There is no way to gauge time it will take to find ZBOT
  - Once found can be eliminated with a simple virus scan.
    - Can be eliminated quickly
CARVER
Recoverability - Cyber (1 of 2)

- Cyber - STUXNET = 5
  - Speeding up or overclocking an enrichment centrifuge runs the risk of
    - Explosive failure
    - Disruption of the cascade
    - Leaks of corrosive and radioactive uranium hexafluoride gas
The casing of the centrifuge is needed to contain the rapidly spinning components. Shrapnel and failure of a single centrifuge can cause a domino effect destroying adjacent centrifuges.

Restoring power and fixing the plant could take a very long time if at all possible.

There will be long term effects of radiation on the population and ecosystem.
### Table 1. Acute Radiation Syndromes

<table>
<thead>
<tr>
<th>Phase</th>
<th>Feature</th>
<th>Subclinical range</th>
<th>Sublethal range</th>
<th>Lethal range</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0-100 rad (cGy)</td>
<td>100-200 rad (cGy)</td>
<td>200-600 rad (cGy)</td>
</tr>
<tr>
<td>Prodromal Phase</td>
<td>Nausea and Vomiting</td>
<td>none</td>
<td>50-100%</td>
<td>75-100%</td>
</tr>
<tr>
<td></td>
<td>Onset</td>
<td>3-6 hrs</td>
<td>2-4 hrs</td>
<td>1-2 hrs</td>
</tr>
<tr>
<td></td>
<td>Duration</td>
<td>&lt;24 hrs</td>
<td>&lt;24 hrs</td>
<td>&lt;48 hrs</td>
</tr>
<tr>
<td></td>
<td>Lymphocytes</td>
<td>&lt;100 @24 hr</td>
<td>&lt;500 @24 hr</td>
<td>&lt;500 @ 24 hr</td>
</tr>
<tr>
<td>Latent Phase</td>
<td>Duration</td>
<td>&gt;2 wks</td>
<td>7-15 days</td>
<td>0-7 days</td>
</tr>
<tr>
<td>Illness Phase</td>
<td>Sign and Symptoms</td>
<td>none</td>
<td>moderate leukemia</td>
<td>severe leukopenia,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>purpura, hemorrhage,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>infection</td>
</tr>
<tr>
<td></td>
<td>Onset</td>
<td>&gt;2 wks</td>
<td>2 days - 2 wks</td>
<td>2-3 days</td>
</tr>
<tr>
<td></td>
<td>Organ System</td>
<td>none</td>
<td>hematopoietic and</td>
<td>GI tract, mucosal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>respiratory (mucosal)</td>
<td>systems</td>
</tr>
<tr>
<td></td>
<td>Hospitalization</td>
<td>0</td>
<td>0-100%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>Fatality</td>
<td>0%</td>
<td>0-80%</td>
<td>90-100%</td>
</tr>
<tr>
<td></td>
<td>Time of Death</td>
<td>0%</td>
<td>3 wks-3 months</td>
<td>1-2 wks</td>
</tr>
</tbody>
</table>

---

**Whole Body Radiation from External Radiation or Internal Absorption**

**Diarrhea, fever, electrolyte disturbance**

**Convulsions, ataxia, tremor, lethargy**

**GI tract, mucosal systems**

**CNS**

**100% 2 weeks**
CARVER
Recoverability - Nuclear (1 of 2)

• Nuclear - Dirty Bomb = 5

“The ease of recovery from [a radiological] attack would depend to a great extent on how the attack was handled by first responders, political leaders, and the news media, all of which would help to shape public opinion and reactions.”

- Making the Nation Safer
National Research Council (2002)

○ When a Dirty Bomb is detonated it releases small radiological particles into the air.

○ These particles move with and are carried by the wind.

○ This spreads the plume and radiation over a larger area.

○ The particles could potentially contaminate drinking water, food, and surfaces making the affected area unlivable and uninhabitable and likely to cause radiation sickness.
• The recoverability of a Dirty Bomb is directly related to the size of the blast and weather factors, such as wind, precipitation, and humidity.
• The more spread out the plume is, the more diluted the radiation becomes.
CARVER
Recoverability - Water

- Water-Sewage gate closings = 1
  - Gates are closed by:
    - Hydraulics
    - Chains on pulleys
    - Computer
  - Hydraulic and chain systems can be manually opened or closed by water authority in time of crisis.
  - Computer models may be stuck open but generally have a chain or hydraulic backup.
CARVER
Recoverability - Electric

- Electric-EMP = 5
  - An EMP will disrupted communication networks and all electronics
  - Communication networks and electronics may never be restored to their original state.
  - The EMP would knock out the electrical power Grid
    - Transformers and power lines would need to be replaced before service is restored.
    - Generators and substations would have to be rebuilt
    - Cars, trucks, and an entire infrastructure would be gone
CARVER
Recoverability - Transit

- Transit - Mass Shootings = 5
  - Mass shootings in large areas of transportation volume will leave the society with horrible images that will not go away in a year.
  - Media footage will be played over and over for years to come.
  - Memorials and charities for victims will be created.
  - A national or city wide day of remembrance will be created.
  - The city will not recover or forget what happened for a very long time.
Vulnerability - Are there effective methods for securing the critical asset?
## CARVER

Vulnerability Assignments

<table>
<thead>
<tr>
<th>Threat</th>
<th>CARVER Value (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - ZEUS/ZBOT &amp; STUXNET</td>
<td>3</td>
</tr>
<tr>
<td>Nuclear - Dirty Bombs</td>
<td>2</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>5</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>4</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>5</td>
</tr>
</tbody>
</table>
1. Cyber - ZEUS/ZBOT and STUXNET = 3
   - ZEUS/ZBOT is easy to remove but difficult to find in a system, creating distrust in financial institutions on the part of a customer, this can possibly create an influx of onsite withdrawals if the attack is widespread enough.
   - The ZBOT spofs online banking pages to steal credentials and can be accessed in the dark web.
Cyber - ZEUS/ZBOT and STUXNET = 3

- STUXNET code has reportedly been released on pastebin and sources have confirmed (Mr. Eugene Kaspersky) that STUXNET is ‘loose in the wild’ and infected Russian Nuclear Plants.
- Stuxnet could potentially be modified by the right hands to cause physical explosions based on centrifugal speeds or by adjusting cooling systems.
CARVER
Vulnerability - Nuclear

- Nuclear - Dirty Bomb = 2
  - Nuclear devices that are improvised are known as ‘dirty bombs.’
  - A Dirty Bomb detonation in SLR would have a massive impact upon the critical infrastructure.
  - Specialized Response Units are required to mitigate nuclear fallout or contamination.
CARVER
Vulnerability - Water

- Water - Sewage Gate Closings = 5
  - Water Sewage SCADA is difficult to breach and difficult to maintain a breach of.
  - The right team of Spec-Ops in the Cyber War should have no issue finding the port used as well as restore systems quickly.
  - The attack will however, have a fear factor as well as draw focus from other targets.
CARVER
Vulnerability - Electric

• Electric - EMP = 4
  o Special Ops. would be able to scramble jets since the delivery method must be several thousand feet in the air.
  o If the object used is similar to a weather balloon licensed illegally using fraudulent documents, a modus operandi of Sovereign Citizens, the attack may be successful.
CARVER
Vulnerability - Transit

- Transit - Mass Shootings = 5
  - Spec. Ops. or Task Force Units involved with MSR (Mass Shooting Response) would be able to respond effectively but only after they ‘receive the call.’
  - This allows attackers to cause a significant amount of damage with a high number of casualties if a ‘kill zone’ is created by AAACU through cyber manipulation of transit systems.
Effect - What are the adverse consequences that would result from a successful natural or accidental or intentional threat aimed at the critical asset?
## CARVER Effect Assignments

<table>
<thead>
<tr>
<th>Threat</th>
<th>CARVER Value (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - ZEUS/ZBOT &amp; STUXNET</td>
<td>3</td>
</tr>
<tr>
<td>Nuclear - Dirty Bombs</td>
<td>4</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>1</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>5</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>4</td>
</tr>
</tbody>
</table>
Effect

