META
SECURITY GROUP

Security Incident Response Team (SIRT) Development

Best Practices for Developing a SIRT Framework and Procedures

By Malcolm E. Palmer
Edward P. Moser

Copyright Notice

META Security Group
20464-A Chartwell Center Drive, Charlotte, NC 28236-6862
704.895.0837 fax: 704.895.8165
www.metasecuritygroup.com

Printed in the United States of America.

Warning and Disclaimer

No part of this publication shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from META Security Group. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this publication, META Security Group (publisher and author) assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Table of Contents

List of Figures

Introduction

This research report from META Security Group*, Security Incident Response Team (SIRT) Development*, provides a best practices reference that organizations can leverage to design a SIRT organizational framework and develop SIRT procedures. The insights provided in this report are derived from the considerable "real world" experience gained by META Security Group consultants in developing SIRT organizational frameworks and procedures for many Fortune 1000 clients.

Audience

The audience for this report is primarily members of Information Security teams. In addition, this report can be useful to executive management and business unit owners to enhance communication within the organization, and provide a common understanding of the foundations required for a more effective SIRT capability.

This report assumes a certain level of understanding of incident response approaches, and a basic, but not necessarily an in-depth, comprehension of intrusion detection system (IDS) technologies.

Key Terms

These fundamental terms, used in this report, are defined below.

Baseline Task: One-time pre-requisite task that provides the foundation for a procedure.

False Positive: A result that indicates that a network, device, application, or system appears to be vulnerable or under attack, when in fact it is not.

Incident: An anomalous event that may indicate a security intrusion.

Intrusion: Malicious activity on or directed towards a system, application, network, or network device.

Organizational Framework: An organizational structure consisting of specific roles and responsibilities.

Policy: The broad rules for ensuring the protection of information assets, and for implementing a security strategy or program.

Procedure: Specific, step-by-step guidance and instructions on how to perform specific tasks.

Risk: The likelihood of loss, damage, or injury. Risk is present if a threat can exploit an actual vulnerability to adversely impact a valued asset.

Threats: The activities or actions that could exploit the vulnerabilities in an organization and place information assets at risk.

Vulnerabilities: The holes and weaknesses in information systems and procedures that intruders can exploit.

Premise

A SIRT (commonly referred to as Computer Security Incident Response Team or Computer Emergency Response Team (CERT)) is a multi-disciplinary, multi-departmental response team that provides an organization with a structured, formal capability to respond to actual or attempted intrusions into its IT infrastructure. Moreover, the SIRT typically includes Information Security team members, as well as representatives from other departments that can support a proactive, pre-coordinated response. By going through the process of developing a SIRT capability, an organization can make the hard decisions associated with authorizing and coordinating responses up front, and make implementation of the SIRT capability that much easier. In addition, an organization that regularly exercises and updates its SIRT capability can ensure its response strategy stays up-to-date and effective.

Purpose

The goal of this paper is to identify key considerations that support the establishment of a practical SIRT organizational framework, as well as provide best practices recommendations for developing specific SIRT procedures.

Document Organization

The remaining portion of this Introduction section, that is, the Background portion, discusses the importance of a formal SIRT capability in the “open,” Internet computing era, as well as the typical issues and challenges that must be overcome.

The SIRT Definition section provides an overview of key considerations for defining the SIRT mission, constituents, and capabilities, as well as identifying or establishing the required policy basis.

The SIRT Organizational Framework section discusses how organizations can leverage and augment existing staff resources to design an organizational framework that establishes the necessary SIRT roles and associated responsibilities.

The SIRT Procedures section outlines the baseline and procedural tasks required to develop the SIRT Routine Operations, Incident Response, and Incident Recovery procedures.

Background

In recent years, organizations have faced the challenge of a major computing paradigm shift from proprietary networks and systems architectures to “open” systems with distributed, heterogeneous servers and clients. Distributed computing and Internet environments increase an organization’s efficiency and competitive position in the new, Web-oriented online marketplace. However, due to the nature of these open computing environments, the risks are greater and the threats are increasing. These threats range from novice cyber vandals looking to deface Web sites, to unsavory IT insiders seeking to steal valuable corporate information, to very knowledgeable cyber espionage agents or would-be terrorists with sophisticated attack methods looking to lift critical corporate assets for personal or political gain. This situation was underscored in a 2001 *Information Week* Research Global Information Security Survey of 4,500 security professionals worldwide (Figure 1).

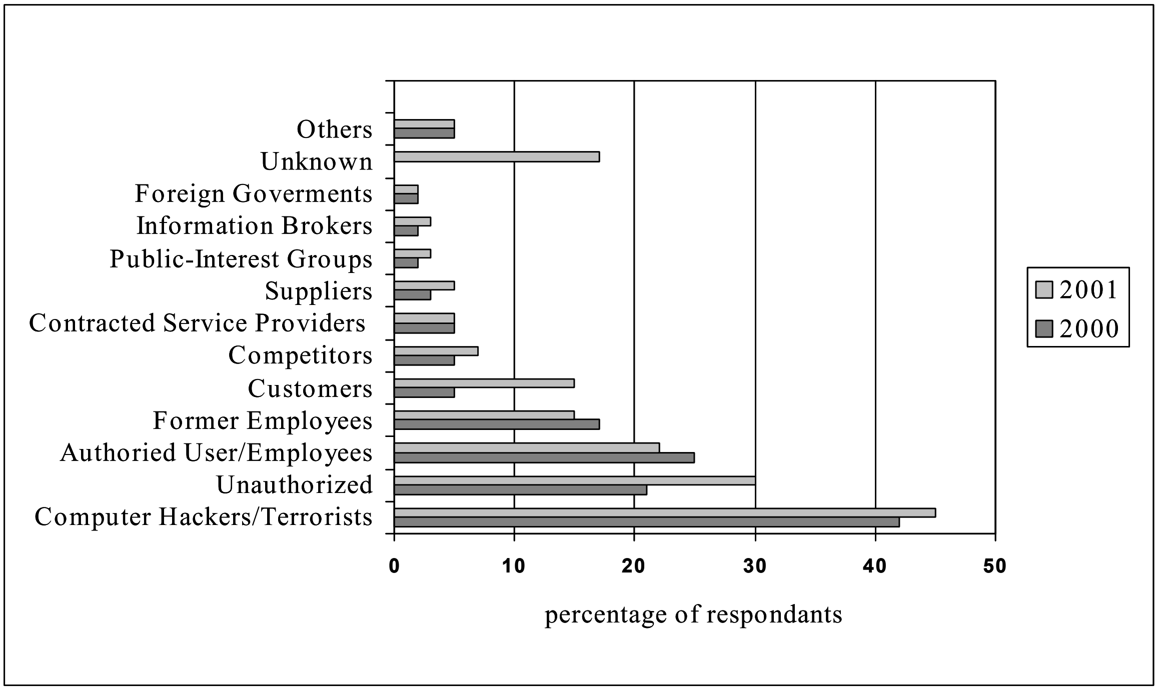

Figure 1: Source of security breaches or espionage

In an effort to quickly detect threat and intrusion activity, many organizations have established monitoring and detection capabilities. In most cases, organizations have deployed host-based and/ or network-based intrusion detection systems (IDS). When an intrusion or anomaly is detected, these IDS tools are usually configured to send alerts and notification (for example, by email, page, console, etc.). Most organizations find themselves overwhelmed by the volume and frequency of the IDS alerts. According to the CERT Coordination Center[1], the 34,754 security incidents reported through the first nine months of 2001 is on pace to double the 21,756 security incidents reported in 2000. Moreover, during a security incident, the staff members are often unsure of what to do, who has authorization to respond, when to do it, how to do it, and who to contact. Time is essential when attempting to contain a security incident.

