# Chapters 32/32A – IFPO - CPO

## What is Risk? and What is Risk Management?

# Purpose

- Risk management is to identify potential problems before they occur so that risk may be reduced, transferred or illuminated. Security professionals can provide management with a greater insight into risk and the impact they may have on the organization through strategic, operational and recognizing risk areas.

# Risk

- Risk is a subjective concept that needs to be viewed and quantified on an individual basis.
- Definitions need to be business specific.
- For many security professionals, an all-hazards approach, which includes the possibility of harm to or loss of people, property, reputation, and/or assets caused by an event, offers a good starting point in defining risk for their organization.

# Risk Management Program

- A risk management program is the formal process utilized to quantify, qualify, and mitigate specific concerns an organization may discover or define.
- It is important for the security professional to identify the program in place and understand the approach accepted in a particular company.
- Questions that aid in defining the program include what the assessment process involves and who manages the overall risk program.

# Risk Management Process

- Risk programs may apply to the enterprise or to a specific business line.
- An enterprise approach is a concerted effort by various divisions within a company to measure risk across the company.
- Other programs may focus on key business divisions. These programs tend to address well-defined and known risks with singularly focused mitigation strategies.
- The security professional should understand the requirement behind the program and the overall process so he or she can fulfill the objectives of the overall risk review.

# Risk Program Components

Although the roles and programs will differ, risk programs have several common components:

- **Risk analysis**
- **Risk assessment and risk rating**
- **Risk mitigation**
- **Risk reporting**

- Each component is necessary for a successful program.

# Risk Analysis

- Risk analysis includes identification of the assets to be protected and the risks to those assets.
- Assets are traditionally viewed as:
  - People (employees/customers, etc.)
  - Facilities (owned/leased properties)
  - Property (sensitive documents/financial instruments/vehicles)
  - Reputation (public perception/client perception)
- Risks to assets must be identified before they can be analyzed.
- Risks should viewed from both the internal (company employees/policies, etc.) and external (natural disasters/competitors, etc.) perspectives. The typical risks to the assets listed previously include:
  - Natural disasters (hurricane/flood/ earthquake)
  - Man-made disasters (fire/workplace violence)
  - Criminal behavior (fraud/embezzlement)
  - Terrorism (international/domestic)

# Risk Analysis

- To accurately evaluate risk, a correlation of assets and threats described must be made. The risks should be described in a formal manner and related directly to the asset.
- Each asset should be addressed in context of the risk.
- Potential damage to the asset is linked directly to the specific risk factor that has been analyzed.

# Risk Assessment and Risk Rating

- Once the risk analysis is complete, a measurement of the risk must take place.
- The risk assessment validates the risk and measures the likelihood of occurrence and the extent of the impact the risk could have.
- During the assessment additional risks may be identified as gaps in protection or other process flaws are discovered.
- The risk assessment will measure the following:
  - Qualification of the risk (whether the risk actually exists)
  - Probability (is likely to occur, very likely, not likely at all)
  - Other risks/vulnerabilities to the asset
  - Knock-on effect (e.g., fire in the facility also damages trucks in loading bays)
  - Total effect of risk (probable loss/total maximum loss)
  - After the risk has been validated, the assessment must then measure the probability of an event occurring.
  - This requires a review of all facts related to the risk and asset to assign a high, medium, or low rating of probability.

# Risk Assessment and Risk Rating

- To properly rate probability the following indicators should be reviewed:
  - Previous occurrences (e.g., whether the facility has been prone to fires in the past)
  - Occurrences in the area or business sector (e.g., burglaries in the neighborhood/ protests against like businesses)
  - Activities in the business sector (whether the business is a target based on its product; e.g., animal rights, etc.)
  - Company profile (e.g., whether the company is well known and thus more of a symbolic target)
  - Geography (whether the plant is next to a terrorist target, or likely to be collateral damage to an attack on a neighbor)
  - Risks should be named and probability assigned to those risks.
  - The assessment results should be documented and the risk rated.
  - The risk rating can be a score, such as a point value or a rating of high, medium, or low.
  - This allows the report to be filtered to show risk criticality.

# Risk Mitigation

- The security professional may have a role in every component of the risk program or play only a limited role, but he or she will always have a role in the mitigation portion of all plans.
- The mitigation phase is where we review and plan to minimize the probability and effects of the identified risk to our assets.
- The application of risk mitigants should be goal oriented and designed to mitigate the specific risk identified. The better defined the goals the better the results.
- Mitigation strategies should look at more than just physical security methods. Options such as training, a robust security plan, and implementing policy changes are also valid, strong mitigation tools to be considered.
- The goal of risk mitigation is to minimize the potential impact of the identified risk to the point where the concern of the risk is minimal.
- Some level of risk must always be accepted.