- Effects
  - The effect of the target attack is the measure of possible impacts:
    - Military
    - Political
    - Economic
    - Psychological
    - Sociological
  - For Example, effects can be collateral damage, triggering of countermeasures, effects on civilian population, etc.
CARVER
Effect - Cyber (1 of 2)

- Cyber - ZEUS/ZBOT = 3
  - If used correctly, the Zeus/Zbot can have devastating effects:
    - launching DDoS attacks
    - Stealing of personal and confidential information
      - Bank Account Numbers
      - Social Security Numbers
  - This can have impact on financial systems, security systems, basically anything the attacker chooses to target.
  - Hardly any effect on civilian populace considering they will have no idea what is happening until the damage is already done.
• Cyber - Stuxnet = 3
  o Effects can cause explosions and/or shutdown systems at Nuclear sites:
    ▪ Cause panic among civilians with the threat of Nuclear fallout.
    ▪ Huge economic effect if power plants are shut down.
  o If explosions occur then collateral damage to surrounding area for years.
  o Countermeasures will be triggered very quickly since attack and method are known.
CARVER
Effect - Nuclear

- Nuclear - Dirty Bomb = 4
  - The press will make this attack felt most strongly.
  - Will be blown out of proportion and cause panic amongst civilian population.
  - The actually explosion and fallout will not literally have an effect, the sociological and psychological effect will be what causes the most damage.
  - This attack will help immensely with target goal of attacks combined, diverting a lot of attention.
CARVER
Effect - Water

• Water - Sewage Gate Closings = 1
  o This is the least effective of the attack methods.
  o Effect could be possible:
    ▪ Flooding
    ▪ Water shutoff for crop fields, dams, water treatment plants, etc.
  o Any attack will most likely be handled within 24 hours.
  o By the time word of the attack spreading, issue will most likely be resolved.
  o This attack will help somewhat with the total attack goal but few resources will be needed to stop it.
CARVER
Effect - Electric

• Electric - EMP = 5
  o Could potentially be the most catastrophic of all.
  o Will shut down all electrical systems causing:
    ▪ Panic with civilian population, no cellphones, cars, tv, etc.
    ▪ Military and police communication and coordination will be shut down.
    ▪ Government will have no way to get messages to the population not to panic and stay calm.
    ▪ Financial, economic, power, etc. systems will shut down.
  o This will be the most effective way of completing the attack goal.
Effect - Transit

- Transit - Mass Shootings = 4
  - The literal effect of mass shootings will not be that effective. 50/100 deaths before stopped is not that much.
  - The real effect will be the fear tactic that will hit the civilian population.
    - Population will be scared to go outside.
    - Blame the government for not doing anything or being able to stop the attack.
  - This will be very beneficial to completing the attack goal, will divert most of the attention of law enforcement and news to let other attacks go on almost unnoticed.
Recognizability - What is the likelihood that terrorists will recognize the critical nature of the asset?
# CARVER

## Recognizability Assignments

<table>
<thead>
<tr>
<th>Threat</th>
<th>CARVER Value (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - ZEUS/ZBOT &amp; STUXNET</td>
<td>2</td>
</tr>
<tr>
<td>Nuclear - Dirty Bombs</td>
<td>4</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>3</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>3</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>5</td>
</tr>
</tbody>
</table>
CARVER
Recognizability

• Recognizability
  o Is the ability in which it can be recognized by an operational element or intelligence and reconnaissance asset under all conditions.
    ▪ Weather
    ▪ Population
    ▪ Seasons
    ▪ Countermeasures
  o Also takes into other factors:
    ▪ Simple or complex?
    ▪ Easy to identify or complicated?
    ▪ Has it been done before and are there clear steps to completion?
CARVER

Recognizability - Cyber (1 of 2)

- Cyber - ZEUS/ZBOT = 2
  - Is something not easily recognizable, perfect example is that many people today are still affected with it.
  - Not a significant impact on system host, hard to detect.
  - Has been done a lot now so it is easy to manipulate code to be undetectable still.
  - Provides easy control for Bot-master.
Cyber - STUXNET = 2

- This cannot be recognized unless by experts, extremely complicated and not simple by any means.
- This has been done before and the steps to create it are clear to attacker.
- The size and complexity of a Nuclear site also decreases the likelihood of detection.
- Only difficult part is getting a USB device to the network since its common knowledge now not to plug in random ones found into computers at Nuclear facilities.
CARVER
Recognizability - Nuclear

- Nuclear - Dirty Bomb = 4
  - Not actually a nuclear bomb and after the initial explosion, the real effect will be the mass panic.
  - Typically the radioactive fallout will not kill or make people sick, it will be the media blowing it out of proportion that will have the real effect.
  - Bomb itself is not any more difficult to make the most other home made bombs.
CARVER
Recognizability - Water

- Water - Sewage Gate Closings = 3
  - This is moderately recognizable, most people would think flood first, not sewage terrorism.
  - Can be handled by sewage gate experts fairly easily.
  - This form of attack is not particularly difficult to execute nor is it easy.
CARVER
Recognizability - Electrical

- Electrical - EMP = 3
  - This is the most devastating form of attack other than a full nuclear explosion.
  - Easily recognizable, once detonated: lights out.
  - All electric systems will be down.
  - Not a particularly difficult form of attack.
  - Biggest problem will be getting an EMP device.
CARVER
Recognizability - Transit

• Transit - Mass Shootings = 5
  o This is the most easily recognizable, obviously with devastating effects to people involved.
  o Fear tactic plays a huge role like DC sniper.
  o Attack requires no training to execute.
  o Steps for completion are clear for attacker.
### CARVER
Threat Analysis Matrix

<table>
<thead>
<tr>
<th>Threat</th>
<th>C</th>
<th>A</th>
<th>R</th>
<th>V</th>
<th>E</th>
<th>R</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber - Zeus/ZBot &amp; STUXNET</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>23</td>
</tr>
<tr>
<td>Nuclear - Dirty Bomb</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>23</td>
</tr>
<tr>
<td>Water - Sewage Gate Closings</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>Electric - EMP</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>26</td>
</tr>
<tr>
<td>Transit - Mass Shooting</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>26</td>
</tr>
</tbody>
</table>
CARVER

Threat Analysis Conclusion

- Given the Threat Analysis Matrix the greatest threats to San Luis Rey are an EMP and Mass Shooting Attack. Between these two threats the most accessible is a Mass Shooting.
- The secondary threats judged to be the next greatest threat from the matrix are Cyber Attacks and Dirty Bombs. These are much more accessible than the EMP device but cause less damage.
- It is recommended to the US Government to enact legislation for State Defense to mitigate these threats in the most cost effective and operationally effective manner.
Vulnerability Analysis
City of San Luis Rey Vulnerabilities

- Nuclear Power Plant - SCADA
- Army Base - Dirty Bomb
- Lake Juniper Water Authority - SCADA
- Airport - EMP air traffic control
- Water Dam
- Cruise Ship - transit mass shooting
- Deep Water Port
- Cyber Attack
## Vulnerability Worksheet

**Target Name:** Lake Juniper Nuclear Power Station- SCADA (LJNPS) In San Luis Rey City (SLR)

<table>
<thead>
<tr>
<th>Question</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) LJ Nuclear Power Station Level Of Visibility: Assess the awareness of the existence and visibility of Power Plant - SCADA System</td>
<td>5</td>
</tr>
<tr>
<td>0=Invisible, 1=Very Low Visibility, 2=Low Visibility, 3=Medium Visibility, 4=High Visibility, 5=Very High Visibility</td>
<td></td>
</tr>
<tr>
<td>2) Criticality of LJNPS in SLR: Assess the usefulness of access to local population, economy government, etc.</td>
<td>5</td>
</tr>
<tr>
<td>0 = No usefulness , 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical</td>
<td></td>
</tr>
<tr>
<td>3) Impact Outside of LJNPS Jurisdiction: Assess the effect loss will have outside of the SLR</td>
<td>5</td>
</tr>
<tr>
<td>0= None       2 = Low               1= Minor            3 = Medium           4= High       5 = Very High</td>
<td></td>
</tr>
<tr>
<td>4) PTE Access to LJNPS: Assess the availability of LJNPS - SCADA System for ingress and egress by PTE (Potential Target Element)</td>
<td>1</td>
</tr>
<tr>
<td>0 = Restricted                         1 = Controlled           2 = Limited              3 = Moderate              4 = Open  5 = Unlimited</td>
<td></td>
</tr>
<tr>
<td>5) Potential LJNPS Threat Hazard: Assess the availability of LJNPS based on SCADA attack</td>
<td>5</td>
</tr>
<tr>
<td>0 = None               1 = Minimal             2 = Low             3 = Moderate               4 = High                     5 = Very High</td>
<td></td>
</tr>
<tr>
<td>6) Potential LJNPS Site Population Capacity:</td>
<td>2</td>
</tr>
<tr>
<td>0 = 0, 1 = 101 – 250   2 = 251 – 5,000       3 = 5,001 – 15,000    4 = 15,001 – 50,000   5 = &gt;50,001</td>
<td></td>
</tr>
<tr>
<td>7) Potential for Collateral Mass Casualties:</td>
<td>4</td>
</tr>
<tr>
<td>0 = 0   1 = 101 – 250       2 = 251 – 5,000       3 = 5,001 – 15,000    4 = 15,001 – 50,000   5 = &gt;50,00</td>
<td></td>
</tr>
</tbody>
</table>