Although being prepared and knowing what to do in advance can help to mitigate the damage from an incident, META Security Group's extensive experience shows that few organizations have established a formal SIRT capability. (Most have established formal plans to guide recovery from natural or physical disasters). The reasons for this are many and typically deep-seated in the organization. Among the typical, entrenched beliefs and corporate issues that must be overcome to establish a SIRT include:

[1] The CERT® Coordination Center is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

- The belief that purely technical solutions such as a firewall and IDS products will protect the organization.
- The expectation that smart, technically competent people inherently know how to respond to incidents.
- The hope and expectation that the organization will not be attacked, given the vast expanse of the Internet and the number of potential targets to occupy an attacker's time and interest (the "can't happen here" syndrome).
- A misperception that a SIRT requires an "army" of staff members, and each team member may need extensive training.

Let's discuss each of these notions in turn.

The belief that purely technical solutions such as a firewall and IDS products will protect the organization. The new Internet technologies and their attendant business applications operate in an environment of threats that have triggered a veritable tidal wave of Information Security technologies. Many organizations are enamored with these technical solutions and believe they can create an impenetrable defense – or at least one that will occupy an attacker long enough to allow an organization to formulate an effective response without a great deal of advance preparation. While firewalls and other technical solutions may be essential components of an organization's Information Security solution approach, there is no such thing as an impenetrable defense -- at least not one achievable with an acceptable return on investment. In addition, some incidents progress very rapidly from initial exploitation to achievement of system-wide impacts. For example, the denial of service (DoS) attacks featured in the news last year paralyzed many organizations while they scrambled to assemble a response team, develop a plan, and begin defending themselves.

The expectation that smart, technically competent people inherently know how to respond to incidents. Many organizations avoid establishing a formal incident response capability, preferring to rely instead on informal response capabilities. The typical attitude is, "We already have people who can do this as part of their job. We don't need to formally organize to accomplish this." Yet the lack of a formal incident response capability leads to uncoordinated, ad-hoc responses. The most immediate downside to this approach is that the organization will have to deal with response-related surprises (for example, "Who in the company pulled us offline, and why?") or delayed responses.

The "surprise" aspect of this common pitfall can be devastating. Unauthorized and uncoordinated responses may lead to a loss of internal confidence in the Information Security Program or even loss of public confidence in the organization. Incident response planning is an example of where it may not be "easier to ask for forgiveness than ask for permission." The absence of a formal incident response capability greatly increases the likelihood that personnel will either delay responding (while seeking approval to act) or will act independently. The response, under such conditions, will not be as effective as one thought out in advance.

The hope and expectation that the organization will not be attacked, given the vast expanse of the Internet and the number of potential targets to occupy an attacker's time and interest. There is no denying that the Internet is vast and growing at an exponential rate. Attackers have a large number of targets to choose from, and the likelihood of any individual attacker targeting a specific organization is extremely low. Unfortunately, this line of reasoning does not accurately reflect the "threat calculus" an organization must perform. The organizations that were so publicly attacked in recent years discovered that obscurity is not credible defensive strategy. All organizations engaged in e-business, or otherwise leveraging the Internet for internal or external constituencies, have definable exposure to potential attackers. Moreover, another category of threat consists of authorized users, and those who may try to connect to the organization's IT infrastructure through authorized systems. The "invited crowd" gains admittance to the organization's IT infrastructure and may unwittingly, or even knowingly, bring along unwanted "gate crashers". Of course, an attacker also may stumble onto or directly target the organization. Indeed, many would-be malicious intruders regularly scan thousands of sites in an ongoing effort to find vulnerabilities.

A misperception that a SIRT requires an "army" of staff members, and each team member may need extensive training. Many organizations are surprised to discover that a SIRT can be established within the current organizational headcount, or with very limited headcount additions or organizational adjustments (such as designating a SIRT manager to lead the other team members assembled from throughout the organization). From a strategic perspective, the SIRT "harnesses" and organizes, to the maximum extent possible, incident response capabilities and activities already resident within the organization. These typically include IDS initiatives, information system log reviews, and undocumented response procedures, as well as insights derived from disaster recovery team structures and plans, network management systems, and help desk capabilities.

META Security Group recognizes that many organizations have the need for a comprehensive and practical SIRT capability that is designed and developed to address these issues. More specifically, organizations require a phased SIRT implementation that initially establishes the organizational framework and then progresses to the development of specific procedures. Such an organization framework and procedures are outlined in the sections that follow.

SIRT Definition

META Security Group's extensive experience with clients suggests that key factors determining the success of the SIRT must be defined prior to establishing the organizational framework or developing specific procedures. These considerations are

- Policy Basis
- Mission Statement
- Constituents and capabilities

In concert with establishing the policy basis and developing a SIRT mission statement, an organization must define the scope of the SIRT by specifying the constituents that it will serve and the services or capabilities that it will provide. Defining the SIRT in these key areas ensures necessary management support and approval, properly sets expectations and establishes a common understanding within the organization, and serves to support subsequent SIRT efforts such as organizational framework design and procedure development.

Policy Basis

The SIRT must have the support and approval of senior management within the organization. Security policies can provide an effective way to demonstrate and document senior management approval of the SIRT, as senior management typically approves these policies. Without this level of support and approval, SIRT-related initiatives and activities such as organizational framework design and procedure development may be challenged and require individual justification and approval. Further, it is critical to identify the specific objectives and requirements in existing Information Security policies that provide the basis for establishing the SIRT.

If existing Information Security policies do not provide a sufficient policy basis for establishing the SIRT, then they must be revised or developed to include statements similar to the following:

> *Company ABC will develop and exercise formal procedures for responding to Information Security intrusions and incidents. Company ABC must establish associated metrics for gauging the effectiveness of these procedures.*

Mission Statement

The SIRT mission should be documented in a brief yet concise statement that is directly traceable to existing Information Security policies. The SIRT mission statement should consist of a few sentences that clearly outline the purpose and objectives of the SIRT capability. The SIRT typically is not intended to function as the virus detection group, the incident recovery group, physical security response group, or to address minor tactical matters. Moreover, some organizations explicitly exclude anti-virus and incident recovery activities, with the former considered an IT department service, and the latter addressed through a dedicated recovery team.

An organization that will focus on responding to network intrusions may specify a mission statement similar to the following:

> *The Company ABC Security Incident Response Team (SIRT) will establish and maintain capabilities to respond effectively to electronic intrusions into the Company ABC network infrastructure. SIRT analysis and planning activities will support proactive development of authorized, coordinated responses to incidents. The SIRT also will contribute to incident recovery activities after network intrusions are contained.*

In addition, an organization should specify its inclination to litigate, and any legal or regulatory responsibility to prosecute, those that attack or attempt to attack its networks.

Constituents and Capabilities

The SIRT typically will be an organization-wide capability serving a single constituency (that is, the entire organization or company). However, the SIRT may serve multiple constituents within the organization that can be specified in terms of the organization’s geographic locations, headquarters, departments, or business units. In addition, the SIRT also may serve external constituents such as customers, partners, and other SIRTs.

The SIRT will provide its constituents with a range of services and capabilities in the areas of:

- Routine Operation
- Incident Response
- Incident Recovery

Routine Operations

Organizations typically focus on the incident response capabilities when establishing a SIRT. However, the SIRT must include capabilities for conducting routine operations. SIRT routine operations or pre-incident capabilities typically include:

- Detect incidents using automated (IDS tools) and manual (log review) techniques.
- Verify automated responses from IDS tools.
- Validate security incidents and identify false positives.
- Prioritize the severity of valid incidents.
- Initiate SIRT incident response efforts for valid incidents.
- Regularly review information sources to maintain currency with security information (for example, advisories, alerts, news, etc.) that can assist SIRT operations.
- Develop and distribute routine status reports on SIRT activities.

Incident Response Capabilities

Proactive planning and coordination are the primary basis of an effective incident response. The SIRT should develop and exercise pre-coordinated plans for responding to expected or typical types of intrusion events. SIRT incident response capabilities typically include:

- Confirm assigned priority for valid incidents.
- Conduct or execute pre-coordinated response plans based on incident category.
- Determine if incidents have been contained.
- Perform basic forensic process to support security investigations.
- Ensure consistent and timely reporting of response activities.
- Document “lessons learned” to improve SIRT operations.
- Initiate SIRT recovery efforts, if necessary.

