Conducting Effective Physical Security Assessments
Abstract / Objectives

“Physical Security Assessments are paramount to a utilities security program. Securing a company facility is critical for keeping employees safe, minimizing theft or vandalism, and demonstrating an organization’s commitment to security. We will discuss conducting an effective assessment on substations, utility office buildings, and other company facilities. We will highlight establishing an assessment program, the use of threat assessment models, how to document areas to be addressed, and prioritizing and scheduling maintenance items discovered during an assessment.”

- Learning Objective #1: Using a threat assessment model
- Learning Objective #2: Identifying a physical security assessment criteria
- Learning Objective #3: Developing a program, ‘from assessment to completion’
Anthony Hurley - Speaker Bio

• Thirty-seven (37) years in the electric utility industry (VP of Operations / Fortune 200 Company)

• Member, and former Chair of the ASIS International Utilities Security Council (USC)
  • Certified Protection Professional (CPP®)
  • Professional Certified Investigator (PCI®)

• Former Vice-Chair, New Jersey Homeland Security and Preparedness, Infrastructure Advisory Committee (IAC)

• Former Energy Sector Chair, New Jersey Homeland Security and Preparedness, Infrastructure Advisory Committee (IAC)

• Adjunct Instructor, NYU, School of Professional Studies
  • Infrastructure Security and Resilience

• Adjunct Instructor, FEMA Emergency Management Institute (EMI)
  • Master Exercise Practitioner (MEP)

• Member, Infragard (FBI Alliance), Austin, Texas Chapter
Physical Penetration Test
... a true Story
Physical Penetration Test ... a true Story

• Invited to be part of a four-person Physical Penetration Team
  • None of the four PenTest members knew each other prior to the assignment

• Target was a University Campus Building that housed a Bio Laboratory
  • We had six (6) hours to gain access to the building and gather intelligence for an attack
  • Bonus was that if able to get roof access, we would have a clear line of sight to VIP suite at stadium

• Team decided to ‘divide and conquer’
  • Two team members travelled to target building to start gathering intelligence
  • Two team members researched the building online

• After just two hours, we had an entry plan

• Upon a successful entry, team spilt up again and for two hours gathered intelligence
  • Accessed target building (past the guard that was stationed at the lobby security counter)
  • Had free access to most building areas, including the electrical and communications rooms
  • Was able to get the bio laboratory to open their secured door
  • Gained access to the roof

Director of Security wanted to know one thing. How did we do it?
Physical Penetration Test ... a true Story

• Research intelligence team identified:
  • List of faculty that worked at the building, including one doing studies abroad
  • List of classes that were taught at that building and schedules

• Site intelligence team identified:
  • One security guard at main entrance
  • Interior construction at the site required construction material being stored on the rear dock area

• Female team member carried a box labeled with name of the faculty working abroad
  • As she approached, arms filled, guard ran and opened the door for her, and even walked her over to the elevators
  • She went to the basement, opened dock area doors, and our other team members joined her
  • Members put on vests and hard hats, and took clipboards from the construction area (no ID badges)
  • Members freely walked around building, and gathered intelligence, taking lots of pictures
  • Maintenance employees opened electrical and communications rooms for us
  • Female team member knocked on bio laboratory door and a male student opened it
  • We then accessed roof with the help of a maintenance employee
  • Team members then exited without incident, regrouped and analyzed the information

How did we do it? A combination of social engineering, manipulating human nature, and leveraging assumed authority.

All the technology and processes in the world are useless if individuals fail to follow the established procedures and protocols.
Utility Critical Infrastructure
What is Critical Infrastructure (CI)?

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

https://www.dhs.gov/critical-infrastructure-sectors
Utility Critical Infrastructure

Critical Infrastructure Security and Resilience

Of these sixteen (16) critical infrastructure sectors, utilities has assets in five (5) of these sectors.

