MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 2.5: Example - Detailed Incident Response Plan

SunPeak Solar Power Substation - Incident Response Plan

This plan outlines procedures for responding to various security incidents at the SunPeak solar power substation. The plan emphasizes a structured approach to minimize damage, ensure business continuity, and facilitate recovery.

I. Incident Classification:

Incidents will be classified according to severity and type:

- Severity: Critical, High, Medium, Low (defined in Appendix A)
- Type: Cybersecurity Incident, Physical Security Incident, Natural Disaster, Insider Threat, Equipment Failure.

II. Incident Reporting:

All incidents must be reported immediately to the Security Supervisor. Use the standardized incident reporting form (Appendix B).

III. Incident Response Team:

The Incident Response Team comprises:

- Security Supervisor (Team Leader)
- IT Security Specialist
- Maintenance Supervisor
- Designated Management Representative

IV. Incident Response Procedures:

A. Preparation:

1. Regular training and drills to ensure team readiness.
2. Maintain updated contact lists and communication protocols.
3. Ensure access to necessary tools and resources.

B. Detection and Identification:

1. Monitoring systems (CCTV, IDS, alarms) will trigger alerts.
2. Initial assessment of the incident type and severity.

C. Containment:

1. Isolate the affected system or area to prevent further damage.
2. Implement temporary security measures (e.g., increased surveillance, access restrictions).
3. For cybersecurity incidents, disconnect affected systems from the network.

D. Eradication:

1. Identify and remove the root cause of the incident (e.g., malware, intruder).
2. Restore compromised systems and data.
3. For physical intrusions, secure the area and gather evidence.

E. Recovery:

1. Restore systems and operations to normal functionality.
2. Conduct a thorough post-incident review.

F. Post-Incident Activity:

1. Complete a detailed incident report (Appendix B).
2. Conduct a thorough post-incident analysis to identify weaknesses and implement corrective actions.
3. Update the security plan based on lessons learned.
4. Inform relevant stakeholders (management, regulatory bodies).

V. Incident Response Procedures by Incident Type:

A. Cybersecurity Incident:

1. Immediately isolate affected systems from the network.
2. Initiate forensic analysis to identify the source and extent of the breach.
3. Restore systems from backups.
4. Implement updated security measures to prevent future attacks.

B. Physical Security Incident:

1. Secure the area and prevent further unauthorized access.
2. Gather evidence (e.g., photos, video footage).
3. Contact law enforcement if necessary.
4. Assess damage and initiate repairs.

C. Natural Disaster:

1. Activate emergency response plan (Appendix C).
2. Ensure the safety of personnel.
3. Assess damage and initiate repairs.
4. Contact relevant authorities.

D. Insider Threat:

1. Initiate a thorough investigation, including interviews and forensic analysis.
2. Implement disciplinary action as appropriate.

3. Review and update security policies and procedures to prevent future insider threats.

E. Equipment Failure:

1. Isolate the affected equipment.
2. Contact maintenance personnel for repair or replacement.
3. Assess the impact on operations and develop contingency plans.

VI. Communication Plan:

- Establish clear communication protocols for internal and external communication.
- Designated spokesperson to interact with media and stakeholders.

VII. Appendices:

- Appendix A: Incident Severity Levels
- Appendix B: Incident Reporting Form
- Appendix C: Natural Disaster Emergency Response Plan

This incident response plan is a living document that should be regularly reviewed, updated, and tested to ensure its effectiveness. Regular drills and training are crucial for ensuring the team's readiness and ability to respond effectively to various incidents.