Incident Recovery Capabilities

Though many organizations address business recovery and continuity efforts through other dedicated recovery teams, the SIRT can perform these tasks, or provide such teams with valuable insight. For example, SIRT incident forensics activities may identify when a particular vulnerability was introduced, how it was exploited, who exploited it, etc. This information can ensure that recovery efforts do not re-introduce a vulnerability or exposure that has been eradicated. Moreover, SIRT members can provide insight into what IT resources were impacted, potential business impact, and recovery priorities. SIRT incident recovery or post-incident capabilities typically include:

- Document SIRT damage assessment findings.
- Coordinate with teams responsible for recovering impacted systems.
- Ensure consistent and timely reporting of recovery activities performed by the SIRT.
- Document “lessons learned” to improve SIRT operations.

SIRT Organizational Framework

The process of designing an effective SIRT organizational framework hinges on establishing an organizational structure consisting of functional roles and corresponding responsibilities. The SIRT roles and responsibilities are outlined below.

Roles

As illustrated in Figure 2, the SIRT organizational structure consists of management, and core and supporting SIRT roles. These SIRT roles, with the possible exception of the SIRT Operations Manager, can be functionally assigned to existing staff to be performed in addition to their current duties.

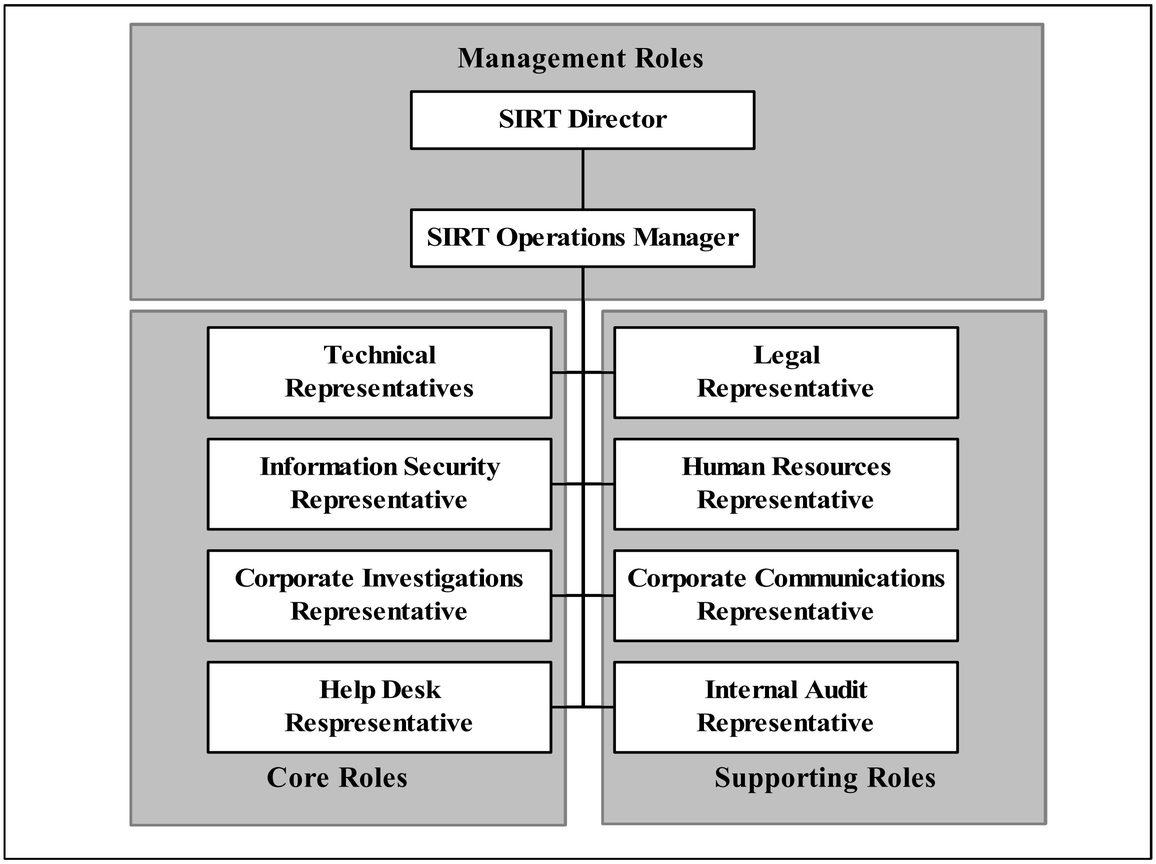
Management Roles
SIRT Director
SIRT Operations Manager
Technical Representatives
Information Security Representative
Corporate Investigations Representative
Help Desk Respresentative
Core Roles
Legal Representative
Human Resources Representative
Corporate Communications Representative
Internal Audit Representative
Supporting Roles

Figure 2: SIRT Organizational Structure

Moreover, the staff members that are assigned the core and supporting SIRT roles only report functionally to the SIRT Operation Manager as it relates to their assigned SIRT roles and corresponding responsibilities.

Management Roles

The SIRT Director role should be assigned to a member of the corporate executive team such as the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or a very senior manager reporting directly to the corporate executive team. If the role of SIRT Director is assigned to an individual at a lower level in the organization (that is, not a member of the corporate executive team or someone who does not report directly to the corporate executive team), then the SIRT organizational structure should include a SIRT Executive Sponsor role as well. The SIRT Executive Sponsor role should be assigned to a member of the corporate executive team. The SIRT Executive Sponsor should provide executive supervision and oversight over the SIRT, as well as interface and communicate with executive management and business owners.

The SIRT Operations Manager should be a dedicated full-time, or nearly fulltime equivalent employee or contractor that reports to the SIRT Director. The SIRT Operations Manager typically is drawn from the Information Security department. Recommended qualifications and skills include well-developed people management skills, a “take charge” approach to tasks, knowledge of intrusion detection approaches, and broad knowledge of security and IT infrastructure technologies and issues.

Core SIRT Roles

The core SIRT roles typically include representatives from key departments within the organization, including:

- Technical Departments
- Information Security
- Corporate Investigations
- Help Desk

These roles are discussed in turn.

The SIRT mission and capabilities largely determine the technical core SIRT roles. For example, an organization that focuses on responding to network intrusions may need representatives from several departments to provide coverage for its network infrastructure, including components such as routers, firewalls, DMZ, WAN, etc.

Another organization that also responds to host-based IDS alerts involving critical servers may include representatives from platform-specific departments such as UNIX, Windows NT, and Novell. In addition, the representative from each of these departments is typically already involved in related activities such as IDS deployment, IDS configuration, log reviews, as well as vulnerability and threat assessments.

The Information Security Representative role is usually fulfilled through the SIRT Operations Manager. However, if the SIRT Operations Manager is not drawn from the Information Security department, Information Security should be represented in a separate core SIRT role, and assigned to a member of the Information Security, IT Security, or similar department. The representative from Information Security is typically already involved in related activities such as IDS configuration, IDS maintenance, log reviews, security resource reviews, as well as vulnerability and threat assessments.

The Corporate Investigations Representative should be assigned to a member of the Corporate Investigations or Corporate Legal team. Many organizations such as financial institutions already have internal capabilities for investigating incidents and performing basic forensics. These capabilities typically focus on physical corporate incidents or incidents involving fraud, misuse, or abuse of corporate assets. Organizations that lack basic internal computer investigation or forensics expertise should consider training and/or retaining computer forensics support from external providers.

The Help Desk Representative should be assigned to a member of the Help Desk, Customer Support, or similar department. Many organizations have implemented capabilities that serve as the focal point for supporting both internal and external customers. These capabilities typically include troubleshooting problems (that is, providing the first level of support, generating trouble tickets, etc.) and providing problem status information. Due to its integral and constant role in communicating and interacting with customers, the Help Desk should be represented in the SIRT as a core role.

Supporting SIRT Roles

The core SIRT roles should be supplemented, as necessary, with team members drawn from departments that support the SIRT functions. The supporting SIRT roles are involved periodically in SIRT operations to provide specific expertise or assistance and typically include representatives from key departments within the organization, including:

- Legal
- Human Resources

- Corporate Communications
- Internal Audit

These roles are discussed in turn.