These are, Energy, which is electric and natural gas; Dams, those that have hydroelectric capabilities; Nuclear reactors, materials and waste; the Water and Wastewater systems, which may operate under the same company or Public Works organization, or may operate as a separate entity; and Communications, which includes telecommunications, and related backbone infrastructure.
Critical Infrastructure Sectors (Utilities)

**Chemical Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

**Commercial Facilities Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

**Communications Sector**
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector-Specific Agency for the Communications Sector.

**Critical Manufacturing Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

**Dams Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

**Defense Industrial Base Sector**
The U.S. Department of Defense is the Sector-Specific Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

**Emergency Services Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

**Energy Sector**
The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.
Critical Infrastructure Sectors (Utilities)

- **Financial Services Sector**: The Department of the Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.
- **Food and Agriculture Sector**: The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.
- **Government Facilities Sector**: The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.
- **Healthcare and Public Health Sector**: The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.
- **Information Technology Sector**: The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.
- **Nuclear Reactors, Materials, and Waste Sector**: The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.
- **Transportation Systems Sector**: The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.
- **Water and Wastewater Systems Sector**: The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Utility sectors highlighted
National Rural Electric Cooperation Association (NRECA)

Electric cooperatives serve:

• 42 million people
• 47 states
• Covers 75% of the U.S.
Why do I need to secure my property and facilities?
The point is that most criminals do not care, and may be targeting your assets for no other reason than it is a power company asset.

Question?

If I were to show you a picture of a substation transformer, which has no distinguishing identifiers, could you tell me;

• What electric company owned it?
• What critical customers it serves 10 miles away?
• If just down the street a teenager is planning to break in to steal copper?
• If there is an upset individual that is planning to damage this asset because their brother lost their job at a power company in another state?
Potential Intruders and Attackers

Know your potential enemy and their tactics

- Individuals seeking financial gain
  - Material theft (i.e. metals/copper, tools, computers, vehicles, personal items, etc.)
  - In extreme cases:
    - Theft of intellectual property / Industrial Espionage
    - Kidnapping / Ransom

- Workplace Violence
  - Domestic Situations

- Domestic Terrorists
  - Animal Rights Activists
  - Environment Activists
  - Sovereign Citizen Movement
  - Hate Groups

- Individuals with a political or religious agenda

- International-based Terrorists

Beware of ‘no one would be interested in my utility’ syndrome
Why would someone enter my facilities?
Know your potential criminal / enemy!!!

• For financial benefit (theft)
• To make a political statement (hanging a banner on a power plant smokestack, etc.)
• To steal intellectual property (laptops, files, etc.)
• Domestic dispute
• Due to your company’s name recognition
• Your company’s name (namesake)
  • American ....
  • National ...
  • U.S. ....
• No reason at all, except to say that they did it (like painting a name on a water tower)
• In extreme cases, to cultivate terror
The goal of an industrial security plan is to deter a threat from attacking. If that is not possible, we must detect the intruder(s) and assess their intent so that we can initiate an appropriate response. We must delay the intruder while we wait for an appropriate force to respond and restrain the intruder(s).
Soft Targets vs. Hard Targets
Intrusion / Attack Cycle

**Attack/Intrusion Planning Cycle**
- Broad Target Selection
  - Planning, Attack/Intrusion and Escape
  - Intelligence Surveillance and Mining
  - Specific Target Selection

**Intelligence Collection Cycle**
- Planning and Assignment
  - Verification
  - Analysis
  - Processing
  - Research and Collection
Soft Targets vs. Hard Targets

Soft Target

- A ‘soft target’ is an individual, facility or asset that is not protected by hardened security measures. For those soft targets that are commercial facilities, the nature of their operation requires that they be open and accessible to the public.

Examples are:

- **Office Buildings w/ Walk-in Centers** *
- **Electrical Substations (depending on technology)** *
- **Transmission Structures** *
- Hotels / Resorts / Restaurants
- Malls / Shopping Centers
- Hospitals / Nursing Homes
- Theatre Halls / Theaters / Concert venues / Sporting Arenas
- Subway / Railway Systems
- Places of religion

* Utilities
Soft Targets vs. Hard Targets

Hard Target

- A ‘hard target’ is an individual, facility or asset that is protected by security measures that have been designed to offer an appropriate layer of protection. Hard targets that are commercial facilities have restricted access and operations, and are controlled with technology or security personnel.

