Development of Incident Response Standard

By Malcolm E. Palmer
Edward P. Moser

Copyright Notice

Scalable Software, Inc.
2929 Allen Parkway, Suite 1400 Houston, TX 77019
713.316.4900 fax: 713.316.4975
www.scalable.com

Printed in the United States of America.

Warning and Disclaimer

Table of Contents

1 Introduction

This research report from Scalable Software*, Development of Incident Response Standard*, provides best practices guidance that organizations can reference and leverage to assess, improve, or develop an Incident Response Standard. The Incident Response Standard should provide specific instructions and requirements for responding to detected threat and intrusion activity. The insights provided in this report are derived from the considerable "real world" experience gained by Scalable Software in developing and assessing Information Security policies, standards, guidelines, and procedures.

1.1 Audience

There are two primary audiences for this report:

1. Organizations that have implemented or are planning to implement the Scalable Software Information Security Policy Framework.

2. Members of Information Security teams.

In addition, this report can be useful to executive management and business unit owners. These individuals can use or reference the report to provide a common understanding of key considerations for an Incident Response Standard and to enhance communication of an overall Policy Framework.

This report assumes a certain level of understanding of the Scalable Software Information Security Policy Framework and terminology, as well as a basic, but not necessarily in-depth, comprehension of incident response approaches. Section 1.2 of this paper provides a high-level overview of the Scalable Software Information Security Policy Framework. Refer to the Scalable Software *Information Security Policy Framework* research report for more detailed and comprehensive information.

1.2 Background and Context

As shown in Figure 1, the Scalable Software Information Security Policy Framework (the Framework) consists of a hierarchical structure that includes:

- An Information Security Program Charter at the top of the hierarchy that empowers all activity within the Information Security Program.

- Seven policies that further define the Information Security objectives in a number of topical areas.

- Key standards that provide more measurable ("auditable") guidance in each policy area.