The Legal Representative should be assigned to a member of the Corporate Legal team. For organizations with an inclination or requirement to prosecute or litigate, this supporting role can provide the SIRT with expertise on litigation as well as preservation of evidence. Organizations that lack the computer incident litigation expertise internally should consider retaining legal support from external providers.

The Human Resources Representative should be assigned to a member of the Human Resource, Employee Relations, or similar department. This representative should be leveraged primarily for his or her corporate policy and procedure expertise, as well as assistance with personnel-related responses to incidents such as disciplinary action and termination.

The Corporate Communications Representative should be assigned to a member of the Corporate Communications, Public Affairs, or similar department. This representative should be leveraged primarily for his or her expertise and assistance with media relations and for communicating proper and consistent data and public relation information about the organization’s responses to incidents.

The Internal Audit Representative should be assigned to a member of the Internal Audit team. This representative should be leveraged primarily for his or her expertise and overall knowledge of compliance to organization’s security policies and procedures.

Responsibilities

To complete the SIRT organizational framework, specific responsibilities should be assigned for the aforementioned SIRT management, core roles, and supporting roles. These responsibilities should be assigned in addition to the duties and tasks specified in the approved SIRT procedures.

Management Responsibilities

The SIRT Director should be assigned responsibilities that primarily involve external management communication and internal SIRT management. Externally, the SIRT Director should be responsible for securing the budget for resources to support the SIRT, representing the SIRT (on management committees, in meetings, etc), and working closely with the management of the departments that are functionally part of the SIRT. In addition, the SIRT Director should interface with execute management and business owners. However, this responsibility should be assigned to the SIRT Executive Sponsor if the SIRT Director is not a member of the corporate executive team or does not report directly to the corporate executive team. Internally, the SIRT Director should be responsible for reviewing and approving the SIRT budget, mission statement, organizational structure, procedures and status reports prior to disclosure or distribution. In addition, the SIRT Director should arrange periodic SIRT exercises including incident simulation and intrusion drills for third-party verification of the SIRT operational and response capabilities.

The SIRT Operations Manager should be assigned responsibilities that range from leading SIRT development efforts to keeping the SIRT Director fully informed. The SIRT Operations Manager should lead efforts to develop the SIRT organizational structure, procedures, and operational budget, as well as conduct post-mortem evaluations to capture lessons learned. In addition, the SIRT Operations Manager should ensure the ongoing execution and performance of SIRT procedures, arrange periodic training for SIRT members, and manage SIRT incident escalations. The SIRT Operations Manager also should prepare and distribute SIRT documentation such as response plans, reports, and advisories that are subject to approval by the SIRT Director.

Core Responsibilities

The Technical Representatives should be assigned responsibilities that focus on representing their respective departments in SIRT operations, communicating SIRT information with their departments, and providing the SIRT with routine operational support. In addition, the Technical Representatives should lead departmental support for SIRT incident detection, assessment and response activities, as well as coordinate 7X24 departmental support to the SIRT. During the development of SIRT procedures, the Technical Representatives should advise the SIRT on strategies for responding to security incidents.

The Corporate Investigations Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations, communicating SIRT information with his or her department, and providing or making arrangements to provide computer forensics capabilities to the SIRT. The Corporate Investigations Representative should lead departmental support for SIRT incident detection, assessment, response and investigation, as well as interface with local, state, and federal law enforcement agencies to facilitate legal responses to incidents. During the development of SIRT procedures, the Corporate Investigations Representative should advise the SIRT on strategies for computer forensics and evidence handling, and provide computer forensics and evidence handling training to other SIRT members. In addition, the Corporate Investigations Representative should coordinate with the SIRT Legal and Technical Representatives to develop or revise the organization’s security policies, standards, and procedures relating to computer forensics, handling of evidence, and legal action.

If the SIRT Operations Manager is not drawn from the Information Security department, Information Security should be represented in a core SIRT role. The Information Security Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations and ensuring that SIRT members have access to and understand the organization’s security policies, standards, and procedures. In addition, the Information Security Representative should assist with development of baseline IDS configurations, and support reviews of available Information Security sources to maintain currency with information (for example, advisories, research findings, etc.) that can assist SIRT operations.

For organizations that have put in place capabilities that serve as the focal point for supporting or interfacing with both internal and external customers, the Help Desk should be represented in a core SIRT role. The Help Desk Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations and communicating SIRT information with the department. In addition, the Help Desk Representative should lead departmental support for SIRT activities, as well as coordinate 7X24 departmental support to the SIRT. During the development of SIRT procedures, the Help Desk Representative should advise the SIRT, in concert with existing troubleshooting and status procedures, on strategies for processing non-routine notifications and responding to security incidents.

Supporting Responsibilities

The Legal Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations, communicating SIRT information with the department, and providing legal advice to the SIRT and executive management. The Legal Representative should advise SIRT and executive management on legal procedures and strategies for security incidents, as well as advise the SIRT Corporate Investigations and Human Resources Representatives on legal strategies associated with the organization’s employees and contractors. During the development of SIRT procedures, the Legal Representative should advise the SIRT on strategies for evidence handling and change of custody. In addition, the Legal Representative should advise the SIRT Corporate Investigations Representative and Technical Representatives on the development and revision of existing security policies, standards, and procedures relating to incident forensics, handling of evidence, and legal action.

The Human Resources Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations, communicating SIRT information with the department, and providing advice and assistance in the development of SIRT procedures. In addition, the Human Resources Representative should interface with management, employees, and contractors to facilitate personnel-related responses to incidents (for example, disciplinary action, termination, etc.).

The Corporate Communications Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations, communicating SIRT information with the department, and providing advice and assistance in the development of SIRT procedures. The Corporate Communications Representative should interface with management and the Help Desk Representative to assist internal communication on incident response and incident status information, as well as lead external communication to the media and public regarding responses to incidents. In addition, the Corporate Communications Representative should educate other SIRT members, management, employees, and contractors on the procedures and guidelines for interacting with the media concerning security incidents.

The Internal Audit Representative should be assigned responsibilities that focus on representing his or her department in SIRT operations, communicating SIRT information with the department, and providing advice and assistance in the development of SIRT procedures. In addition, the Internal Audit Representative should support reviews of available Information Security sources to keep current information (for example, advisories, research findings, etc.) that can assist SIRT operations.

SIRT Procedures

SIRT procedures provide an organization with the step-by-step guidance and instructions needed to establish and manage the SIRT capabilities described in the Constituents and Capabilities Section of this report. As shown in Figure 3, these SIRT procedures should address routine operations, incident response, and incident recovery activities.

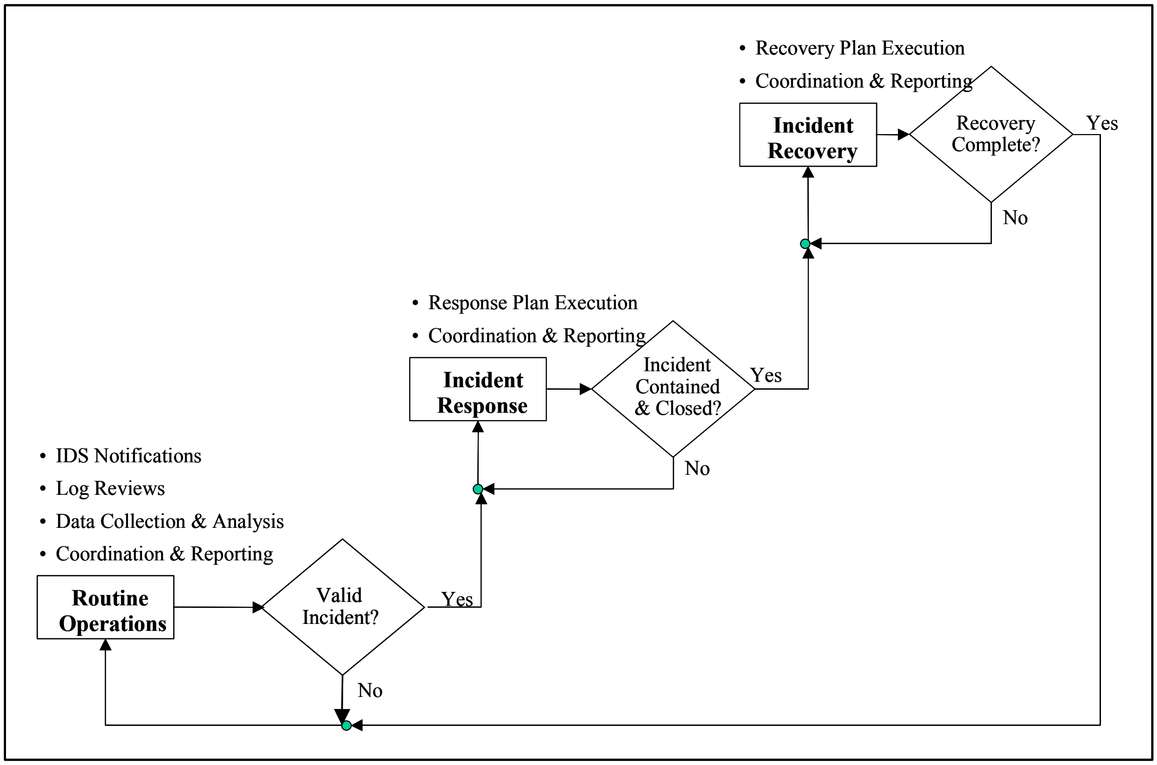
• Recovery Plan Execution
• Coordination & Reporting
Incident Recovery
Recovery Complete?
Yes
No
• Response Plan Execution
• Coordination & Reporting
Incident Response
Incident Contained & Closed?
Yes
No
• IDS Notifications
• Log Reviews
• Data Collection & Analysis
• Coordination & Reporting
Routine Operations
Valid Incident?
Yes
No