**Total Score Rating:** Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form. 0-2 pts. =1, 3-5 pts. =2, 6-8 pts. =3,9-11 pts. =4, 12-14 pts. =5,15-17 pts. =6,18-20 pts. =7, 21-23 pts. =8, 24-26 pts. =9, 27-29 pts. =10, 30-32 pts. =11, 33-35 pts. = 12

**Total Score Rating:** Basic Target Vulnerability Assessment Rating: **27**
Vulnerabilities
Nuclear Power Plant - (SCADA) (1 of 14)

- SCADA components
- Methods of access
- Industrial Control Systems (ICS)
- Controller Units
  - Programmable Logic Controllers (PLCs)
  - Remote Terminal Units (RTU)
  - Distributed Control Systems (DCS)
- Modbus/TCP (protocols used in PLC communication)
- Control, Business, Internet networks
- Sensors, Motors, Valves
- Human-Machine Interfaces (HMI)
Vulnerabilities
Nuclear Power Plant - (SCADA) (2 of 14)

• SCADA Sensors
  o Temperature
  o Water Levels
  o Radioactivity Levels
  o Oil Levels & Maintenance Alarms
  o Noise Level
  o Flow Rate
  o Pump/fan speeds
  o Pressure
Vulnerabilities
Nuclear Power Plant - (SCADA) (3 of 14)

• Access to Control System LAN
  o Common network architectures
  o Dial up access to RTU
  o Vendor Support
  o IT controlled communication gear
  o Corporate VPN
  o Database Links
  o Poorly Configured Firewalls
  o Peer Utility Links

• Discovery of the process

• Control of the process
  o Sending commands directly to data acquisition equipment
  o Exporting HMI screen
Vulnerabilities
Nuclear Power Plant - (SCADA) (4 of 14)

• Common Architecture of a Control System
• Control separated by 2 firewalls
  o Internet / Attacker
  o Business Corp Network
  o Control System Network
Access to the control system LAN
- Common Architecture of a Control System
- Control System in DMZ
  - Internet / Attacker
  - Business Corp Network
  - Control System Network
Vulnerabilities
Nuclear Power Plant - (SCADA) (6 of 14)

- Common Architecture of a Control System
- 2 control system networks separated by firewalls
  - Internet / Attacker
  - Business Corp Network
  - Control System Network/s
Vulnerabilities
Nuclear Power Plant - (SCADA) (7 of 14)

- Common Architecture of a Control System Data DMZ
- DATA DMZ prevents communication directly from Business to Control LAN
- Separated by firewalls
  - Internet / Attacker
  - Business Corp Network
  - Control System Network
Vulnerabilities
Nuclear Power Plant - (SCADA) (8 of 14)

• RTU - attackers will dial every extension in an organization looking for modems directly connected to control systems
  o modems will identify themselves
  o typically no authentication
• Vendor Support - attackers will attempt access of internal vendor resources or external vendor laptops to exploit targets
• IT Controlled Communication gear - attackers will often attempt to take control of fibre optic, wireless links and other pathways that are typically tasked to the IT departments
Vulnerabilities
Nuclear Power Plant - (SCADA) (9 of 14)

• Corporate VPN - attackers will compromise remote users and wait for them to make remote connections to the target
• Database Links - attackers can use databases on the corporate LAN to execute commands on databases on the control LAN
• Poorly Configured Firewalls - attackers typically take advantage of permitted traffic across firewalls. These weaknesses are typical and increase with time and increased desire to integrate between control and business LAN.
• Peer Utilities - attackers will attempt to compromise utility and manufacturing partners who may have access to the target control system. Weakest link is where the exposure will initiate
Other Vulnerabilities that exist
  o Legacy operating systems that are part of the control system
  o Lack of normal corporate patching schedules due to instability
  o Legacy protocol shortcomings in security
  o Lack of general physical security
  o Lack of policies driving security
  o Lack of resources to enforce policies if in place
  o Companies refuse to realize the vulnerabilities until they are proven
Vulnerabilities
Nuclear Power Plant - (SCADA) (11 of 14)

- Lake Juniper Nuclear Power Station
- Adjacent is Robert Muller Dam
- Adjacent Lake Juniper Water Authority Intake
Vulnerabilities
Nuclear Power Plant - (SCADA) (12 of 14)

- Fukushima reactor
- Lake Juniper Power Station will at minimum have radiation leak and maximum total meltdown without water to cool the reactor.
Vulnerabilities
Nuclear Power Plant - (SCADA) (13 of 14)

• Contamination Types
  o Internal Contamination - ingesting radioactive materials through breathing, swallowing or an open wound
  o External Contamination - radioactive materials in dust, powder or liquid come into contact with skin, eyes, hair and clothing
  o Radioactive Contamination - radioactive materials released into the air, water, soil, plants and buildings
Vulnerabilities
Nuclear Power Plant - (SCADA) (14 of 14)

• Acute Radiation Syndrome - radiation sickness that occurs when a person is exposed to high doses of radiation usually over a short time frame
• Symptoms include
  o vomiting, nausea, headache, diarrhea
  o after initial symptoms a person can appear healthy for a time
  o depending on the dose following symptoms can include
    ▪ hair loss, loss of appetite, fatigue, fever, nausea, vomiting, diarrhea, seizures and coma
    ▪ seriously ill stage can last a few hours up to several months
    ▪ skin damage also can accompany high doses of radiation
      • skin can heal for short time, yet to have full symptoms return
### Vulnerability Worksheet Target Name: Army Base

<table>
<thead>
<tr>
<th>1) Army Base Level Of Visibility: Assess the awareness of the existence and visibility of the Army Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=Invisible, 1=Very Low Visibility, 2=Low Visibility, 3=Medium Visibility, 4=High Visibility, 5=Very High Visibility</td>
</tr>
<tr>
<td>Rating: 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2) Criticality of Army Base in SLR: Assess the usefulness of access to local population, economy, government, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = No usefulness, 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical</td>
</tr>
<tr>
<td>Rating: 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3) Impact Outside of Army Base Jurisdiction: Assess the effect loss will have outside of the SLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0= None                          2 = Low                                              1= Minor                      3 = Medium 4= High                  5 = Very High</td>
</tr>
<tr>
<td>Rating: 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4) PTE Access to Army Base: Assess the availability of Army Base for ingress and egress by PTE (Potential Target Element)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = Restricted                         1 = Controlled           2 = Limited              3 = Moderate              4 = Open  5 = Unlimited</td>
</tr>
<tr>
<td>Rating: 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5) Potential Army Base Threat Hazard: Assess the availability of Army Base possible shut down due to dirty bomb which would eliminate a major disaster response force</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = None               1 = Minimal             2 = Low             3 = Moderate               4 = High                     5 = Very High</td>
</tr>
<tr>
<td>Rating: 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6) Potential Army Base Site Population Capacity:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = 0, 1 = 101 – 250            2 = 251 – 5,000      3 =  5,001 – 15,000   4 = 15,001 – 50,000                  5 = &gt;50,001</td>
</tr>
<tr>
<td>Rating: 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7) Potential for Collateral Mass Casualties:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = 0       1 = 101 – 250            2 = 251 – 5,000      3 = 5,001 – 15,000         4 = 15,001 – 50,000 5 = &gt;50,001</td>
</tr>
<tr>
<td>Rating: 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic Target Vulnerability Assessment Rating: Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-2 pts. =1  9-11 pts. =4  18-20 pts. =7  27-29 pts. =10  3-5 pts. =2  12-14 pts. =5  21-23 pts. =8  30-32 pts. =11  6-8 pts. =3  15-17 pts. =6  24-26 pts. = 9  33-35 pts. = 12</td>
</tr>
<tr>
<td>Rating: 8</td>
</tr>
</tbody>
</table>
Vulnerabilities
Niven Army Base - Dirty Bomb (1 of 16)

