Risk Assessment & Risk Handling

Risk Assessment

- Risk assessment in general
  - the premises liability of owners has been extended into streets and other public areas ASIS POA, SM, Sect. 7.2.2
  - The ASIS Facilities Physical Security Measures Guideline defines risk management as "a business discipline consisting of three major functions
    - Loss prevention
    - Loss Control
    - Loss indemnification
  - A proactive strategy for security/risk mitigation supports sustainable, healthy, productive organizations and is a critical responsibility of senior leadership and governing boards ASIS GDL FPSM-2009,
  - Risk assessment was developed in the insurance industry ASIS CSO.1-2013, Sect.
  - Informed decision making is the basis of risk management ASIS POA, PS, Sect. 1.2
  - Boards of Directors, shareholders, stakeholders, and the public expect organizations and agencies to ASIS POA, PS, Sect. 1.2
    - Anticipate risks
    - Manage risk
    - Have a protection strategy
    - Respond to threats
  - A senior executive should be responsible for all of the organization's security/risk strategy ASIS CSO.1-2013, Sect.
  - The senior security executive should be able to protect both tangible and intangible assets
    - Intangible Assets:
      - Brand (Trademarks, reputation, Loyalty)
      - Market Position (Customer lists, Legal Monopolies, Licenses, Contracts)
      - Business System (Trademarks, reputation, Loyalty)
      - Knowledge (Trademarks, reputation, Loyalty)
  - *Risk*: An uncertain situation with a number of possible outcomes, one or more of which is undesirable ASIS CSO.1-2013, Sect.
  - Risk includes all negative events for an organization, their *impact*, *likelihood, and* how soon they may occur (*imminence*)
    - Risk assessment defines and quantifies all these risks
  - Risk assessment techniques maybe
    - Heuristic(ad hoc)
    - Inductive(qualitative) (bottom-up approach)
      - Risks identified at the beginning of the analysis

        - Identified risks are the starting point, not the result
        - This method may produce incomplete results
        - This method makes use of "event trees" that trace an initiating event through a sequence with different possible outcomes
        - Does not readily lend itself to feedback loops in the event trees
        - This method focuses on scenarios, which may fail to account for concurrent attacks
    - Deductive(quantitative) (top-down approach)
        - Risks result from a systemic, deductive, top-down approach
        - Uses "logic diagrams" and " fault trees" along with event trees
- Societal risk: When an entire population is at risk

ASIS POA, PS, Sect. 1.

- Risk management
    - Systematic
    - Statistically-based
    - Holistic
    - Employs formal risk assessment and management
    - Addresses sources of system failures
- Risk assessment is part of the risk management process
    - Risk assessments attempt to find answers to three, primary questions
        - What can go wrong?
        - What is the likelihood of it going wrong?
        - What is the impact if it goes wrong?
    - Risk management attempts to answer four, primary questions
        - What can be done about identified risks?
        - What options are available?
        - What are the associated tradeoffs of the options?
        - What are the impacts of current management decisions on future options?

ASIS POA, PS, Sect. 1.2

- Risk assessment helps identify threats, assets, and vulnerabilities through a systematic, defensible process

- Risk assessment involves
    - Identifying internal and external threats and vulnerabilities
    - Identifying the probability and impact of an event arising from such threats or vulnerabilities
    - Defining critical functions necessary to continue the organization's operations
    - Defining the controls in place necessary to reduce exposure
    - Evaluating the cost of such controls

ASIS POA, PS, Sect. 1.2

- Risk formula R = T x A x V
    - R = residual risk
    - T = threat, a combination of threat definition and the likelihood of an attack
    - A = asset to be protected
    - V = vulnerability, represented by system effectiveness

ASIS POA, PS, Sect.

    - Risk management is a key concept in PPS design
        - Risk Management (ISO): "Coordinated activities to direct and control an organization with regard to risk"
        - Although definitions of risk management vary, they generally agree that it relies on
            - Risk assessment (which relies on vulnerability assessment)
            - Threats
            - Asset value
            - Vulnerability

- Major types of risk assessment
  - Quantitative(hard numbers, history, statistics, etc.)
  - Qualitative("feel", predictions, experience, etc.)
- Security typically relies on qualitative, not quantitative, assessment

ASIS POA, PS, Sect. 1.2

- Risk is expressed in
  - Threat
  - Consequence (impact)
  - Vulnerability (likelihood, probability)
- Risk Analysis includes
  - Risk Assessment
  - Risk Evaluation
  - Risk Management Alternatives