Figure 3: SIRT Procedures

Routine Operations

The most effective SIRT capabilities, in addition to their incident response and incident recovery responsibilities, perform routine or daily activities such as processing IDS notifications, reviewing system logs and vulnerability alerts, as well as coordinating and reporting on SIRT activities. The SIRT Routine Operations procedure should consist of the following key sub-procedures:

- Automated Detection

- Manual Detection
- Information Review and Analysis
- Report Preparation

Automated Detection

In an effort to automate the detection of threat and intrusion activity, many organizations have established monitoring and detection capabilities. In these cases, organizations have deployed IDS tools including network and/or host-based sensors. These tools typically are configured to send alerts and notifications (for example, by e-mail, pager, console displays, etc.) when an intrusion or anomaly is detected. However, prior to developing or implementing an automated detection sub-procedure for processing IDS notifications, an organization should perform several baseline tasks including establishing incident criticality categories (that is, number of levels, descriptions, and examples), defining and implementing a standard IDS configuration (that is, attack signatures, automated responses, etc.), and establishing a dedicated SIRT repository for SIRT-related information and documentation (for example, procedures, incident records, reports, IDS configuration, etc).

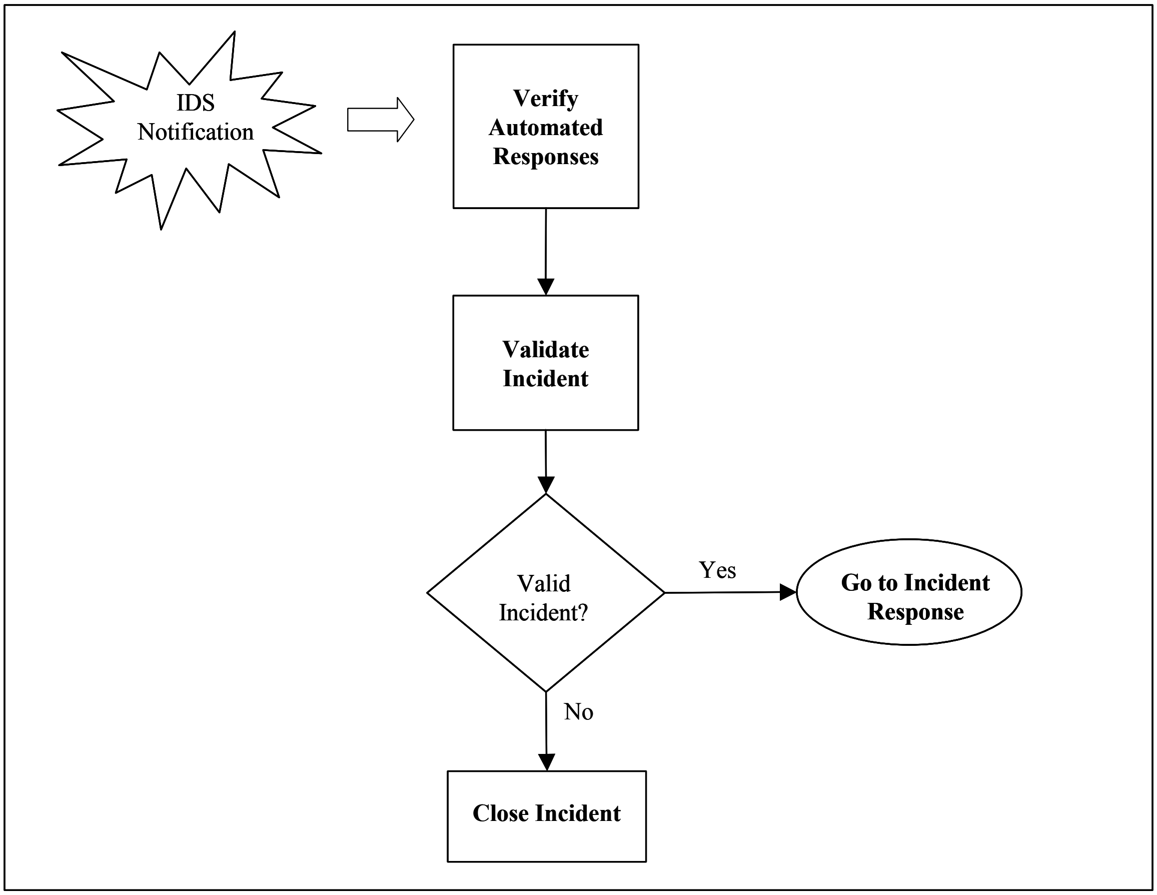

Figure 4: Routine Operations Procedure: Automated Detection

The automated detection sub-procedure should identify the procedural tasks the SIRT performs to routinely process incident notifications from the IDS tools. As illustrated in Figure 4 above, these procedural tasks primarily involve verifying IDS responses and validating incidents. If the IDS tools have been configured for automated response (for example, terminate a session, reconfigure a device, etc.), then the SIRT should confirm that the response was actually performed. Failure by the IDS to respond may require the SIRT to troubleshoot and/or perform the responses manually. In addition, the SIRT should verify that the incident is valid and not a false positive before initiating the SIRT Incident Response procedure. For example, production testing or some device failures on the network may trigger false IDS alerts and notifications.

Manual Detection

Many organizations conduct manual detection activities (that is, reviewing logs) to avoid sole reliance on the IDS tools. However, manual detection should only be performed on critical systems or devices for events the IDS does not detect, and limited to the IT infrastructure that the IDS directly protects. Prior to developing or implementing a manual detection sub-procedure, an organization should perform several baseline tasks, including establishing incident criticality categories (that is, number of levels, descriptions, and examples), identifying logs and information for review (that is, log files, review frequency and methods, incidents and anomalies, etc.), and establishing a dedicated section in the SIRT repository for manually detected incident records.

The manual detection sub-procedure should identify the procedural tasks that the SIRT performs to routinely process manually detected incidents. As illustrated in Figure 5 below, these procedural tasks primarily involve reviewing log files for anomalies, coordinating with the SIRT, and validating incidents.