Vulnerabilities
Niven Army Base - Dirty Bomb (2 of 16)

• Introduction
• Vulnerability assessment method / target characteristics
• Types of adversary and attack modes
• Countermeasures of current security policies
• Consequences of dirty bomb
• Recommendations
Vulnerabilities
Niven Army Base - Dirty Bomb (3 of 16)

• Introduction
  o Purpose is to provide information and guidance
  o Help people of SLR make informed decisions
  o Mitigate the effect of dirty bomb attacks

• Dirty bomb, risk, vulnerability
  o Severity and frequency of a dirty bomb on SLR is low
    ▪ The vulnerability of such an attack is low
    ▪ The possibility is rare
Vulnerabilities
Niven Army Base - Dirty Bomb (4 of 16)

- **Scope**
  - Objective is to examine prominent man made dirty bomb
  - Identify threats and coordinate responses
  - Reduce economic losses
  - Factors to be considered
    - Demography and geography
    - Weather and climate
    - Industries and other technologies
Vulnerabilities
Niven Army Base - Dirty Bomb (5 of 16)

• Vulnerability assessment method
  o Social vulnerability and role contributed by dirty bomb risk
  o Critical facilities
    ▪ Niven Army Base
      • Public Health
      • Niven Army Hospital
  o Critical infrastructures
    ▪ Healthcare
    ▪ Food (safety, distribution, and food processing)
    ▪ Post exchange / Post commissary
    ▪ Safety (chemical, biological, and nuclear safety; emergency services)
Vulnerabilities
Niven Army Base - Dirty Bomb (6 of 16)
Vulnerabilities
Niven Army Base - Dirty Bomb (7 of 16)

- Located South of Niven and 90 miles NW of San Luis Rey
- Primary function is to sustain combat operation on land
- Core Competencies
  - Prompt response
  - Support Civil Authority
  - Shape the Security Environment
  - Forcible Entry Operations
  - Sustained Land Dominance
Vulnerabilities
Niven Army Base - Dirty Bomb (8 of 16)

- Military base is opened to anyone with an ID
- General security rules inefficient
- No screening for people with access card
- Random checks made
- People can walk or park near building at their choice
Vulnerabilities
Niven Army Base - Dirty Bomb (9 of 16)

- Critical Infrastructures
  - Niven Army Hospital
  - Medical office building
  - Administration building
  - South Fire Station
  - North Fire Station
Vulnerabilities
Niven Army Base - Dirty Bomb (10 of 16)

• Types of adversaries and attack modes
  o Active terrorists
    ▪ Middle East
    ▪ Home grown
    ▪ Criminals
  o Insider threats
    ▪ radicalization of soldiers
Vulnerabilities
Niven Army Base - Dirty Bomb (11 of 16)

• Types of adversaries and attack mode
  o Attack mode
    ▪ Dirty bomb
      • Radiological Dispersion Devices
      • Radioactive materials spread around by conventional explosives
      • Readily available online
      • Available precursors
      • Not expensive to produce
Vulnerabilities
Niven Army Base - Dirty Bomb (12 of 16)

- Dirty Bomb Attack Scenario of Niven Army Base
  - Terrorists hijack two construction trucks with 11,000 lb of TNT with radioactive payload each and drove to main gate to get access to the base
  - Park the bombs in between critical infrastructure nodes
    - Base PX and administration building
    - Adjacent to hospital
  - Initial blasts Killed a few dozen soldiers and civilians
  - Radiation quickly dispersed
  - Fire emergency personnel responded
  - Dirty bomb detonation officially confirmed
Vulnerabilities
Niven Army Base - Dirty Bomb (13 of 16)

• Dirty Bomb Attack Scenario of Niven Army Base
  o Dirty Bomb news traveled quickly to Niven and SLR
  o People are in fear and have tried to leave SLR
  o Crowded trains, buses, and highways
  o Businesses are closing their doors
  o Communication jammed (heavy traffic)
  o Social and economic disorder
Vulnerabilities
Niven Army Base - Dirty Bomb (14 of 16)

- Countermeasures of current security policies
  - Existing Vulnerability security policies and procedures are Low
    - Lack of inter-agency coordination
    - Lack of Federal Response Plan
    - Limited trained personnel
    - Limited public communication
Vulnerabilities
Niven Army Base - Dirty Bomb (15 of 16)

• Consequences
  ○ Created a climate of fear
  ○ Large number of casualties
  ○ Economic loss
  ○ Social Chaos
  ○ Weapon of Mass Disruption
Vulnerabilities
Niven Army Base - Dirty Bomb (16 of 16)

• Recommendations
  o Improve physical security
    ▪ Employee training
    ▪ 100 % ID Check
    ▪ Surveillance equipment
    ▪ RDD detectors
    ▪ X-Ray machines & canine dogs
  o Establish a 3 layer perimeter defense around critical infrastructures
  o Federal Response Plan
  o Better cooperation with local and state law enforcement and public safety officers
## Vulnerability Worksheet

**Target Name:** Lake Juniper Water Authority- SCADA

<table>
<thead>
<tr>
<th>1) LJWA Level Of Visibility: Assess the awareness of the existence and visibility of LJWA- SCADA System</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = Invisible, 1 = Very Low Visibility, 2 = Low Visibility, 3 = Medium Visibility, 4 = High Visibility, 5 = Very High Visibility</td>
</tr>
<tr>
<td>Rating: 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2) Criticality of LJWA in SLR: Assess the usefulness of access to local population, economy government, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = No usefulness, 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical</td>
</tr>
<tr>
<td>Rating: 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3) Impact Outside of LJWA Jurisdiction: Assess the effect loss will have outside of the SLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = None, 2 = Low, 1 = Minor, 3 = Medium, 4 = High, 5 = Very High</td>
</tr>
<tr>
<td>Rating: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4) PTE Access to LJWA: Assess the availability of LJWA - SCADA System for ingress and egress by PTE (Potential Target Element)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = Restricted, 1 = Controlled, 2 = Limited, 3 = Moderate, 4 = Open, 5 = Unlimited</td>
</tr>
<tr>
<td>Rating: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5) Potential LJNPS Threat Hazard: Assess the availability of LJWA possible shut down due to dirty bomb water contamination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = None, 1 = Minimal, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High</td>
</tr>
<tr>
<td>Rating: 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6) Potential LJNPS Site Population Capacity:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
</tr>
<tr>
<td>Rating: 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7) Potential for Collateral Mass Casualties:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
</tr>
<tr>
<td>Rating: 2</td>
</tr>
</tbody>
</table>

**Total: 23**

**Basic Target Vulnerability Assessment Rating:** Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.

| 0-2 pts. = 1 | 9-11 pts. = 4 | 18-20 pts. = 7 | 27-29 pts. = 10 |
| 3-5 pts. = 2 | 12-14 pts. = 5 | 21-23 pts. = 8 | 30-32 pts. = 11 |
| 6-8 pts. = 3 | 15-17 pts. = 6 | 24-26 pts. = 9 | 33-35 pts. = 12 |

**Final Rating:** 8
Vulnerabilities
Lake Juniper Water Authority - SCADA (1 of 8)

- Lake Juniper Water Authority (LJWA) is one of main important government objects in the metropolitan region.
- Four independent towns made up San Luis County: Juniper Shore, Lakeview, Northfield, and Port Estaban.
- We choose to focus on Lake Juniper Water Authority because of its criticality to the population in the area.
- LJWA Provides electricity and clean water for the entire region and possibly more.
Vulnerabilities
Lake Juniper Water Authority - SCADA (2 of 8)