ASIS GDL GSRA 11 2002, Sect. IX

- The recommended approach for conducting general security risk assessments
  - Understand the organization and identify the people and assets at risk
  - Specify loss risk events/vulnerabilities
  - Establish the probability of loss risk and frequency of events
  - Determine the impact of the events
  - Develop options to mitigate risks
  - Study the feasibility of implementation of options
  - Perform a cost/benefit analysis

ASIS GDL GSRA 11 2002, Sect. X

- The value of risk analysis depends on the skill of the analysts

ASIS GDL GSRA 11 2002, Sect. A2

- Higher risk in high rise buildings
  - More people = more property, and more property = more opportunity for crime
  - More people = more chances of crime internally
  - More people = more anonymity
  - Easy access to the public in CBD's –easy access to mass transit
  - Elevators and stairwells can be risky places
  - Risky, neighboring tenants
  - Tough to control threats and respond to incidents (too many people and the environment is complex)
  - Evacuations are very difficult
  - The most critical threats in high-rise structures include
    - Fire
    - Explosion
    - Contamination of life-support systems such as air and potable water supplies

ASIS POA, AP, Sect. 2.2.1 & Sect. 2.2.2

-
  - The ability to mitigate threats for high-rise structures depends on
    - Its structural design
    - The use of technology to
      - Deter and detect a threat
      - Communicate a threat's nature and location
      - Initiate automatic or organizational responses

ASIS POA, AP, Sect. 2.2.1

❖ Assets

- Three general types of assets:
  - People
  - Property
  - Information

- Tangible assets can be seen, touched, or directly measured in
  - Facilities/buildings
  - Equipment
  - Inventory
  - Vehicles
  - Raw materials
  - Cash/money
  - Accounts receivable
  - Supplies/consumables
  - Telecommunications systems
  - Other capital assets
- Intangible assets can include
  - Reputation/image
  - Goodwill/trust
  - Brand recognition
  - Relationships
  - Vendor diversity
  - Longevity/history
  - Past performance
  - Experience
  - Quality assurance processes
  - Workforce morale/spirit/loyalty
  - Workforce retention
  - Management style
  - Human capital development
  - Liaison agreements
  - Market share
- Mixed (tangible and intangible) assets can include
  - People
  - Intellectual property
  - Knowledge
  - Proprietary processes
  - Information technology
  - capabilities
  - Land/real estate
  - Infrastructure
  - Credit rating/financial stability
  - Customers (customer base)
  - Contracts in place
  - Financial investments
  - Geographic location
  - Staffing sources/recruiting
  - Certifications (e.g., ISO 9000)
  - Continuity posture/resiliency
  - Safety posture

ASIS POA, SM, Sect. 4.1.1

- The amount of protection required by an enterprise is a function of
  - The value of the asset
  - The risk tolerance of the enterprise

ASIS POA, PS, Sect. 1.7.

- Three general methods of valuing assets
  - Dollars (most important measure)

- Consequence criteria
- Policy (prescribed protection levels)

- Asset value may be expressed in
  - Criticality
  - Consequence of loss
  - Severity

ASIS POA, PS, Sect. 1.5

- Loss isn't measured just by replacement –it includes lost income, sales, downtime, etc. (indirect costs)

ASIS POA, SM, Sect. 6.1

- Threats and loss events
  - Security losses are
    - Direct (money, negotiable instruments, property, information…)
    - Indirect (harm to reputation, loss of goodwill, loss of employees, harm to employee morale…)
  - Both direct and indirect costs can be measured in terms of lost assets and lost income
    - Often, a single loss results in both kinds of costs

ASIS POA, PS, Sect. 1.6

- (Lost revenue, Financial losses, Increased insurance premiums, Labor expenses, Deductabilities, Preventive damages, Management time)
- (Negative media, higher wages, Loss of brand loyalty, Poor employee morale, Public relations costs, Negative consumer perception, Loss of insurance coverage, Loss of Shareholder derivative suits)

ASIS GDL GSRA 11 2002, Sect. A1

- *Pure Risks*
  - Crime
  - Natural disaster
  - Industrial disaster
  - Civil disturbance
  - War/insurrection
  - Terrorism
  - Accident
  - Conflicts of interest
  - Maliciously willful or negligent personal conduct

ASIS GDL GSRA 11 2002, Sect.