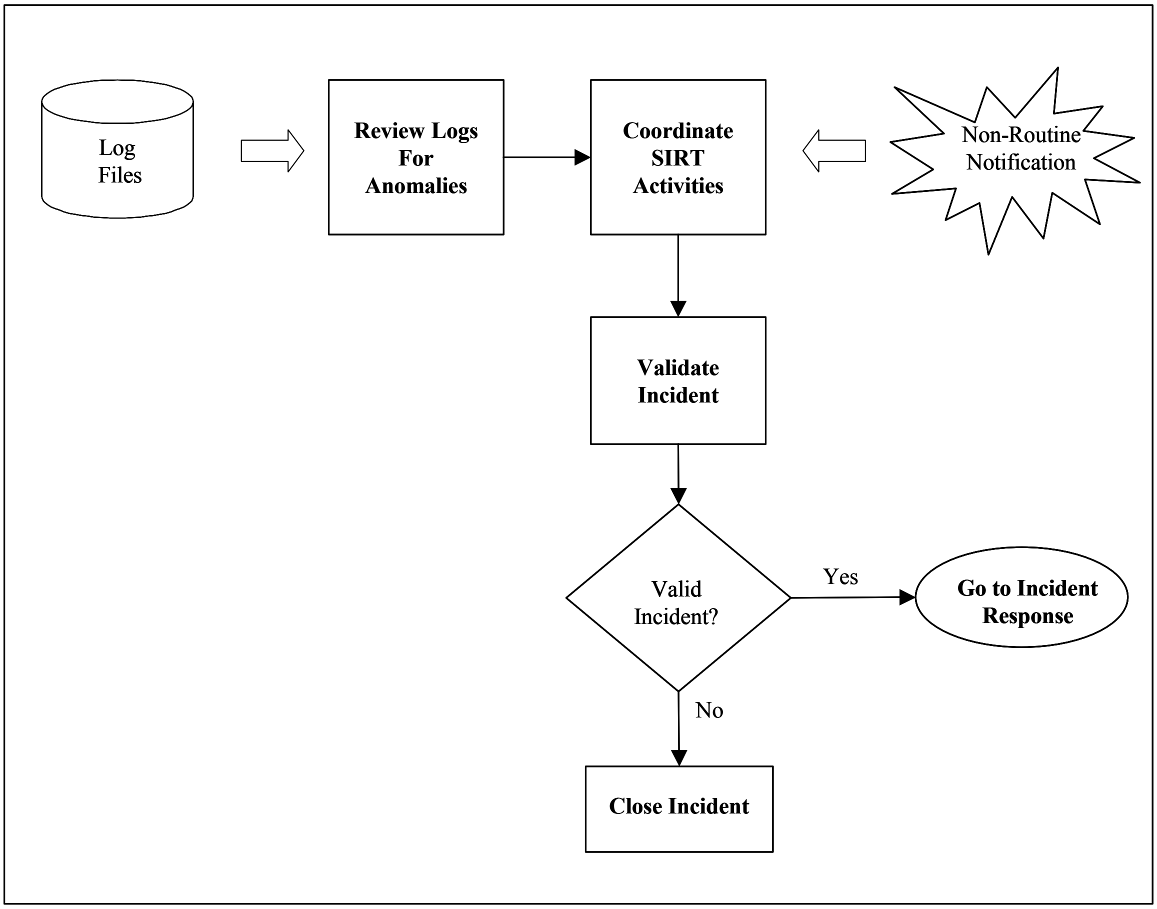

Figure 5: Routine Operations Procedure: Manual Detection

If suspicious activities or anomalies are detected when reviewing log files in accordance with the approved methods and frequencies, then the SIRT should determine if the IDS has already detected the incident. This coordination is critical since log activity may correspond with or immediately follow IDS notifications. Moreover, this SIRT coordination will enhance data collection and correlation efforts, as well as avoid dual processing of the same or related incidents.

The SIRT also should verify that the incident is valid, and not a false positive, before initiating the SIRT Incident Response procedure. In addition, the SIRT should manually process non-routine incidents notifications. For example, a telephone call to the Help Desk indicating that the Web site has been defaced should be directed to the SIRT.

Information Review and Analysis

The SIRT should stay current with expected intrusion characteristics and appropriate responses by reviewing and analyzing the latest data from Information Security sources. However, prior to developing or implementing an information review and analysis sub-procedure, an organization should perform baseline tasks, including identifying Information Security sources and establishing a dedicated section in the SIRT repository for security information such as advisories, alerts, news, and links. Many departments and personnel within an organization (for example, Information Security, Internal Audit, network and security administrators, etc.) already review and/or subscribe to these Information Security sources. The SIRT can serve as a point of coordination for this information, or simply leverage it to update its procedures.

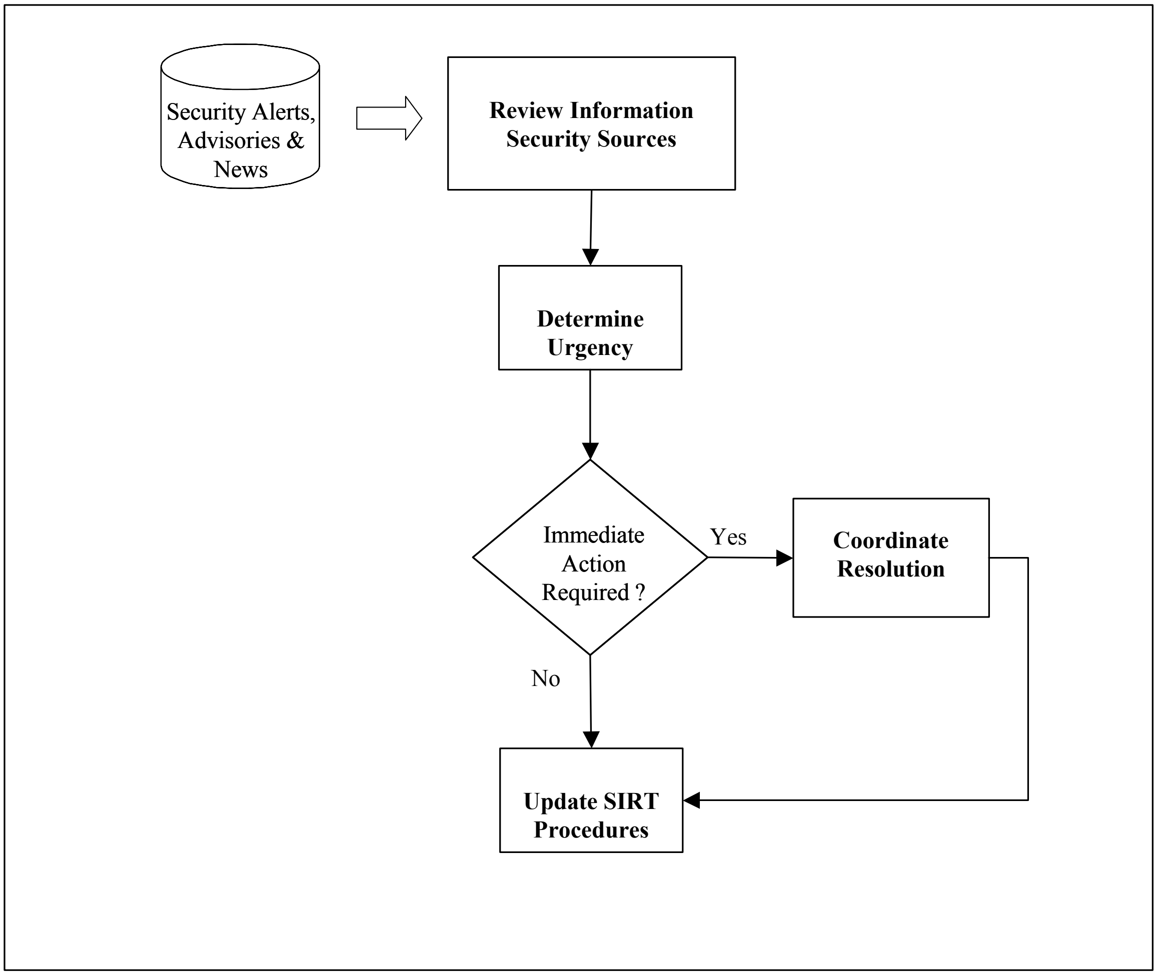
Security Alerts, Advisories & News
Review Information Security Sources
Determine Urgency
Immediate Action Required ?
Yes
Coordinate Resolution
No
Update SIRT Procedures

Figure 6: Routine Operations Procedure: Information Review and Analysis

The information review and analysis sub-procedure should identify the procedural tasks that the SIRT performs to routinely review and analyze Information Security sources. As illustrated in Figure 6, these procedural tasks primarily involve reviewing Information Security sources, determining urgency, and coordinating resolution for critical alerts. The SIRT should routinely review and analyze Information Security sources for the latest security advisories, alerts, and news. For urgent alerts that require immediate action, the SIRT should coordinate with appropriate departments within the organization to determine when updates or patches will be applied and by whom. The SIRT should use the analysis results to update the SIRT procedures as necessary.