● SCADA System vulnerabilities include:
  ○ Tend to be set up on OS with already vulnerabilities existence such as:
  ○ Remote access allowed for maintenance.
  ○ Wireless/ Ethernet connection
  ○ Potential physical damage
Vulnerabilities
Lake Juniper Water Authority - SCADA (3 of 8)

• Basis for Attack
  o If the SCADA System is breach, the Water - Sewage Gate can be controlled (Open/close) remotely.
  o Gates can be opened or closed causing too much water for flooding or too little water to be pumped.
  o If intake pipes that deliver cooling water to nuclear plants are drained, this could cause nuclear plant shut down.
Vulnerabilities
Lake Juniper Water Authority - SCADA (4 of 8)

- Basis for Attack
  - A dirty bomb or some kind can be guided in the main water pipes and detonated
  - The radiation and water contamination would deny the city days with clean drinking water before the water pipelines can be repair, if repair is even possible.
  - Causes the city to rebuild the entire pipelines from scratch or forever be vulnerable to contaminated water from the pipes.
Vulnerabilities
Lake Juniper Water Authority - SCADA (5 of 8)

• Basis for Attack
  ○ The whole city’s power and it’s neighboring towns can be lost.
  ○ The longer it takes for repair the more money and casualties it could cause.
  ○ Lost of power not only can affect traffic lights and building elevators, but also homes and offices that have no back up generator on top of not having clean water.
Vulnerabilities
Lake Juniper Water Authority - SCADA (6 of 8)

• Basis for Attack
  o The entire city’s clean water and seafood items can be affected to cause major outbreak in the population.
  o This could cause more casualties than anticipated due to the heavy use of water.
  o Just the idea of contaminated water can scare the population from using it the way they should, causing psychological damage.
San Luis Rey Overview Power Map
Vulnerabilities
Lake Juniper Water Authority - SCADA (7 of 8)

• Consequences
  o Vulnerabilities being exploited, based information we have on SLR, is low due to SCADA System vulnerabilities.
  o Potential losses include casualties such as:
    ▪ Death
    ▪ Money
    ▪ Accidents
    ▪ Sickness
    ▪ Unhealthy environment
    ▪ Psychological damage
Vulnerabilities
Lake Juniper Water Authority - SCADA (8 of 8)

• Recommendations
  o Increase SCADA System Security to prevent breach
  o Set water contamination sensor in the water main intake pipelines
  o Don’t depend on one source of Power & clean water supplier.
  o Find alternative source of power for plan B in the case of an emergency.
  o Build another clean water and power supplier on Port Estaban Deep Water.
  o Test seafood items like fish, shrimp and lobster etc periodically.
<table>
<thead>
<tr>
<th><strong>Vulnerability Worksheet</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target Name: Airport</strong></td>
</tr>
<tr>
<td><strong>Total Score Rating: 9</strong></td>
</tr>
</tbody>
</table>

1) **Airport Level Of Visibility**: Assess the awareness of the existence and visibility of Power Plant - SCADA System
   0 = Invisible, 1 = Very Low Visibility, 2 = Low Visibility, 3 = Medium Visibility, 4 = High Visibility, 5 = Very High Visibility
   - **5**

2) **Criticality of Airport in SLR**: Assess the usefulness of access to local population, economy, government, etc.
   0 = No usefulness, 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical
   - **5**

3) **Impact Outside of Airport Jurisdiction**: Assess the effect loss will have outside of the SLR
   0 = None, 2 = Low, 1 = Minor, 3 = Medium, 4 = High, 5 = Very High
   - **2**

4) **PTE Access to Airport**: Assess the availability of Airport - System for ingress and egress by PTE (Potential Target Element)
   0 = Restricted, 1 = Controlled, 2 = Limited, 3 = Moderate, 4 = Open, 5 = Unlimited
   - **3**

5) **Potential Airport Threat Hazard**: Assess the availability of Airport & air traffic control shutdown possible by EMP
   0 = None, 1 = Minimal, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High
   - **5**

6) **Potential Airport Site Population Capacity**:  
   0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = >50,001
   - **2**

7) **Potential for Collateral Mass Casualties**:  
   0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = >50,001
   - **2**

**Total**

**Basic Target Vulnerability Assessment Rating**: Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.

- 0-2 pts. = 1  
- 3-5 pts. = 2  
- 6-8 pts. = 3  
- 9-11 pts. = 4  
- 12-14 pts. = 5  
- 15-17 pts. = 6  
- 18-20 pts. = 7  
- 21-23 pts. = 8  
- 24-26 pts. = 9  
- 27-29 pts. = 10  
- 30-32 pts. = 11  
- 33-35 pts. = 12

- **9**
The San Luis Rey International Airport is a complex city in its own and has a lot of potential vulnerability. It’s Located at the western edge of city and has a high EMP Altitude for bomb. For these reasons, we recommend a separate evaluation of the airport as part of a future stand alone analysis.
<table>
<thead>
<tr>
<th>vulnerable worksheet</th>
<th>target name: water dam</th>
<th>total score</th>
<th>rating: 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) water dam level of visibility: assess the awareness of the existence and visibility of power plant - scada system 0=invisible, 1=very low visibility, 2=low visibility, 3=medium visibility, 4=high visibility, 5=very high visibility</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) criticality of water dam in slr: assess the usefulness of access to local population, economy government, etc. 0 = no usefulness , 2 = moderate usefulness, 1 = very low, 3 = significant usefulness, 4 = highly useful, 5 = critical</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) impact outside of water dam jurisdiction: assess the effect loss will have outside of the slr 0= none, 2= low, 1= minor, 3= medium, 4= high, 5= very high</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4) pte access to water dam: assess the availability of ljnps - scada system for ingress and egress by pte (potential target element) 0 = restricted, 1 = controlled, 2 = limited, 3 = moderate, 4 = open, 5 = unlimited</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) potential water dam threat hazard: assess the availability of ljwa possible shut down due to dirty bomb or flood, which would shut down the whole city’s power supplier or contaminate the clean water. 0 = none, 1 = minimal, 2 = low, 3 = moderate, 4 = high, 5 = very high</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6) potential water dam site population capacity; 0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7) potential for collateral mass casualties; 0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total

34

Basic Target Vulnerability Assessment Rating: Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.

0-2 pts. =1
3-5 pts. =2
6-8 pts. =3
9-11 pts. =4
12-14 pts. =5
15-17 pts. =6
18-20 pts. =7
21-23 pts. =8
24-26 pts. =9
27-29 pts. =10
30-32 pts. =11
33-35 pts. =12

12
Vulnerabilities
Robert Muller Dam (2 of 15)

• Introduction
• Vulnerability assessment method / target characteristics
• Types of adversary and attack modes
• Countermeasures of current security policies
• Consequences of IED/ improvised nuclear device
• Recommendations
Vulnerabilities
Robert Muller Dam (3 of 15)

- Introduction
  - Built in 1908 along Lake Juniper
  - Located in the North East part of SLR
  - Great source of water for the metropolitan area
  - Provides hydroelectric power
  - Reduces threats of flooding
Vulnerabilities
Robert Muller Dam (4 of 15)
Vulnerabilities
Robert Muller Dam (5 of 15)

• Dirty bomb or Improvised Nuclear Device (IND), risk, vulnerability
  o Severity and frequency of a dirty bomb or IND on Dam is low
    ▪ The vulnerability of such an attack is low
    ▪ The possibility is medium
• History of Water Related Terrorism
  o 2006 - Sri Lanka, Tamil Tiger rebels cut the water supply to government-held villages in northeastern Sri Lanka
  o 2004 - India, Twelve Indian security forces were killed by an IED planted in an underground water pipe during “counter-insurgency operation in Khanabal area in Anantnag district”
Vulnerabilities
Robert Muller Dam (6 of 15)