Examples are:

- **Power Generation Stations**
- **Nuclear Power Plants**
- **Electrical Substations (depending on technology)**
- **Office Buildings w/ Transmission Control Rooms**
- **Docks at power plants**
- Military Bases
- Refineries / Oil / Gas Terminals
- Research Facilities
- Federal Buildings / Embassies

*Utilities
Layered Approach to Security
The Layered Approach to Security
How many interpret ‘layered’

- Many interpret a layered approach to security as physical barriers.
- For the outer perimeter, they utilize fencing, and natural or constructed barriers such as creeks and landscaped walls. They may control the access to a facility's grounds through the use of technology, or security personnel.
- Building exteriors are protected by either locked access doors, or are controlled with technology such as card readers or security personnel. Lighting, sensor, and camera technology can be used as well.
- Building interiors may offer an additional layer of security, through controlled door and elevator access, and technology which restricts access to certain internal areas and rooms.
The Layered Approach to Security

Robust ‘layered’ security

- **Intelligence**, which you have the ability to access and evaluate, can serve as your outermost layer. It provides your security organization with trends and models that allow you to evaluate your security plans and determine if your measures are appropriate. If not, in advance you may want to revise if warranted.

- **Partnerships**, with similar industries, other security professionals, law enforcement, and homeland security professionals, allow you to share intelligence concerns, and validate that countermeasures and protocols are appropriate for the current threat status.

- **Awareness Programs** empower employees, contractors, neighbors, and vendors to serve as a layer of security just outside of your facilities physical perimeters.
Using a threat assessment model
Some Common Assessment Tools

- CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability)
- HITRAC (Homeland Infrastructure Threat & Risk Analysis Center)
- RAMCAP (Risk Analysis and Management for Critical Asset Protection)
- MSRAM (Maritime Security Risk Analysis Model)
- NPRA/NPI (National Petrochemical & Refiners Association/American Petroleum Institute)
- USDHS Infrastructure Survey Tool (USDHS/IST)
- Many more …
- Some custom a variation to fit the needs of their organization
Protective Security Advisors (PSA’s)

Protective Security Advisors (PSA’s) are part of the U.S. Department of Homeland Security, Office of Infrastructure Protection. The PSA program was created to provide subject matter experts who are trained in critical infrastructure protection and vulnerability mitigation.

They work with other Department of Homeland Security agencies, advise and assist state, local, and private sector officials and critical infrastructure facility owners and operators.

https://www.dhs.gov/protective-security-advisors

Do you know who you are Protective Security Advisor is?
Protective Security Advisors (PSA’s)

Primary mission is to proactively engage with federal, state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect critical infrastructure. A few of interest to you include:

- Planning, coordinating, and conducting security and resilience surveys and assessments.
- Planning and conducting outreach activities and providing access to critical infrastructure security and resilience for critical infrastructure owners and operators.
- Conduct joint site visits and vulnerability assessments of critical infrastructure assets with the Federal Bureau of Investigations, and the United States Secret Service to provide vulnerability assessments, security planning, and coordination during National Special Security Events (NSSE’s) and other large-scale special events.
Identifying a physical security assessment criteria

Example of one tool: CARVER + Shock
Criticality

• What is the level of impact on our operation if this asset was crippled today?

• What is the morbidity, mortality, economic, and/or environmental impact on this critical infrastructure if damaged?
Accessibility

- What is the openness of the target?
- How easily can they conduct reconnaissance and gather Intelligence?
- How available is facility information online?
- Can they gain unauthorized access to the facility?
- Can they conduct an intrusion or attack?
- Can they exit undetected?
- What are the existing and functioning security measures?
- What is the likelihood the threat can accomplish their intended goal by entering this facility/asset?
Recuperability

• How long would it take to mitigate the effects of the intrusion / attack?
  • Response times
  • Are there alternate method's of providing this service?
• What precautions are already in place?
Vulnerability

• Do they have the motivation, and willingness to accept the risk of conducting the intrusion / attack to attain their desired effect?

