HANDLING LOCAL INCIDENTS

Craig J. Emerson

Information Security Department
Energy Systems
Protective Services Organization

Submitted to the 18th DOE Computer Security Group Training Conference
Seattle, Washington
April 22-25, 1996

Prepared by the
Oak Ridge Y-12 Plant
Oak Ridge, Tennessee 37831
managed by
Lockheed Martin Energy Systems, Inc.
for the
U. S. DEPARTMENT OF ENERGY
under contract DE-AC05-840R21400

HANDLING LOCAL INCIDENTS

Craig J. Emerson
Information Security Department
Lockheed Martin Energy Systems, Inc.
P. O. Box 2009
Oak Ridge, TN 37830

Introduction

The appropriate handling of local Automated Information System (AIS) security incidents is of a growing concern. With increased network connectivity, some types of incidents have become more prevalent. It is important that incidents are handled consistently from one situation to another. In some cases action must be taken immediately to resolve a situation. The appropriate people must be involved with resolving an incident. In many cases, confidentiality is important and only the people directly involved with the incident need to be included. Failure to take some of these actions could result in compromise of information or could result in a potential lawsuit.

What is an incident?

The DOE Orders describe an incident as an adverse event associated with an AIS that: 1) is a failure to comply with security regulations or directives; 2) results in attempted, suspected, or actual compromise of classified information or loss of data integrity; 3) results in the waste, fraud, abuse, loss, or damage of government property or information; and/or 4) reveals hardware or software vulnerability.

Some examples of possible incidents include but are not limited to the following:

1. any fraudulent action involving an AIS
2. intentional destruction or alteration of a government owned AIS
3. unauthorized non-work-related information (e.g. games, personal business) residing on any government owned AIS
4. processing classified information or connecting to a classified network without an approved Security Plan
5. processing classified information in a manner other than specified in approved Security Plan
6. unauthorized testing of an AIS
7. printer ribbons, cards, diskettes, hardcopy output, magnetic media, etc. inappropriately protected
8. including an authenticator in an automated logon sequence
9. sharing an authenticator
10. masquerading as another user
11. unauthorized disclosure of information

12. viruses, Trojan horses, or worms
13. hacker/crackers or other unauthorized access attempts
14. interruption or denial of service
15. using an AIS for non work-related activities

The Dilemma

The ideal situation for handling incidents would be to have a full time, on call staff of trained individuals. Individuals fluent with various operating systems, backups for these individuals, and support staff would make up the team. Unfortunately, this is not possible for most organizations. In real life, organizations can not afford to keep staff on standby and there is seldom enough technical expertise. In addition, incidents frequently occur at the most undesirable times.

Possible solution

No matter what solution is chosen for the shortage of time and resources, well written procedures describing the process are a must. They are required by the Orders. DOE Manual 5639.6A-1, Manual of Security Requirements for the Classified Automated Information System Security Program, requires that procedures for recording, reporting, investigating, documenting, and responding to AIS security incidents be approved by the Classified AIS Security Operations Manager (CSOM). Equally as important, these procedures must be followed.

Procedures can be divided into three categories. The first describes to the field (i.e. the end-user) what to do when an incident is suspected. The second procedure describes how the incident is handled by the information security organization once they receive notification of the incident. The third could be categorized as guidelines. The guidelines or checklists describe the details of how to handle a specific type of incident.

The shortage of full-time standby personnel to respond to incidents can be managed by appointing an Incident Coordinator. This person should be empowered by management to resolve incidents. Management is still relied on to make the major decisions but the Incident Coordinator can make the day to day decisions. The Incident Coordinator must have a good understanding of the general business operations, must have good overall technical skills, and must have excellent communications skills.

The appointment of an Incident Coordinator can help solve many organizational problems. In some cases management insists on being involved with the day to day resolution of every incident. This is not only a poor use of management skills but it also

ensures that adequately trained backup individuals will not be available. In other cases incidents may be coordinated and handled by whoever receives the initial notification. This results in inconsistent handling of incidents, poor record keeping, and a competitive spirit among the group of security folks.

The Incident Coordinator has a wide range of responsibilities associated with each incident. As soon as the initial notification of a potential incident is received, he evaluates the situation and assigns a response team to resolve the problem. The incident response team is specific for each incident. The team consists of technical experts and support persons that are best suited for the incident.

The Incident Coordinator is responsible for keeping management informed as to the status of the incident as well as involving other appropriate persons. Depending on the incident, people from Human Resources, General Counsel, Operations Security, Classification, DOE, Information Security, and Internal Audit could be involved. If the incident has the potential to involve other sites, the Computer Incident Advisory Committee (CIAC) is notified.

The Incident Coordinator must also be cognizant of situations that involve possible criminal activity. These types of incidents must be reported to outside agencies. The Incident Coordinator then follows the lead of the outside investigator. In other cases, the Incident Coordinator must recognize circumstances that would represent a possible occurrence. These situations must be reported through the appropriate channels very shortly after they are discovered.

The use of an Incident Coordinator helps assure consistency in handling incidents as well as preventing details from being ignored. The use of a data base or other mechanism for tracking incidents helps keep track of them while they are being resolved. Often times a new incident will pop up before others are resolved. In cases like this, it is easy to forget follow up details if they are not properly tracked. In addition, a tracking data base can provide an historical perspective or metric of the numbers and types of incidents.

Finally, the Incident Coordinator assures that the appropriate reporting procedures are followed once the incident has been resolved.

Many people see the handling of incidents as an exciting thing. There is a tendency to charge ahead and get things resolved. This should not be the case. Incidents must be handled according to established procedures. Individuals handling procedures must act in a professional manner. They should not be confrontational during investigations. Finally, the information regarding the

incident must be treated with confidentiality.

Conclusion

The resolution of AIS security incidents must be done in an orderly and consistent manner. By following established procedures, enabling an Incident Coordinator, and acting with professionalism most problems resulting from improper handling of incidents can be avoided.