- 2004 - Pakistan, In military action aimed at Islamic terrorists, including Al Qaida and the Islamic Movement of Uzbekistan, homes, schools and water wells were damaged and destroyed
- 2003 - Iraq, Sabotage/bombing of main water pipeline in Baghdad. The sabotage of the water pipeline was the first such strike against Baghdad’s water system
- 2003 - USA, Four incendiary devices were found in the pumping station of a Michigan water-bottling plant. The Earth Liberation Front (ELF) claimed responsibility, accusing Ice Mountain Water Company of “stealing” water for profit. Ice Mountain is a subsidiary of Nestle Waters
Vulnerabilities

Robert Muller Dam (7 of 15)

○ 2002 - Colombia, The Revolutionary Armed Forces of Colombia (FARC) detonated an explosive device planted on a German-made gate valve located inside a tunnel in the Chingaza Dam, which provides most of Bogota’s water

○ 2002 - Nepal, The Khumbuwan Liberation Front (KLF) blew up a hydroelectric powerhouse of 250 kW in Bhojpur District on January 26

○ 2001 - Israel, Palestinians destroy water supply pipelines to West Bank settlement of Yitzhar and to Kibbutz Kisufim

○ 2000 - Australia, 23 April, 2000, police arrested a man for using a computer and radio transmitter to take control of the Maroochy Shire wastewater system and release sewage into parks, rivers and property
Vulnerabilities
Robert Muller Dam (8 of 15)

• Scope
  o Objective is to examine prominent IND and man-made IED
  o Identify threats and coordinate responses
  o Reduce economic losses
  o Factors to be considered
    ▪ Demography and geography
    ▪ Weather and climate
    ▪ Industries and other technologies
Vulnerabilities
Robert Muller Dam (9 of 15)

• Social vulnerability and role contributed by IND or IED

• Critical facilities
  o Robert Muller Dam
  o Robert Muller hydroelectric power station
  o LJWA Operation center
  o Robert Muller Spillway

• Critical infrastructures
  o Healthcare
  o Food (safety, distribution, and food processing)
  o Banking and Finance
  o Communications
  o Emergency services
  o Safety
Vulnerabilities
Robert Muller Dam (10 of 15)

• Types of adversaries and attack mode
  o Attractive target
    ▪ Terrorists
    ▪ Political activists
    ▪ Criminals
  o The chance that terrorist will hit the dam is real
  o Easily accessible to the public
  o Computer control system may be accessible to hackers
Vulnerabilities
Robert Muller Dam (11 of 15)

• IND/IED attack scenario of Robert Muller Dam
  o Terrorist drives a speedboat armed with 20 lb of Semtex, and 1000 lb of TNT with radioactive payload
  o Initial blast destroys the dam
  o Water inundates the city
  o 280 square miles affected
  o 680,000 people are vulnerable
  o Hydroelectric power station stopped
  o Nuclear power station affected
  o Radiation quickly dispersed
  o Fire emergency personnel respond
Vulnerabilities
Robert Muller Dam (12 of 15)
Destroyed
Vulnerabilities
Robert Muller Dam (13 of 15)

• Countermeasures of current security policies
  o Existing Vulnerability security policies and procedures are Low
    ▪ Lack of physical security to hydroelectric plant, dam and water supply
    ▪ Lack of inter-agency coordination
    ▪ Lack of Federal Response Plan
    ▪ Limited trained personnel
    ▪ Limited public communication
Vulnerabilities
Robert Muller Dam (14 of 15)

- Consequences
  - Thousand of deaths due to flooding
  - Psychological fear
  - Economic loss
  - Social Chaos
Vulnerabilities
Robert Muller Dam (15 of 15)

• Recommendations
  o Improve physical security
    ▪ Access granted to those critical to operations
    ▪ Lighting and motion sensors around perimeter
    ▪ Surveillance equipment
    ▪ Prevent SCADA hacking
      • Water Systems should not be connected to internet
      • Water Systems need appropriate electronic security
  o Federal Response Plan
  o Better cooperation with local and state law enforcement and public safety officers
<table>
<thead>
<tr>
<th>Vulnerability Worksheet</th>
<th>Target Name: Cruise Ships</th>
<th>Total Score Rating: 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Cruise Ships Level Of Visibility: Assess the awareness of the existence and visibility of Power Plant - SCADA System</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>0=Invisible, 1=Very Low Visibility, 2=Low Visibility, 3=Medium Visibility, 4=High Visibility, 5=Very High Visibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Criticality of Cruise Ships in SLR: Assess the usefulness of access to local population, economy government, etc.</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>0 = No usefulness , 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) Impact Outside of Cruise Ship Jurisdiction: Assess the effect loss will have outside of the SLR</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>0= None                          2 = Low                                              1= Minor                      3 = Medium 4= High                  5 = Very High</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>4) PTE Access to Cruise Ships Assess the availability of LJNPS - SCADA System for ingress and egress by PTE (Potential Target Element)</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>0 = Restricted                         1 = Controlled           2 = Limited              3 = Moderate              4 = Open  5 = Unlimited</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) Potential Cruise Ships Threat Hazard: Assess the availability of LJWA possible shut down due to dirty bomb or flood, which would shut down the whole city’s power supplier or contaminate the clean water.</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>0 = None               1 = Minimal             2 = Low             3 = Moderate               4 = High                     5 = Very High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6) Potential Cruise Ships Site Population Capacity:</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>0 = 0, 1 = 101 – 250          2 = 251 – 5,000      3 = 5,001 – 15,000   4 = 15,001 – 50,000                  5 = &gt;50,001</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>7) Potential for Collateral Mass Casualties:</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>0 = 0         1 = 101 – 250       2 = 251 – 5,000       3 = 5,001 – 15,000       4 = 15,001 – 50,000 5 = &gt;50,001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Basic Target Vulnerability Assessment Rating: Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>0-2 pts. =1 9-11 pts. =4 18-20 pts. =7 27-29 pts. =10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-5 pts. =2 12-14 pts. =5 21-23 pts. =8 30-32 pts. =11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-8 pts. =3 15-17 pts. =6 24-26 pts. =9 33-35 pts. = 12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Vulnerabilities
Cruise Ship

- Dimensions of a Cruise Ship
  - Draught: 9.3 m (31 ft) 2 m (236 ft) above water line
  - Draught: 9.3 m (31 ft)
  - Depth: 22.55 m (74 ft)
  - Decks: 16 passenger decks
  - Length: 360 m (1,181 ft) overall
  - Beam: 47 m (154 ft) waterline 60.5 m (198 ft) extreme
  - Height: 7
Vulnerabilities
Cruise Ship (1 of 8)

• 6,000 Passengers and thousands of crew members
Vulnerabilities
Cruise Ship (2 of 8)

- Passengers
  - 4500 or more people stranded for hours or days on one ship.
  - No air conditioning.
  - No hot food or telephone service available.
  - Unable to flush toilets.
  - Water contamination due to untreated sewage.
  - Several passengers with food poisoning unable to evacuate.
  - No electricity.
  - Life boats not safe.
Vulnerabilities
Cruise Ship (3 of 8)

• Resolution:
  o Some states passed laws to address water contamination issues.
  o States in violation will be fined $25,000 per day.
  o Global cruise industries have introduced many new safety directives and strict international regulations to prevent fires or other hazardous occurrences.
  o $300 million was invested to upgrade safety on-board.
  o Engine fire suppression systems implemented.
  o Ships hospital patient safety systems have increased.

• Recommendation:
  o More power generators on-board to prevent electrical outages.
Vulnerabilities
Cruise Ship (4 of 8)

• Security
  o Level 3 Security on Cruise Ships:
    ▪ Security on the cruise lines could be military, private, or naval
    ▪ Cameras are located everywhere on the ship
    ▪ Every U.S port now maintains and enforces a minimum 300 foot “no float zone,” a security perimeter that prohibits private craft from coming near the cruise ships.
    ▪ Cruise ships are getting armed U.S. Coast Guard as escort in and out of ports.
    ▪ 96 Hour notification before entering into a port
    ▪ Screens all passengers belonging before entering the ship
    ▪ No access to sensitive areas such as: vessels & engine room
Vulnerabilities
Cruise Ship (5 of 8)

- Security
  - GPS systems are vulnerable to hackers and terrorist as they use it to hijack ships and commercial planes.
  - Electronic GPS “spoof” can get built for $3,000 and can take down sophisticated navigation systems.
  - Feeding counterfeit radio signals to a yacht can make it drive off course, into harsh waters or collide with another ship.
  - Because aircrafts have similar navigation systems, a commercial plane can be “spoofed” as well.
Vulnerabilities
Cruise Ship (6 of 8)

• Security
  o Resolution:
    ▪ University of Texas students designed a closed loop controller to dictate the heading of the vessel even when the vessel wants to go a different direction.
    ▪ Awareness of GPS hacking.
  o Recommendation:
    ▪ Approval of the designed loop controller by Homeland Security.
    ▪ Increase GPS security.
Vulnerabilities
Cruise Ship (7 of 8)

• Mass Shootings
  o Mass Shootings on a cruise line would be tougher to pull off due to security measures, however when Skeet Shooting was around on Cruise lines it would have been easier to accomplish.
  o Past shooting in Barbados, on March 19, 2013 at the port where a couple were dropped off after British Cruise.