Report Preparation

The SIRT should establish metrics for gauging the effectiveness of the SIRT procedures, and foster ongoing awareness of SIRT activities, by providing executive, senior, and business unit management with periodic status reports on SIRT activities.

However, prior to developing or implementing a report preparation sub-procedure, an organization should perform several baseline tasks, including developing status report templates, establishing an approved distribution list, and establishing a dedicated section in the SIRT repository for storing the reports.

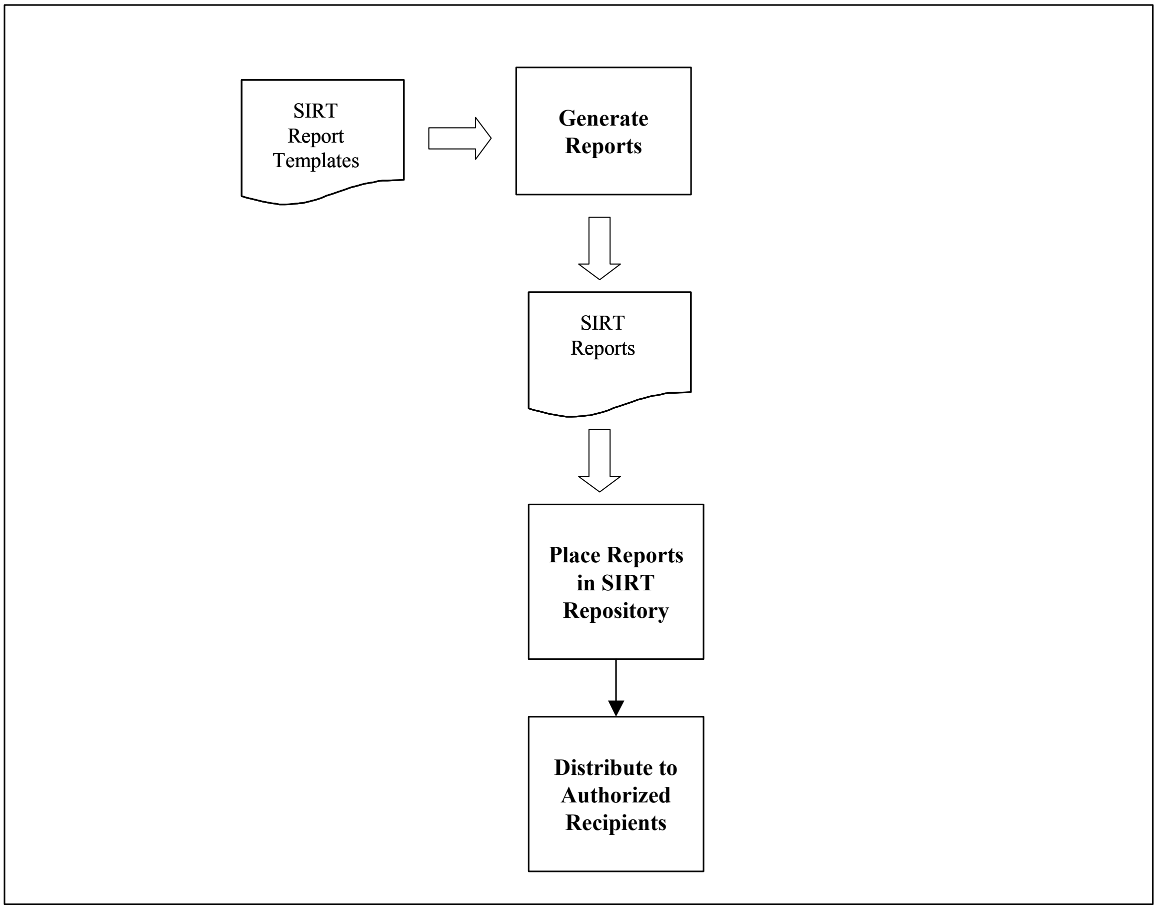
SIRT Report Templates
Generate Reports
SIRT Reports
Place Reports in SIRT Repository
Distribute to Authorized Recipients

Figure 7: Routine Operations Procedure: Report Preparation

The report preparation sub-procedure should identify the procedural tasks the SIRT performs to routinely prepare and distribute SIRT reports. As illustrated in Figure 7, these procedural tasks primarily involve generating and distributing status reports. The SIRT should use the status report templates and relevant information from the SIRT repository to generate status reports on a weekly and monthly basis. The status reports should summarize SIRT activities and lessons learned, provide status information on unresolved incidents, provide intrusion detection metrics (for example, the number automated alerts, false alarms, etc.), as well as list new security advisories and alerts. Upon approval, SIRT reports should be stored in the SIRT repository and distributed to authorized recipients.

Incident Response

Following the validation of security incidents or intrusions during routine operations, SIRT members must be sure of what to do, when to do it, who has authorization to take certain actions (such as pulling a Web site offline), and whom to coordinate with and contact as an incident unfolds. The SIRT Incident Response procedure provides the guidance and instructions needed to quickly execute pre-coordinated responses to security incidents and intrusions. These responses will depend on the nature of the intrusion event and the criticality of the potentially impacted assets.

Prior to developing or implementing the SIRT Incident Response procedure, an organization should perform several baseline tasks, including establishing basic containment criteria (that is, the conditions that determine that an incident has been contained), outlining the basic forensics process, establishing basic recovery criteria, as well as developing a response plan template.

In addition, the SIRT should develop pre-coordinated plans or step-by-step instructions for responding to expected or typical types of intrusion events. Since some responses may impact internal or external business operations, the SIRT should work with business unit managers and other departments within the organization to develop and coordinate, in advance, response plans that may directly impact those departments. For example, the organization may decide to block access to the external Web site for a short period of time if an intruder defaces this site, and it must be repaired. Similarly, the organization may configure Information Security products or IDS tools to selectively stop certain network services in a defined segment of the IT infrastructure, if an intruder is exploiting these services to impact the organization’s business operations. These examples represent actions that may be necessary under some conditions. Such high-profile responses such as blocking access to the external web site represent one end of the response spectrum. SIRT response planning activities should address the full response spectrum, including, at the low end of the spectrum, information logging and personnel notification and alerting.

The SIRT Incident Response procedure should identify the procedural tasks the SIRT performs to respond to valid security incidents. As illustrated in Figure 8, these procedural tasks primarily involve executing response plans, assessing response effectiveness, and coordinating a follow-on response.

