

[WP-013]

Whitepaper: Incident Response Management

An Overview of How to Respond to Security Threats

Version 040819

August 2004

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2004 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s). Source information was taken from former-Netigy, Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

Overview of Incident Response Management

When system interruptions, malfunctions and intrusion occurs, uncertainty often exists concerning the probably cause and whether the cause was intentional or accidental. Coupled with the complexity of the issue, its interrelationships of systems, software, hardware and human interventions and their variables, a seemingly simple situation (in reality) can (often) pose a formidable task in determining its cause, thus affecting the possible remedy.

As with any incident response management planning team, the implementation of this task may be more or less as manageable, irrespective of the organization's size. Thus, a strong foundation of tools, methodologies and principles, is recommended for its utilization, which is built based upon four underlying principles:

- ❖ **AVOIDANCE:** This employs the underlying processes that seek to create a secure environment.
- ❖ **ASSURANCE:** Ensuring policies, standards and practices are followed.
- ❖ **DETECTION:** Accurately detect an intrusion attempt (best possible method is in real-time) and taking immediate (and appropriate) action to terminate successfully the intrusion (attempt), and possible apprehend the infiltrator.
- ❖ **RECOVERY:** Restore the system (and its environment) to full operational status.



Within a methodology that is available as a group, individual assignment, or any combination, the process consists of the following philosophies:

IRM: Avoidance

- ❖ Facilitates risk analysis processes that identifies and prioritizes risks (and their impacts), while mitigating controls and documenting any actions plans, cost-benefit (return on investment [ROI]) analysis and prediction models, of protecting the organization's assets.
- ❖ Policies and procedures are made more effective through a comprehensive approach that develops concise, effective security policies and procedures by:
 - Facilitate the implementation of any (and all) controls within the organization.
 - Provide the foundation for an effective information security program through simplified and agreed upon policy and procedure templates.
 - Create a customized set of policies and procedures, some of which may be taken from public sources and tailored to the organization's individual use.
- ❖ Define, establish and implement a Computer Incident Response Team (CIRT) for the enterprise-wide utilization throughout the organization. The organization is trained on CIRT establishment by identifying key, critical systems.

IRM: Assurance

- ❖ The first step in delivering a life-cycle incident management system is properly identification and closure of any known or existing vulnerabilities within the enterprise (network).
- ❖ Use state-of-the-art and/or modified commercial or "underground" tools and software products, along with any proprietary tools that will test both internal and perimeter networks, hosts, servers and access connections.
- ❖ Provide periodic perimeter scans of any networking devices, access connection portals, firewalls and proxy servers; scans may be done through internal methods or remotely on a periodic basis, typically monthly or quarterly.
- ❖ Report findings of any suspicious activities or problematic areas (see "investigative management", under **RECOVERY**).



IRM: Detection

Remote intrusion monitoring (RIM) programs implemented through intrusion detection systems (IDS) and/or intrusion prevention systems (IPS), or through a security management service provider. RIM identifies, monitors, analyzes and attempts interpretation of data packets monitored, systems activities, then compares the data to a baseline state.

- ❖ RIM provides a feedback loop of information that assists the organization in preventing similar intrusions or interruptions from occurring in the future, thus providing the basis for forensics, investigative and subsequent litigation (or prosecution) support and services.
- ❖ Operational forensics tools establishment and setup/configuration help provide a baseline for establishing and configuring the necessary tools, models and processes to collect, preserve and evaluate any evidence data collected that may pertain to any system intrusion attempt or interruption.

IRM: Recovery

- ❖ Operational forensics development is established by identifying the nature and cause of the intrusion attempt or interruption as well as collecting, preserving and evaluating the evidence data collected; additionally, this process may identify alternative recovery methods.
- ❖ Utilizing the operational forensics methodologies established within the enterprise organization, deploy the CIRT which responds to intention and/or accidental system intrusion attempts or interruptions with the goal of remedying the situation quickly, appropriately and professionally; much of this process is a matter of containment, followed by communications internally, and if exposure to the outside, externally.
- ❖ Establish an investigative management team which is utilized when all other measures of intrusion management and incident response/recovery methods have failed to identify the cause of the intrusion attempt or interruption, or have failed in preventing any consequences resulting from the attack or attempt. Team members possess traditional technology skills (such as network, host and server platform security), and if require, also possess some specialized talents of varied professions in investigative management and operational forensics, which can assist in the CIRT team efforts with forensics, possible criminal investigations, legal and court procedures, evidence collection and preservation, and (ultimately) system recovery.



Questions to be Answered

Some of the questions that should be raised before even considering any of the methods listed are as follows:

1. Do you have mission critical or key-mission critical systems, data, services and/or devices (such as customer databases, patient records, etc.) or web servers that are time-dependent or sensitive to service interruptions?
2. Does your business resumption plan (BRP) include detecting and handling system intrusion attempts, attacks and interruptions?
3. When a system intrusion attempt (or attack) or interruption occurs, can your organization's systems detect the symptoms and alert your organizational staff quickly, effectively and reliably?
4. Is your organization prepared to conduct a preliminary and detailed investigation into the cause of the system intrusion attempt, attack or interruption?

Benefits of Using IRM

The benefits from implementation an incident response management team includes:

- ❖ Ensuring that the organization is prepared in advance for handling any system intrusion attempts, attacks or interruptions.
- ❖ Improving the likelihood of successfully recovering from a system intrusion attempt, attack or interruption.
- ❖ Helping assess whether the interruption was accidental or intentional in nature.
- ❖ Providing alternative assessments and perspectives of the system intrusion attempt, attack or interruption in problematic determination, as well as during investigative management proceedings.

Some features of utilizing a remote intrusion monitoring (RIM) system:

- ❖ Ensure a timely detection and response to system intrusion attempts, attacks and interruptions.
- ❖ Provide a professional forensics evaluation and handling methodology for evidentiary information handling and management.
- ❖ Assists management in quickly determining and identifying the cause of an intrusion attempt, attack or interruption, what how to recover from its effect(s).
- ❖ Provide validation and assurance of systems prior to the recovery methods, esp. when attempting to restore mission critical services and/or system environments.



Answering these questions and establishing an incident response management team is the first step in the road to recovery.