• Other possible occurrences
  o Bombs on a Cruise Ship or dropped near the port
Vulnerabilities
Cruise Ship (8 of 8)

• Conclusion:
  o Cruise Ships have a lot of security inside, but in the open waters vulnerabilities exist.
  o Not enough security is established in the sky or surrounding of the cruise ships.

• Recommendation:
  o Possibilities for Aerial attacks exist
  o Secure the open waters and also aerial range around the ships which can help eliminate some vulnerabilities that are possible.
  o Check who purchases the tickets to go on a cruise, since anyone that pays for a ticket can go on the cruise ships regardless of their criminal history.
<table>
<thead>
<tr>
<th>Vulnerability Worksheet</th>
<th>Total Score Rating: 10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target Name:</strong> Deep Water Port</td>
<td></td>
</tr>
<tr>
<td>1) Deep Water Port Nuclear Power Station Level Of Visibility: Assess the awareness of the existence and visibility of Power Plant - SCADA System</td>
<td>5</td>
</tr>
<tr>
<td>0 = Invisible, 1 = Very Low Visibility, 2 = Low Visibility, 3 = Medium Visibility, 4 = High Visibility, 5 = Very High Visibility</td>
<td></td>
</tr>
<tr>
<td>2) Criticality of Deep Water Port in SLR: Assess the usefulness of access to local population, economy government, etc.</td>
<td>5</td>
</tr>
<tr>
<td>0 = No usefulness, 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical</td>
<td></td>
</tr>
<tr>
<td>3) Impact Outside of Deep Water Port Jurisdiction: Assess the effect loss will have outside of the SLR</td>
<td>3</td>
</tr>
<tr>
<td>0 = None, 2 = Low, 1 = Minor, 3 = Medium, 4 = High, 5 = Very High</td>
<td></td>
</tr>
<tr>
<td>4) PTE Access to Deep Water Port: Assess the availability of LJNPS - SCADA System for ingress and egress by PTE (Potential Target Element)</td>
<td>1</td>
</tr>
<tr>
<td>0 = Restricted, 1 = Controlled, 2 = Limited, 3 = Moderate, 4 = Open, 5 = Unlimited</td>
<td></td>
</tr>
<tr>
<td>5) Potential Deep Water Port Threat Hazard: Assess the availability of LJWA possible shut down due to dirty bomb or flood, which would shut down the whole city’s power supplier or contaminate the clean water.</td>
<td>5</td>
</tr>
<tr>
<td>0 = None, 1 = Minimal, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High</td>
<td></td>
</tr>
<tr>
<td>6) Potential Deep Water Port Site Population Capacity:</td>
<td>5</td>
</tr>
<tr>
<td>0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
<td></td>
</tr>
<tr>
<td>7) Potential for Collateral Mass Casualties:</td>
<td>5</td>
</tr>
<tr>
<td>0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>29</td>
</tr>
<tr>
<td><strong>Basic Target Vulnerability Assessment Rating:</strong> Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.</td>
<td>10</td>
</tr>
<tr>
<td>0-2 pts. = 1, 9-11 pts. = 4, 18-20 pts. = 7, 27-29 pts. = 10</td>
<td></td>
</tr>
<tr>
<td>3-5 pts. = 2, 12-14 pts. = 5, 21-23 pts. = 8, 30-32 pts. = 11</td>
<td></td>
</tr>
<tr>
<td>6-8 pts. = 3, 15-17 pts. = 6, 24-26 pts. = 9, 33-35 pts. = 12</td>
<td></td>
</tr>
</tbody>
</table>
Vulnerabilities
Deep Water Port

- Facts about Deep Water Port:
  - 57 Million tons of cargo a year
  - Tourists
  - Shops
  - Vessels placed onto ships
  - More than 300 ports in the United States

- Exchange of currency and goods:
- Each additional foot of water means that they have the ability to place 100 additional loads on the container; or on board of the vessel, which means more profit.
Vulnerabilities
Deep Water Port

- Deep Water Port - Deeper depth of water, which lets in larger cargo ships with heavier loads.
- Many Tourists travel near the water ports and cruise ships are always coming in through the ports.
- Port Authority - Secures incoming and outgoing cruise and vessels.
Vulnerabilities
Deep Water Port

• Marine Transportation System (MTS)
• MTS comes up with all the rules and regulations of the open seas
• Other Agencies that secure the Ports include: Military, and Government Agencies
• Companies must follow requirements in the areas of air and water quality, hazardous waste disposal, and aquatic species protection.
Vulnerabilities
Deep Water Port

Example of a Deep Water Port:

- Calypso Deep Water Port - Planned transfer Station
  - Tankers carry liquefied natural gas to dump their load, vaporize the liquid fuel into a gaseous state and send it through a pipeline towards Port Everglades where it will be introduced into the Florida Gas Transmission Pipeline System
  - Offloads Liquefied Natural Gas 7 to 10 miles from the densely populated Galt Mile Beach, it affects every resident of Playa del Mar, the Galt Mile and City of Fort Lauderdale

- Risks: Dangerous and able to affect many different cities
Vulnerabilities
Deep Water Port

• Reason for vulnerability of Deep Water Ports:
  o Economic benefits to the region
  o Way of obtaining resources
  o Possibility of mass casualties, which would affect a large number of people and merchandise
  o Security Measures can mitigate the casualty rates
Vulnerabilities
Deep Water Port

- Recommendation for Security at the Deep Water Port
  - Secure Gas Lines to prevent major damage
## Vulnerability Worksheet

**Target Name:** Cyber Attack

<table>
<thead>
<tr>
<th>Vulnerability Area</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Communication System Level Of Visibility: Assess the awareness of the existence and visibility of SLR’s Communication Systems</td>
<td>3</td>
<td>0 = Invisible, 1 = Very Low Visibility, 2 = Low Visibility, 3 = Medium Visibility, 4 = High Visibility, 5 = Very High Visibility</td>
</tr>
<tr>
<td>2) Criticality of Cyber Attack in SLR Communication Systems: Assess the usefulness of access to local population, economy government, etc.</td>
<td>4</td>
<td>0 = No usefulness, 2 = Moderate usefulness, 1 = Very Low, 3 = Significant usefulness, 4 = Highly Useful, 5 = Critical</td>
</tr>
<tr>
<td>3) Impact Outside of SLR Jurisdiction: Assess the effect loss will have outside of the SLR</td>
<td>3</td>
<td>0 = None, 1 = Low, 2 = Minor, 3 = Medium, 4 = High, 5 = Very High</td>
</tr>
<tr>
<td>4) PTE Access to SLR Communication Systems: Assess the availability of Communication System for ingress and egress by PTE (Potential Target Element)</td>
<td>2</td>
<td>0 = Restricted, 1 = Controlled, 2 = Limited, 3 = Moderate, 4 = Open, 5 = Unlimited</td>
</tr>
<tr>
<td>5) Potential Cyber Attack Threat Hazard: Assess the availability of Cyber Attack possible loss of internet access and all virtual type of communications.</td>
<td>5</td>
<td>0 = None, 1 = Minimal, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High</td>
</tr>
<tr>
<td>6) Potential LJNPS Site Population Capacity:</td>
<td>N/A</td>
<td>0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
</tr>
<tr>
<td>7) Potential for Collateral Mass Casualties:</td>
<td>N/A</td>
<td>0 = 0, 1 = 101 – 250, 2 = 251 – 5,000, 3 = 5,001 – 15,000, 4 = 15,001 – 50,000, 5 = &gt;50,001</td>
</tr>
</tbody>
</table>

### Total Score Rating: 6

**Basic Target Vulnerability Assessment Rating:** Convert total score to a rating number from 1-12 using the following Key. Transfer Final Rating to top right hand box in this form.