# Risk Reporting

When reporting risk, the security professional should keep the following in mind:

- The written presentation will “live” longer than the oral presentation.
- Understand the stakeholders to whom you will be reporting.
- Where will this report go?
- Present the facts without exemption; there are many reasons for accepting or ignoring risk. Present the findings and proposed plan, and then allow the decision process to begin.
- Include the security survey and other supporting products utilized to identify the facts.
- There is always a measure of risk acceptance—no plan is absolute.
- Remembering to whom you ultimately report and the scope of your role will help create a true summation of the process. The report and the presentation must be fact driven.
- The report should emphasize the threat, the risk (in real terms) that the threat poses to the organization, the suggested steps to reduce the risk, and a summary that relays the frequency of reevaluation.

# The Risk Management Process

**Risk management process**

1. Asset identification and valuation
2. Threat definition
3. Vulnerability assessment
4. Risk analysis
5. Protective measures

This is a continuous cycle that must constantly be reevaluated

# Assets

- The first step in risk assessment is identification and valuation of assets.
- All three types of assets—tangible, intangible, and mixed— should be considered and incorporated into the risk assessment process.
- Each component of the risk management process must be evaluated. This can be done either qualitatively or quantitatively.
- **Qualitative analysis:**
  - An approach which does not use numbers or numeric values to describe the risk components.
    - High, medium, low, critical, negligible, etc.
- **Quantitative analysis:**
  - An approach which uses numeric measures to describe the value of assets or the level (severity or probability) of threats, vulnerabilities, impact, or loss events.
    - Simple scale 1-5 based on severity.

# Threat

- Threats fall into three categories: intentional, natural, and inadvertent.
- **Intentional threats:**
  - Adversaries are judged on their capabilities to cause a loss event and their intentions to do so.
  - Evaluation of intentional threats is based on identification and study of potential adversaries.
- **Natural threats:**
  - Rather than adversary capabilities and intentions, natural threats are typically evaluated using historical trends and statistics.
- **Inadvertent threats:**
  - Include accidents, errors, and omissions.
  - The most overlooked or neglected threats are inadvertent threats.
  - People make mistakes, and those mistakes are the most likely things to hurt an organization.
  - Inadvertent threats are the most difficult to predict and prepare for.
  - The best defenses are preparation, education and awareness, and realization that the threat exists.

# Vulnerability

- One important difference between a threat and a vulnerability is that a vulnerability is a characteristic of the organization or facility. As such, it is generally something over which the organization can exercise at least some degree of control. Threats, by contrast, are usually *outside* the control of the organization.

- Vulnerabilities are measured in term of *observability* and *exploitability*.
- **Observability:**
  - The ability of an adversary to see and identify a vulnerability.
- **Exploitability:**
  - The ability of the adversary to take advantage of the vulnerability once they become aware of it.
- For inadvertent threats, the observability/ exploitability approach is again slightly different. In this case, we measure our vulnerabilities via two questions:
  1. Are we aware of the vulnerabilities?
  2. Are the particular vulnerabilities subject to relevant inadvertent threats?

# Risk Analysis

- The assessor puts all of the information on assets, threats, and vulnerabilities together, and then considers the potential impact or consequences of a loss event.
- Assessments should be performed by a multidisciplinary team of subject matter experts in order to reach credible and justifiable numbers as input to the analysis.
- Need to consider low-probability/high-consequence risks as well as those that are most likely to occur in our workplace.
- Examples of such risks are terrorist attacks and catastrophic workplace violence incidents.

# Risk Matrix

| CONSIDER THE SEVERITY OF INJURY/ILLNESS — RISK ASSESSMENT MATRIX | Very unlikely to happen | Unlikely to happen | Possibly could happen | Likely to happen | Very likely to happen |
|---|---|---|---|---|---|
| Catastrophic (e.g fatal) | Moderate | Moderate | High | Critical | Critical |
| Major (e.g Permanent Disability) | Low | Moderate | Moderate | High | Critical |
| Moderate (e.g Hospitalisation/Short or Long Term Disability) | Low | Moderate | Moderate | Moderate | High |
| Minor (e.g First Aid) | Very Low | Low | Moderate | Moderate | Moderate |
| Superficial (e.g No Treatment Required) | Very Low | Very Low | Low | Low | Moderate |

CONSIDER THE LIKELIHOOD OF A HAZARDOUS EVENT OCCURRING