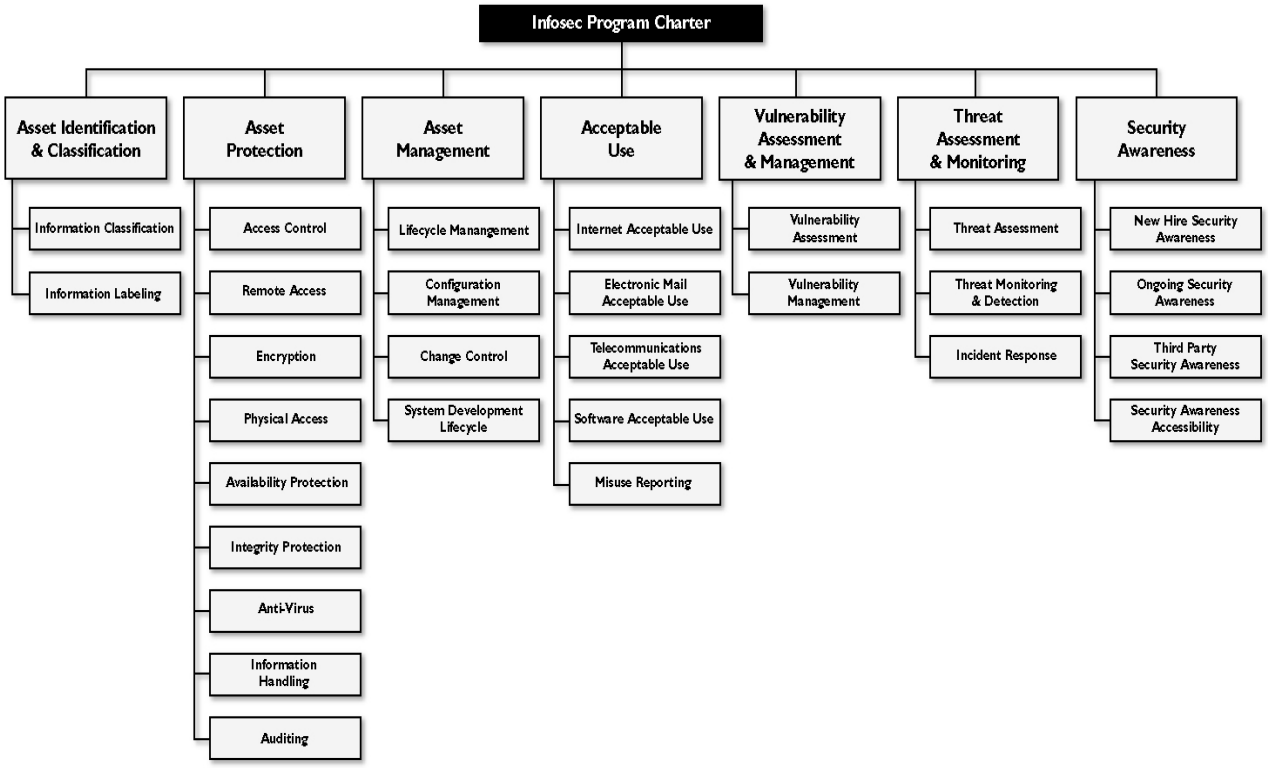

Figure 1: The Scalable Software Information Security Policy Framework

This hierarchical structure ensures that the elements at lower levels in the Framework such as standards are referentially associated with the risk management approach and traceable back to the objectives established at the Framework's Security Program Charter and policy levels.

Scalable Software has significant experience in developing customized standards for numerous organizations across multiple vertical markets. Our experience suggests that several organization-specific factors must be considered when developing standards. This paper identifies these factors, and outlines a structure for the Incident Response Standard that is traceable and consistent with the Framework.

1.3 Document Organization

The Key Considerations section discusses specific factors that organizations should consider when developing the Incident Response Standard.

The Sample Incident Response Standard section outlines a sample standard established on the basis of the key considerations discussed in the report.

2 Key Considerations

Scalable Software has found through its extensive experience with clients that an Information Security standard within the Framework should contain the following major components:

- Purpose Statement
- Scope Statement
- Terms and Definitions
- Requirements
- Responsibilities
- Enforcement and Exception Handling
- Review and Revision Expectations

Sections 2.1 to 2.7 discuss key considerations for each major section of the Incident Response Standard.

2.1 Purpose Statement

As defined in the Scalable Software Information Security Policy Framework, a standard provides more measurable criteria for satisfying and supporting the high-level objectives defined and authorized by the policies. In order to maintain the traceable framework hierarchy, the purpose statement for the Incident Response Standard should derive from the *Threat Assessment and Monitoring Policy* (see Figure 1).

The *Threat Assessment and Monitoring Policy* defines the objectives for establishing specific standards and guidelines on the assessment and ongoing monitoring of threats to information assets. The Incident Response Standard builds on these policy objectives by providing specific instructions and requirements for developing and exercising formal plans, and associated metrics, for responding to security incidents and intrusions. More specifically, the standard should require the establishment of a formal Security Incident Response Team (SIRT) to develop and maintain capabilities to respond effectively to electronic intrusions into the IT infrastructure.

2.2 Scope Statement

The scope of the Incident Response Standard should summarize the SIRT mission by clearly outlining the purpose and response objectives of the SIRT capability. In addition, the scope of a standard defines to whom the standard applies. The scope statement for the Incident Response Standard should apply to all SIRT members (that is, managers, core members, and supporting members) and their management. SIRT managers are those that have primary responsibility for managing and leading SIRT routine operations and incident response efforts

associated with their SIRT assignments. Core SIRT members are those designated representatives from key departments are functionally responsibility for performing SIRT routine operations and incident response duties. Supporting SIRT members are those designated representatives from key departments that supplement the core SIRT members by providing specific expertise or assistance.

2.3 Terms and Definitions

The Incident Response Standard introduces new terms and corresponding definitions. In addition, this standard should restate or reference terms that were previously defined in the charter or policies. The following key terms and definitions are among those that should be defined, restated, or referenced:

- **Incident** – Should provide a definition that refers to an anomalous event that may indicate a security intrusion.