- *Loss risk event* (threat) categories
  - Crimes
  - Non-crime(human or natural)
  - Consequential

ASIS GDL GSRA 11 2002, Sect. A1

- Safety-related events may have the same impact as security events

ASIS POA, PS, Sect. 1.3

- Threat classes
  - Insiders
  - Outsiders
  - Collusion
- Threat tactic categories
  - Deceit
  - Force
  - Stealth
  - Combination
- Threat Spectrum: A detailed list of threats; the key to determining the Design Basis Threat (DBT)

- Design Basis Threat (DBT): The threat against which countermeasures are designed to protect

ASIS POA, PS, Sect. 1.3

- Types of events or incidents that may occur at a site can be determined by
  - History of previous events
  - Events occurring/occurred at similarly situated sites
  - Events occurring/occurred within the industry (a type of business)
  - Natural disasters common to the geographical area
  - Recent developments/trends

ASIS GDL GSRA 11 2002, Sect. A1

- Historical data to assist in predicting threat likelihood is generally insufficient due to two reasons
  - The information about past losses is unavailable
  - The information about past losses is not organized to permit statistical processing

ASIS POA, PS, Sect. 1.4

- Threat considerations
  - Motivation
  - Tools
  - Competence
  - Knowledge

ASIS POA, PS, Sect. 1.7.2

- A risk analysis that considers the entire threat spectrum must be performed because
  -
  - As the threat capability increases, the performance of individual security elements or the system as a whole will decrease

ASIS POA, PS, Sect. 1.7.4

- Probability of Loss formula $P = f / n$
  - P = Probability
  - f = Statistical data (how often the event has previously occurred)
  - n = Total number of "experiments" seeking the event (i.e. days of the year, etc.)

ASIS GDL GSRA 11 2002, Sect. A2

- Cost Abatement: Coverage of losses by insurance
  - Insurance pay-off should be subtracted from the total loss of an asset
  - Insurance payments/premiums should reduce the insurance pay-off
- Consequence criteria can be determined through the use of a "consequence table"

ASIS POA, PS, Sect. 1.6

- Data sources for assessing the probability
  - Crime analysis: Looks at crimes that have defeated countermeasures, and
    - When they occurred
    - How often they occurred
    - The impact of their occurrence
    - Revised countermeasures to prevent further occurrences

ASIS POA, SM, Sect. 8.3

- Probability factors for threats and loss events
  - Physical environment (neighborhood/vicinity)
  - Overall geographical location

- Social environment
- Political environment
- Economic environment
- Historical experience for the organization
- Historical experience for the industry
- Procedures and processes
- Criminal state-of-the-art

ASIS GDL GSRA 11 2002, Sect. A1 & Sect. A2

- Criminal state-of-the-art is a major probability factor
- Threat likelihood may be expressed in
  - Frequency
  - Probability
  - Qualitative estimate

ASIS POA, PS, Sect. 1.3

- Consider all the "environments" when determining the probability
- Vulnerability testing the PPS
- Vulnerability: A weakness that can be exploited by an adversary
- Vulnerability assessment: The process of identifying and quantifying vulnerabilities
- Vulnerability analysis: A method of identifying the weak points of a facility, entity, venue, or person

ASIS POA, PS, Sect. 1.7

- A vulnerability assessment is used to determine PPS effectiveness

ASIS POA, PS, Sect. 1.2

- A vulnerability assessment also determines system requirements before design and implementation

ASIS POA, PS, Sect. 1.7.3

- Frequency of vulnerability assessments
  - Before system implementation
  - Upon upgrades
  - Periodic system effectiveness tests

ASIS POA, PS, Sect. 1.7

- A threat exploits a vulnerability to compromise an asset
- Vulnerability assessment team
  - Team leader: A security specialist experienced in security systems design and project management
  - Team members
    - Security systems professional
    - A response expert
    - A data analyst
    - Operations representatives
    - Subject matter experts, such as…
      - Technical writers
      - Locksmiths
      - Explosives personnel
      - Safety or EH & S
      - Legal
      - IT professionals

A vulnerability assessment should include, at a minimum

- Facility and operations description ("facility characterization")
- Threats and assets
- Constraints related to the VA or the site

- Existing countermeasures
- Vulnerabilities in countermeasures
- Baseline analysis of system effectiveness
- Recommendations for countermeasures improvement
- Analysis of expected improvements

ASIS POA, PS, Sect. 1.7.3

- A site survey is part of the vulnerability assessment

ASIS POA, PS, Sect. 1.7.

- Tests
  - Functional testing (components are performing as expected)
  - Operability testing (components are being used properly)
  - Performance testing (repeats tests to determine component effectiveness against different threats)
- Testing conditions
  - Day vs. night
  - Different times of the year/seasons
  - Operating hours vs. non-operating hours, shift changes
  - Different weather conditions
  - Normal operations vs. duress operations (emergencies, labor strikes, etc.)