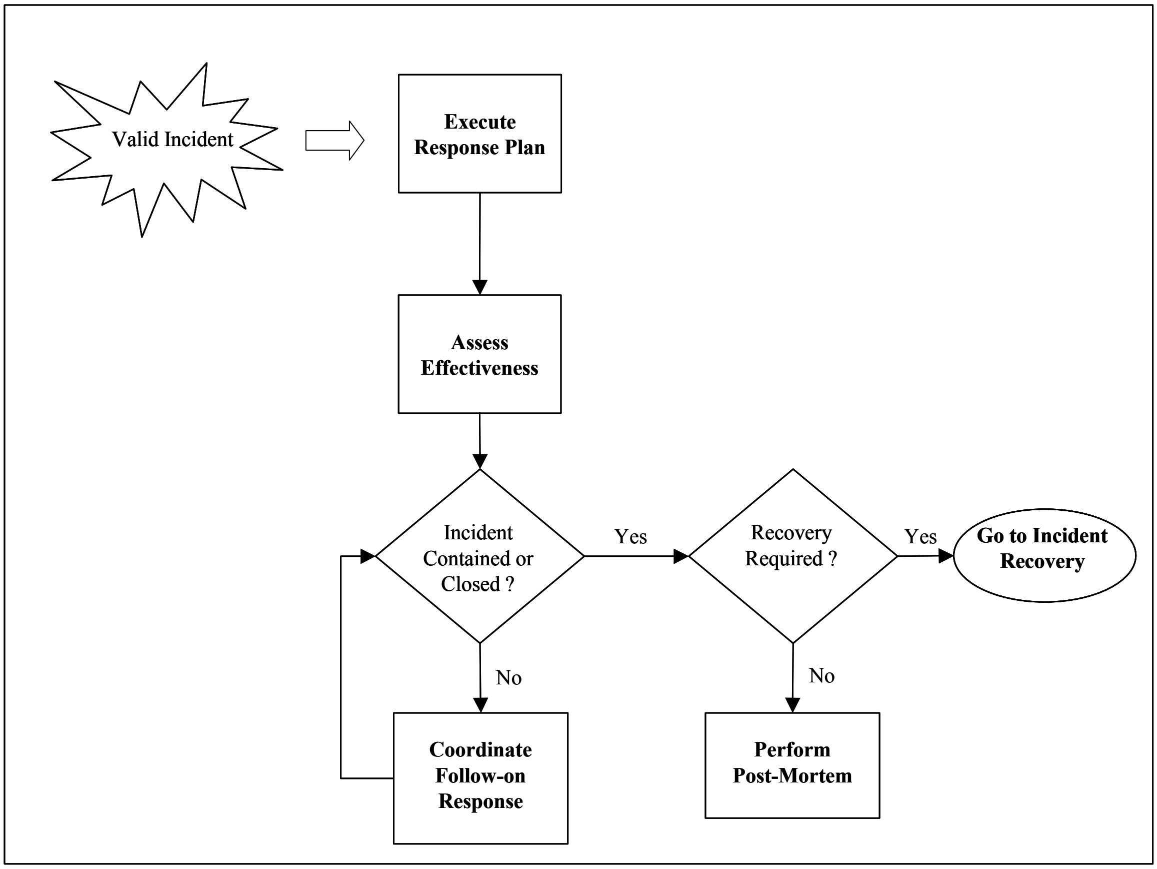

Figure 8: Incident Response Procedure

Based on the assigned incident category, the SIRT should execute the appropriate response plan by performing the documented step-by-step instructions. As it conducts the incident response activities, the SIRT should coordinate with or notify impacted departments and external organizations, as well as provide management with periodic status reports on the response activities. SIRT members also should meet during the incident to check the status and effectiveness of the response in containing the incident. If the initial response does not contain the incident (that is, does not meet the basic containment criteria), then the SIRT should meet to coordinate a follow-up response. This coordination effort should ensure that response plan instructions are followed completely, as well as collect additional data and assign additional tasks.

However, if the initial response does contain the incident (that is, meets the basic containment criteria), then the SIRT should determine whether to initiate the SIRT Incident Recovery procedure. If the basic recovery criteria are met, then the SIRT should initiate the SIRT Incident Recovery procedure. Otherwise, the SIRT should perform response post-mortem activities to assess lessons learned and to update SIRT procedures and response plans.

Incident Recovery

Many organizations, to ensure the continuity of business operations, already have implemented business recovery or resumption capabilities and plans. In these organizations, the SIRT typically offers assistance to the internal departments or teams responsible for business resumption activities. The recovery assistance may range from simply documenting lessons learned by the SIRT to providing forensic data in support of broader post-incident activities. The SIRT Incident Recovery procedure provides the guidance and instructions to assist internal capabilities with recovery and resumption efforts. However, prior to developing or implementing the incident response procedure, an organization should perform the baseline task of developing a damage assessment report template.

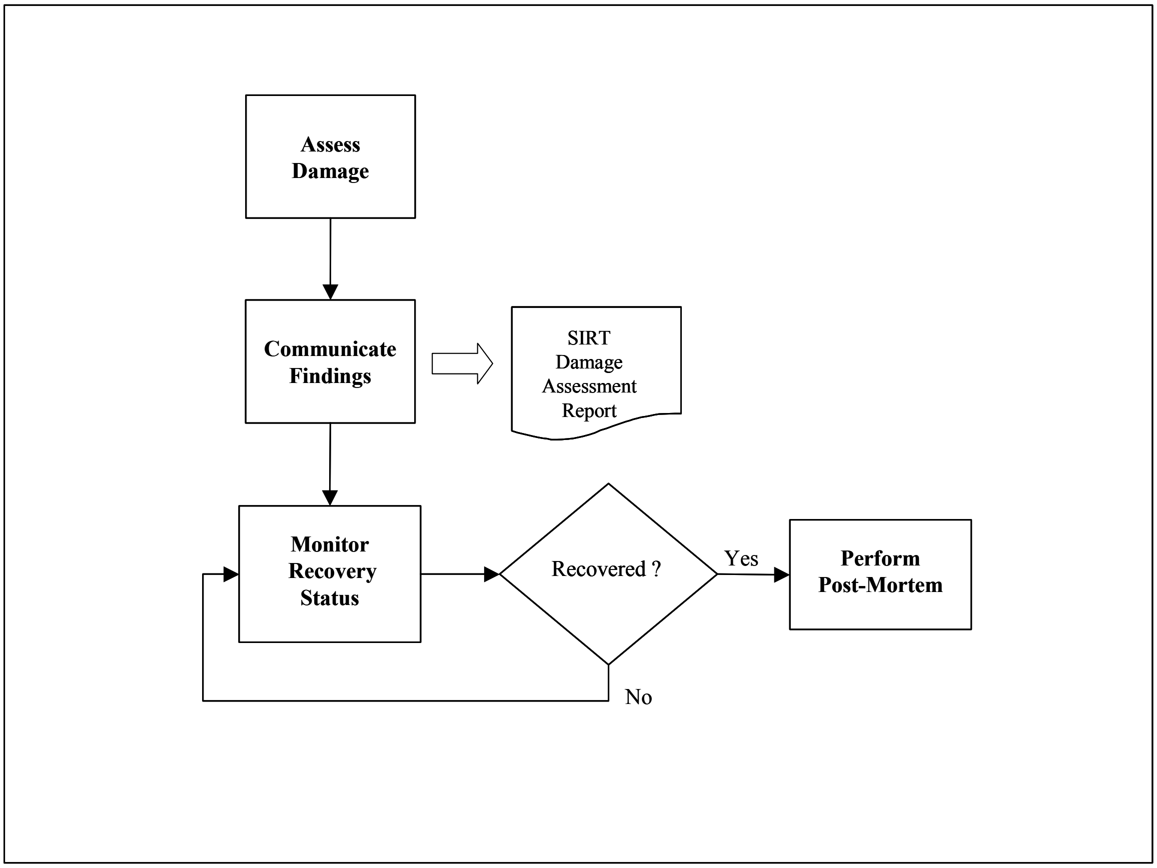

Figure 9: Incident Recovery Procedure

The SIRT Incident Recovery procedure should identify the procedural tasks that the SIRT performs to assist with incident recovery efforts. As illustrated in Figure 9, these procedural tasks primarily involve assessing damage, communicating SIRT findings, and monitoring the status of recovery efforts. The SIRT should use the damage assessment report template and relevant information from the SIRT repository to generate the SIRT Damage Assessment Report. The report should summarize SIRT incident response and forensics activities and findings, identify impacted resources (that is, inventory list of systems, networks, service business lines that are impacted), as well as provide any insight and information on the potential or actual impact on lines of business. Upon approval, the report should be stored in the SIRT repository and distributed to authorized recipients. The SIRT also should monitor the status of recovery efforts. When the recovery efforts have been completed, the SIRT should initiate post-mortem activities.

Conclusion

META Security Group recognizes that a SIRT, including the establishment of its organizational framework and procedures, represents a substantial departure from the some of the informal approaches that many organizations currently use to respond to security incident and intrusions. However, organizations increasingly will establish formal SIRT capabilities to support and protect business operations in the current and projected threat environment that is characterized by expanded use of “open” computing environments and reliance on the Internet, as well as the real threat of internal and external attacks on e-commerce applications.