- **Intrusion** – Should provide a definition that refers to malicious activity on or directed towards a system, application, network, or network device.

- **Information Assets** – Should restate or reference the definition in the *Asset Identification and Classification Policy*.

- **Threat** – Should restate or reference the definition in the *Threat Assessment and Monitoring Policy*.

2.4 Requirements

The Incident Response Standard should provide specific instructions and requirements for establishing a SIRT, including formal plans and associated metrics, for responding effectively to electronic security incidents and intrusions into the IT infrastructure.

The following sections cover general, response, and recovery requirements.

2.4.1 General Requirements

The general requirements for the Incident Response standard should involve developing the SIRT operational concept, developing pre-coordinate response plans, and establishing SIRT metrics. The Incident Response standard should require the development of the SIRT concept of operations (CONOP) that formally documents the SIRT mission statement, SIRT constituents and capabilities, SIRT organizational structure, as well as roles and responsibilities. The standard also should require the development of response plans that are coordinated, in advance, between the SIRT and other departments. This coordination is required since some responses may impact internal or external business operations. In addition, the standard should require the establishment and maintenance of SIRT metrics that

formally address the number of detected incidents, average detection and response times, as well as SIRT performance during exercises.

2.4.2 Response Requirements

The response requirements for the Incident Response Standard should involve developing a formal procedure, executing response plans, assessing response effectiveness, facilitating ongoing communications, and conducting periodic exercises. The Incident Response Standard should require the development of the SIRT Incident Response Procedure that formally describes how to confirm incident priorities, conduct pre-coordinated responses, determine incident containment, perform basic computer forensics, initiate incident recovery efforts, as well as document "lessons learned to improve SIRT operations. The standard also should require SIRT members to perform their designated response tasks, periodically evaluate the effectiveness of the response, and coordinate with or notify management, as well as impacted departments and external organizations. In addition, the standard should require SIRT response capabilities to be exercised, at least annually, for performance evaluation purposes.

2.4.3 Recovery Requirements

The recovery requirements for the Incident Response Standard primarily should involve developing a formal SIRT recovery procedure. The Incident Response Standard should require the development of the SIRT Incident Recovery Procedure that formally describes how the SIRT will coordinate with established business resumption and recovery capabilities, ensure consistent and timely reporting of SIRT recovery activities, and document "lessons learned to improve SIRT operations.

2.5 Responsibilities

The Incident Response Standard should assign, to members of the SIRT, the responsibilities for meeting the requirements. These responsibilities also should expound on and be consistent with the responsibilities outlined in the *Threat Assessment and Monitoring Policy*. Moreover, the responsibility assignments should be consistent with the *Information Security Program Charter*. Table 1 identifies typical responsibilities and assignments associated with this standard.

Table 1: Responsibilities and Assignments

Responsibilities	Typically Assigned to
Approves the standard.	Chief Information Security Officer (CISO)
Ensure the development, implementation, and maintenance of the standard.	Chief Information Security Officer (CISO)

Responsibilities	Typically Assigned to
• Secure the budget for resources to support the SIRT. • Interface with Company execute management and business owners. • Arrange periodic SIRT exercises including incident simulation and intrusion drills. • Approve SIRT documentation prior to distribution.	SIRT Executive Sponsor or SIRT Management
• Work closely with the management of the departments that are functionally part of the SIRT. • Lead efforts to develop the SIRT organizational structure, procedures, and operational budget. • Conduct post-mortem evaluations to capture lessons learned. • Ensure the ongoing execution and performance of SIRT procedures. • Arrange periodic training for SIRT members. • Manage SIRT incident escalations. • Ensure that SIRT documentation is developed and distributed in a timely manner.	SIRT Management
• Represent their respective departments in SIRT operations • Communicate SIRT information within their departments • Lead departmental support for SIRT activities • Coordinate 7X24 departmental support to the SIRT • Interface with local, state, and federal law enforcement agencies to facilitate legal responses to incidents • Assist with development of baseline IDS configurations • Support reviews of available Information Security sources to maintain currency	Core SIRT Members