- 0-2 pts. = 1
- 3-5 pts. = 2
- 6-8 pts. = 3
- 9-11 pts. = 4
- 12-14 pts. = 5
- 15-17 pts. = 6
- 18-20 pts. = 7
- 21-23 pts. = 8
- 24-26 pts. = 9
- 27-29 pts. = 10
- 30-32 pts. = 11
- 33-35 pts. = 12

- Total = 17
Vulnerabilities
Cyber (1 of 6)

• San Luis Rey is a major telecommunications hub of satellite and internet access.

• Their fiber optic cables and satellites are leased by national and international firms, NGTT cooperation being one of them.

• NGTT cooperation is one of the top five internet access providers in the world and hosts the third largest server farm in the United States.

• Serves hundreds of commercial customers throughout the world.
Vulnerabilities
Cyber (2 of 6)

• The SLR City region has also become the center for several telephone call centers:
  o There are four local television stations
  o Two cable television companies
  o Fourteen radio stations
  o All broadcast & communication services serve the metropolitan region, and all use the SLR satellites.
Vulnerability Analysis Communication Area Map
Vulnerabilities
Cyber (3 of 6)

• Basis of San Luis Rey Cyber Attack
  o A terrorist group of hackers or anyone who wants to put the City of SLR in jeopardy can hack the SLR Communication system to mislead people of SLR and deny them internet access.
  o Potential losses include: millions of dollars by the SLR and companies that leased their satellites and fiber optic systems.
  o Media broadcasting, Communication and Internet access would be lost.
Vulnerabilities
Cyber (4 of 6)

• Existing Security Measures of San Luis Rey Communication Systems
  o Vulnerabilities exploited based on SLR is Medium:
    ▪ NGTT cooperation leased fiber optic cables to provide internet access.
    ▪ Local television stations and several telephone call centers and Broadcasting radios are publicly known.
Vulnerabilities
Cyber (5 of 6)

• Consequences
  o Potential Problems facing SLR include:
    ▪ Potential loss in millions of dollars from the SLR and companies that leased their satellites and fiber optic connections, Internet access, TVs & Radios broadcasting network.
    ▪ Money, Lawsuit, confusion by misleading information broadcasted.
    ▪ Loss of clients, trust and jobs.
Vulnerabilities
Cyber (6 of 6)

• Recommendations
  - Invest in system security and employee training against system breach.
  - Monitor communication system at all times.
  - Conduct test drills periodically to mitigate an actual system compromise.
## Vulnerabilities

### Rating Scale

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Scale Value (1-12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water Dam</td>
<td>12</td>
</tr>
<tr>
<td>Nuclear Power Plant - Supervisory Control And Data Acquisition (SCADA)</td>
<td>10</td>
</tr>
<tr>
<td>Deep Water Port</td>
<td>10</td>
</tr>
<tr>
<td>Airport - EMP air traffic control</td>
<td>9</td>
</tr>
<tr>
<td>Lake Juniper Water Authority - SCADA</td>
<td>8</td>
</tr>
<tr>
<td>Army Base - Dirty Bomb</td>
<td>8</td>
</tr>
<tr>
<td>Cruise Ship - transit mass shooting</td>
<td>8</td>
</tr>
<tr>
<td>Cyber Attack</td>
<td>6</td>
</tr>
</tbody>
</table>
Vulnerabilities

Conclusion

● Overall, we feel that the water Dam vulnerability poses the highest level of risk and there should be a financial commitment to add resources to mitigate that risk.

● After adding all the eight vulnerability worksheets, the vulnerability rating scale for the entire City of San Luis Rey totals to 71.
Risk Assessment

Risk = Likelihood x Consequences

Likelihood = Threat x Vulnerability

OR

Threat / Vulnerability
Risk Assessment

Initial Risk Assessment of The City of San Luis Rey:

IRA = 30%
(High) Low - Medium

<table>
<thead>
<tr>
<th>Qualitative</th>
<th>Quantitative</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>81 - 100%</td>
</tr>
<tr>
<td>Medium - High</td>
<td>56 - 80%</td>
</tr>
<tr>
<td>Medium</td>
<td>31 - 55%</td>
</tr>
<tr>
<td>Low - Medium</td>
<td>14 - 30%</td>
</tr>
<tr>
<td>Low</td>
<td>7 - 13%</td>
</tr>
<tr>
<td>Very Low</td>
<td>0 - 6%</td>
</tr>
</tbody>
</table>
Risk Assessment

• Reasoning:
  o Lack of existing security policies and procedures
  o Lack of communication between local and federal law enforcement agencies and private securities
  o Lack of organization and training within Police Department
    ▪ In regard to a terrorist attack on the City
  o No Updated Emergency Operation Plan/Disaster Plan

This leaves The City of San Luis Rey with a higher than normal risk level.
The San Luis Rey Emergency Operation Plan (SLREOP)
Disaster Plan

- The San Luis Rey Emergency Operation Plan (SLREOP) allows officials to:
  - Identify operational concepts and procedures to support emergencies
  - Establish procedures for implementing a National Incident Management System (NIMS) and Standardized Emergency Management System (SEMS)
  - Facilitate multi-agency and multi-jurisdictional coordination during emergencies
Disaster Plan
Communication to Public

• Provide clear communication to the community, including:
  o Cause of disaster
  o Hazard and protective info
  o Status of response operations
  o How to get help
  o How to volunteer or assist with recovery
Disaster Plan
Response Priorities and Goals

• Priorities for response
  o Protect life
  o Stabilize incident
  o Conserve Property
  o Environmental protection

• Goals for response
  o protect safety of citizens, emergency responders and the public
  o Save and protect critical infrastructure
  o Protect business and residential property
  o Restrain the spread of environmental damage
Disaster Plan
Cyber Security Recommendations

• Implement a Cyber-Security Awareness Month
• Provide free antivirus
• Avoid connecting Critical Infrastructure systems to the internet.
• Perform regular backups of critical systems and store in an off-site location
Disaster Plan
Nuclear Attack Recommendations

● Address immediate medical concerns

● Perform assessment of area for safety
  ○ Check radiation levels

● Make public announcement with safety instructions
  ○ Recommend Shelter-In-Place if appropriate

● Restrict access to areas with unsafe levels of radiation or unsafe structures
Disaster Plan

Water Supply Attack Recommendations

- Assess initial damages and isolate location of problem
- Request support as appropriate (emergency operations personnel and clean up teams); County EOC; FEMA
- Ensure access to clean water supply
- Notify public of safety/health concerns
- Maintain accurate records of access to facilities and preventative maintenance
- Conduct routine diagnostics on SCADA systems
- Implement Access Intrusion Detection Systems
Disaster Plan
EMP Recommendations

• Install Faraday shielding around critical communications facilities at
  o emergency services (police & fire)
  o military base
  o power plant

• Have alternate plan for communications if needed
Disaster Plan
Cruise Ship Attack Recommendations

• Implement Boarding security using L3 ProVision Scanner
• Train Crew in security measures
  o Include use of non-lethal and lethal weapons
• Use Intelligence sharing technology to communicate with relevant agencies
RISK ASSESSMENT AFTER DISASTER PLAN RECOMMENDATIONS

RA after implementing recommendations:

RA = 17%
(Low) Low - Medium
Conclusions

- The top two threats, determined by the CARVER Method, are Electric and Transit
- The top vulnerability, determined by the U.S. Department of Homeland Security, is the Robert Muller Water Dam
- Existing Security Policy and Procedures are lacking, making the measures a vulnerability of San Luis Rey
- Keeping the San Luis Rey Emergency Operation Plan (SLREOP) updated will help bring security policies and procedures to the forefront, allowing agencies to become trained and prepared.
- Implementing recommendations outlined in the San Luis Rey Emergency Operation Plan (SLREOP) and Vulnerability Analysis Section will mitigate risk by 13%
References


References


References


References