• Do they have the true capability to orchestrate the intrusion / attack?

• Do they possess:
  • Expertise
  • Funding
  • Supplies
  • Manpower
  • Equipment
Effect

• What are the long term ramifications of an intrusion or an attack on the specific asset or facility?

• How well will the company be able to operate without this asset or facility in service?

• Are there impacts related to;
  • Political, such as agency and regulatory oversight
  • Economic, and the business ability recover
  • Public opinion / Brand reputation
  • Environmental
Recognizability

• The ease by which the threat can recognize the target component during the conditions under which they must attack.

• Can the threat recognize the target by a method other than sight.
Shock

• Although many intrusions do not have any significant national or even local exposure, what if an intruder conducted an incident that devastated a community.

• Shock is the result of a combination of the following:
  • Physical, Psychological, and Economic effect caused by the damage to the targeted asset and/or facility
  • How the effects of this damage is magnified by national exposure of the event and how that can be exploited by the threat
Developing a program, from ‘Assessment to Completion’
Vulnerability Assessments

\[ R = C \times T \times V \]

- \( R \) = Likelihood an event will occur
- \( C \) = Consequence (Impact)
- \( T \) = Threat
- \( V \) = Vulnerability

Risk Assessments add the probability that the threat will actually intrude / attack.
Conducting Risk & Vulnerability Assessments

- Identify the asset(s) that you intend to conduct the assessment on.
  - Identify the operational processes at this location
  - Identify a thorough inventory of critical assets
  - Identify potential consequences for that specific asset location

- Identify the specific threat scenario (mode of intrusion/attack) for each asset
  - Methodology that would likely be used to intrude/attack (the how?)
  - Motivation behind the intrusion/attack (the why?)
  - Identify all existing security measures that are in place, and their effectiveness
  - Consider information from law enforcement and intelligence from agencies

- Vulnerability
  - How vulnerable are the specific assets to the specific threats that were identified?

- What are the consequences for this location?
  - Will there be loss of life or injuries?
  - What would be the financial impact to the corporation?
  - Is there a key product that would not be available?
Planning the Assessment

- Select an assessment team that is robust, and comprised of team members from different levels of the organizations and disciplines. Examples would be:
  - Leadership from the specific facility
  - Key employee(s) from the specific facility
    - Manager / Employee (from all shifts)
    - Maintenance worker / Security Guard
  - Contract subject-matter experts (i.e. Security, architect, engineer, former military, etc.)
  - Crime subject-matter experts, such as Law Enforcement

- Train the assessment team members on the use of the tool selected

- Establish document control and QA/QC process to ensure data quality

- Advise you perform several ‘practice’ assessments as a team to ensure members are consist and comfortable with the task at hand
Once the assessment is completed

- The assessment tool that you selected generates a ranking / rating that will assist you in identifying the level of importance for each asset
  - Due to the nature of the identified vulnerabilities, keep this information confidential
- You need to decide if the mitigation solutions will be proposed by your assessment team, or an appropriate vendor. If the later, consider having your team involved with the identification and design of the mitigation solutions proposal.
- Inevitably, during your assessment, your team will discover existing security measures that have failed, or have been taken out of service. For each asset, as you propose mitigation solutions, you will need to determine if you will leave this failed security measures offline or have repaired.
- Depending on your organization, you now have to determine how best to propose, gain approval and execute the mitigation plan.
Speakers Contact Information

Anthony Hurley, CPP®, PCI®, MEP
Managing Director, Utility Practice
Witt O’Brien’s, a SEACOR Company

(216) 554-0558
alhurley@wittobriens.com
LinkedIn: https://www.linkedin.com/in/aenergyman/