Responsibilities	Typically Assigned to
with information that can assist SIRT operations • Advise the SIRT on strategies for processing non-routine notifications and responding to security incidents.	
• Represent their respective departments in SIRT operations • Communicate SIRT information within their departments. • Lead departmental support for SIRT activities • Provide legal advice to the SIRT and executive management • Interface with management, employees, and contractors to facilitate personnel-related responses to incidents. • Assist with internal communication on incident response and incident status information. • Lead external communication to the media and public regarding responses to incidents. • Support reviews of available Information Security sources to maintain currency with information that can assist SIRT operations.	Supporting SIRT Members
• Work closely with SIRT management to ensure that their departmental representatives are performing their SIRT functionally assigned responsibilities, as well as the duties and tasks specified in approved SIRT procedures.	Managers of SIRT member

2.6 Enforcement and Exception Handling

The Incident Response Standard should reiterate or expound upon the enforcement statement established in the *Threat Assessment and Monitoring Policy*. The exception handling statement should reference an existing procedure or outline specific steps for requesting and submitting an exception to the standard. In addition, the exception handling statement should

reiterate the need to comply with the current standard while exception requests are under consideration.

2.7 Review and Revision Expectations

The Incident Response Standard should reiterate or expound upon the review and revision statements established in the *Threat Assessment and Monitoring Policy*.

3 Sample Incident Response Standard

This section outlines a sample Incident Response Standard that is consistent with the Framework and incorporates the key considerations discussed in the body of this report.

Sample Incident Response Standard

The Company ABC (the "Company) *Threat Assessment and Monitoring Policy* defines objectives for establishing specific standards for assessing and monitoring threats to information assets.

This *Incident Response Standard* builds on the objectives established in the *Threat Assessment and Monitoring Policy*, and provides specific requirements for developing and exercising formal plans, and associated metrics, for responding to security incidents and intrusions. The Company will satisfy these requirements through a formal Security Incident Response Team (SIRT).

I. Scope

The Company SIRT will establish and maintain capabilities to respond effectively to electronic intrusions into the Company 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.

All SIRT members, as well as their management, are covered by the *Incident Response Standard* and must comply with its associated procedures and guidelines.

Information assets are defined in the *Identification and Classification Policy*.

Incident refers to an anomalous event that may indicate a security intrusion.

Intrusion refers to malicious activity on or directed towards a system, application, network, or network device.

Threats are the intentional or accidental actions, activities or events that can adversely impact Company information assets, as well as the sources, such as the individuals, groups, or organizations, of these events and activities.

.

II. Requirements

A. GENERAL REQUIREMENTS

1. The Company shall develop a *SIRT Concept of Operations (CONOP)* that:

   - Summarizes the overall mission of the SIRT
   - Defines the SIRT constituents and capabilities
   - Defines the SIRT organizational structure

- Defines specific roles and responsibilities of SIRT members
- Summarizes the operational capabilities of the team

2. The SIRT, as defined in the *CONOP*, shall develop plans for responding to expected or typical types of intrusion events, as well as develop contingency plans for responding to new or unanticipated types of intrusions.

3. The planned responses shall be dependent on the nature of the intrusion event and the criticality of the potentially impacted Company information assets.

4. The SIRT shall maintain awareness of company information asset criticality definitions and shall develop incident response procedures that reflect these definitions.

5. The SIRT shall work with other departments as necessary to coordinate, in advance, responses that may directly impact those departments.

6. SIRT planning activities shall address the full response spectrum. One end of the spectrum includes information logging as well as personnel notification and alerting. The other end of the spectrum includes higher profile responses (e.g., blocking access to the external web site, denying access from specific external networks, etc.).

7. The SIRT shall maintain metrics that address at least the following:

   - Incidents detected per reporting period, by severity category
   - Average time from incident detection to response initiation.
   - Average time from response initiation to incident containment.
   - SIRT performance during exercises

B. RESPONSE REQUIREMENTS

1. An *Incident Response Procedure* shall be developed to describe how to:

   - 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 SIRT response activities.
   - Document "lessons learned" to improve SIRT operations.
   - Initiate SIRT recovery efforts, if necessary.