ASIS POA, PS, Sect. 1.7.3

- Testing approaches
- Compliance-based
  - Conformance to specified policies or regulations
  - "Feature-based" approach
  - Effective only for low threats, low loss impacts, and CBA-supported cost decisions
  - Easier to perform
  - The metric for this analysis is the presence of the specified equipment and procedures
- Performance-based
  - Evaluates how each element of the PPS operates

ASIS POA, PS, Sect. 1.7.

- A six-step process for performance-based vulnerability assessments
  - Create an adversary sequence diagram for all locations
  - Conduct a path analysis
  - Perform a scenario analysis
  - Complete a neutralization analysis, if appropriate
  - Determine system effectiveness and risk
  - Develop and analyze system effectiveness upgrades (if the risk is unacceptable)

ASIS POA, PS, Sect. 1.7.4

- Three general steps of the "systems approach to problem-solving "
  - Vulnerability Assessment
  - Countermeasures
  - Implementation

ASIS POA, PS, Sect. 1.1

- The biggest mistake made when conducting a VA is to concentrate on individual PPS components and address upgrades only at that level, not at the level of the overall system

- Three primary functions of a PPS to be tested
  - Detection measures
    - Probability of detection
    - The time required to report and assess alarms
    - Includes entry controls
      - Throughput
      - False acceptance rate
      - False rejection rate
  - Delay measures
    - Layers of security sum up to total delay time
    - Delay time considered after detection
  - Response measures
    - Time to interruption of the adversary
    - Accuracy of deployment
- An effective assessment system provides two types of information
  - Whether the alarm is valid or a nuisance
  - Key details about the cause of the alarm (what, who, where, how many)

ASIS POA, PS, Sect. 1.7.3

- Vulnerability assessment methods
  - CARVER + Shock Vulnerability assessment
    - Developed by the U.S. Government during WWII as a targeting process
    - Declassified in 2003
    - **C**riticality (impact of attack)
    - **A**ccessibility (ability to get in and out)
    - **R**ecoverability (the ability of the target to recover)
    - **V**ulnerability (ease of compromising target)
    - **E**ffect (direct loss)
    - **R**ecognizability (target identifiability)
    - **Shock**(combined health, economic and psychological impacts)

ASIS POA, PS, Sect. 11.3.1

  - The Vulnerability Identification Self-Assessment Tool (ViSAT) (DHS)
    - Evaluates strengths and weaknesses of individual security operations
    - Online; 200 questions
    - Emphasizes a team approach
    - Covers seven areas:
      - The security plan, policies, and procedures
      - Security force and security awareness training
      - Cargo, personnel, and vehicle access control
      - Physical security issues
      - Security technology
      - Communication security
      - Information security
  - Risk Self-Assessment Tool (RSAT) (DHS)
    - Designed for large venues
    - Emphasizes designation of a single person as event security director
    - Each security team member has specific duties

ASIS POA, PS, Sect. 3.2

- Risk management options
  - Mitigation
  - Acceptance
  - Transfer
  - Spreading
  - Avoidance

  - "Risk Financing" = Insurance
-

ASIS POA, PS, Sect.

Risk Handling

- Risk Mitigation
  - Risk can be reduced in three ways
    - Preventing an attack
    - Protecting against an attack
    - Mitigating consequences of an attack
  - Mitigation means reducing consequences
    - Mitigation focuses solely on reducing consequences
    - May be implemented before, during, and after an attack

ASIS POA, PS, Sect. 1.2

-

  - General categories of risk reduction (mitigation) options
    - Equipment and hardware
    - Policies and procedures, management practices
    - Staffing

ASIS GDL GSRA 11 2002, Sect. A1

  - A security countermeasure can be planned if the loss event has the following characteristics
    - The event will produce an actual loss, measurable in some standard medium (money)
    - The loss is not the result of a speculative risk

ASIS GDL GSRA 11 2002, Sect. A2

  - Mitigation strategies must be evaluated by
    - Availability
    - Affordability
    - Feasibility
    - Application to operations

ASIS GDL GSRA 11 2002, Sect. A1

  - Except for certain high-value, irreplaceable items, an organization should base its protection strategies on a realistic, cost-effective rationale

ASIS POA, SM, Sect. 5.1

  - Often overlooked as asset protection tools, procedural controls are the least expensive countermeasures one can employ
    - Revised procedures can enhance security while improving the bottom line for the enterprise

ASIS POA, SM, Sect. 5.2