2. The SIRT shall verify the existence of network and system intrusions, and take actions to contain the threat, in accordance with the *Incident Response Procedure*.

3. The type of threat activity, together with the criticality of potentially impacted assets, shall provide the direct basis for conducting the incident response.

4. SIRT members shall perform their designated, pre-coordinated tasks, in accordance with the *Incident Response Procedure*.

5. SIRT members shall meet periodically during the incident to check the status and effectiveness of the response.

6. The SIRT shall coordinate with or notify impacted departments and external organizations as it conducts the incident response activities.

7. The SIRT shall provide Company management with periodic status reports on the response activities.

8. The SIRT shall transition to incident recovery activities when the incident or intrusion is contained and meets pre-defined SIRT recovery criteria.

9. SIRT incident response capabilities shall be exercised, for evaluation purposes, at least annually. However, the SIRT members (with the possible exception of a senior SIRT manager) shall not be notified in advance of the exercises.

C. RECOVERY REQUIREMENTS

1. An *Incident Recovery Procedure* shall be developed to describe how the SIRT will work within established business resumption and recovery capabilities.

2. The *Incident Recovery Procedure* shall describe how to:

    - Document SIRT damage assessment findings.
    - Coordinate with Company departments or 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.

III. Responsibilities

The Chief Information Security Officer (CISO) approves the *Incident Response Standard*. The CISO also is responsible for ensuring the development, implementation, and maintenance of the *Incident Response Standard*.

SIRT Managers are the members that have primary responsibility for managing and leading SIRT routine operations and incident response efforts associated with their functional SIRT assignments. SIRT managers are responsible collectively for securing the budget for resources to support the SIRT; interfacing with Company execute management and business owners; working closely with the management of the departments that are functionally part of the SIRT; arranging periodic SIRT exercises including incident simulation and intrusion drills for third-party verification of the SIRT operational and response capabilities; leading efforts to develop the SIRT organizational structure, procedures, and operational budget; conducting post-mortem evaluations to capture lessons learned; ensuring the ongoing execution and performance of SIRT procedures; arranging periodic training for SIRT members, and manage SIRT incident escalations; and ensuring that SIRT documentation is developed, approved, and distributed in a timely manner.

Core SIRT members are those designated representatives from key Company departments that have primary responsibility for performing SIRT routine operations and incident response efforts. Core SIRT members are responsible collectively for representing their respective departments in SIRT operations; communicating SIRT information within their departments; leading departmental support for SIRT activities; coordinating 7X24 departmental support to the SIRT; interfacing with local, state, and federal law enforcement agencies to facilitate legal responses to incidents; assisting with development of baseline IDS configurations; supporting reviews of available Information Security sources to maintain currency with information that can assist SIRT operations; and advising the SIRT, in concert with existing troubleshooting and status procedures, on strategies for processing non-routine notifications and responding to security incidents.

Supporting SIRT members are those designated representatives from key Company departments that supplement the core SIRT members by providing specific expertise or assistance. Supporting SIRT members are responsible collectively for representing their respective departments in SIRT operations; communicating SIRT information within their departments; leading departmental support for SIRT activities; providing legal advice to the SIRT and executive management; interface with management, employees, and contractors to facilitate personnel-related responses to incidents; assisting with internal communication on incident response and incident status information; leading external communication to the media and public regarding responses to incidents; and supporting reviews of available Information Security sources to maintain currency with information that can assist SIRT operations.

Managers of SIRT members are responsible for working closely with SIRT management to ensure that their departmental representatives are performing their functionally assigned SIRT responsibilities, as well as the duties and tasks specified in approved SIRT procedures.

IV. Enforcement and Exception Handling

Failure to comply with the *Incident Response Standard* and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment

for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Incident Response Standard* should be submitted to <Insert Title> in accordance with the *Information Security Standards Exception Procedure*. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this standard will continue to observe the *Incident Response Standard.*

V. Review and Revision

The *Incident Response Standard* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Insert Name>
Chief Information Security Officer