Building an Effective Incident Response Plan

November 14, 2012

Alex Rodriguez-Triana
Information Security Consultant
GSEC, ITILv3
Enterprise Risk Management, Inc.
# About our Firm

## Company Background
- Founded in 1998
- 8(A) Economically Disadvantaged Woman Owned Small Business (EDWOSB)
- GSA MOBIS 874
- GSA Schedule 70
- GSA FABS 520
- GSA 8(a) STARS Subcontractor to Zia Engineering

## Market Presence
- More than 130 clients
- Large and complex domestic and international clients
- Offices in:
  - Washington DC
  - Miami
  - Orlando
  - Philadelphia

---

© 2012 Enterprise Risk Management, Inc. All rights reserved.
About our Firm

Capabilities

- Cyber Security
- Risk Management
- Risk and Vulnerability Assessments
- Penetration Testing and Social Engineering
- Incident Response Planning and Business Continuity
- IT Security Outsourcing and Specialized Security Training
- Wireless Security Assessments and Wireless
- Network Design and Security Implementation
- Digital Forensics
- Security Breach Investigation
- Fraud Analysis and Forensics

Regulatory Compliance

- Gramm Leach Bliley (GLBA)
- Fair and Accurate Credit Transactions Act (FACTA)
- Sarbanes-Oxley (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Family Education Rights and Privacy Act (FERPA)
- Bank Secrecy Act (BSA)
- Payment Card Industry (PCI)
Introductions

Alex Rodriguez-Triana
GSEC, ITILv3
Information Security Consultant

MS Electrical Engineering
MS Industrial & Systems Engineering
MBA

Core Experience:
• Security Operations
• Incident Response
• Risk and Vulnerability Management
• Project Management
• Penetration Testing
• IT Audit
Outline

• Introduction / Background
• Creating an Incident Response Program
• How to handle an incident
  – Preparation
  – Detection & Analysis
  – Containment
  – Eradication
  – Remediation / Recovery
  – Post-Incident Activities
• Q&A
Introduction

• **Event** - Any observable occurrence in a system or network

• **Incident** - A violation of computer security policies, acceptable use policies, or standard computer security practices

• **Incident Response** - The process of detecting and analyzing incidents and mitigating an incident’s effect on an organization

• **Computer Incident Response Team (CIRT)** - A capability set up for the purpose of assisting in responding to computer security-related incidents
Incident Response Program

- Goals of an Incident Response Plan:
  - Verify that an incident has occurred
  - Maintain or restore Business Continuity
  - Reduce the impact of the incident
  - Prevent future attacks/incidents
  - Determine attack vectors and how the incident occurred
  - Follow a consistent incident handling methodology
  - Improve the organization’s security posture
  - Keep management informed and follow proper chain of command procedures

*Incidents will occur...it’s not if but when*
Incident Response Team

- The Computer Incident Response Team (CIRT) is responsible for:
  - Developing and preserving the IRP
  - Defining and classifying incidents
  - Determining the tools and technology utilized in intrusion detection
  - Determining if the incident should be investigated and the scope
  - Securing the network
  - Conducting follow-up reviews
  - Promoting awareness throughout the organization
Incident Response Team

- Team members shall include, but is not limited to, the following:
  - Chief Information Security Officer (CISO)
  - Security Manager
  - IT Service Request Desk
  - Incident Handlers
  - Security Operations Center Analyst
  - Network Engineer
  - Web Application Development Engineer
  - IT Windows/Unix Systems Administrator
  - Internal Audit & Governance
CIRT Roles and Responsibilities

• Chief Information Security Officer (CISO)
  - Monitors progress of all security and incident investigations
  - Assists in developing appropriate communication to impacted parties
  - Provides guidance throughout investigations on issues relating to privacy of customer/employee personal information
  - Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach
  - Assists in legal matters

• Security Manager
  - Escalates to senior and executive management
  - Assists in developing appropriate communication to impacted parties
  - Provides guidance throughout investigations on issues relating to privacy of customer/employee personal information
  - Ensures evidence gathering, chain of custody, and preservation is appropriate
  - Gathers and reviews all work done by CIRT
  - Provides proper training on incident handling

• IT Service Request Desk
  - Provides a point of contact for all possible and realized computer incidents
  - Creation and distribution of incident tickets to appropriate parties
  - Provides customer service to users

• IT Windows/Unix Systems Administrator
  - Ensures all service packs and patches are current on mission-critical computers
  - Ensures backups are in place for all critical systems
  - Examines system logs of critical systems for unusual activity
  - Reviews audit logs of mission-critical servers for signs of suspicious activity

• Internal Audit / Governance
  - Periodically reviews policies and procedures for compliance with information security standards
CIRT Roles and Responsibilities

- Incident Handlers / Security Operations Center Analyst / Network Engineers / Web Application Development Engineer
  - Central point of contact for all security incidents
  - Determines the nature and scope of the incident
  - Contacts qualified information security specialists for advice as needed
  - Escalates to senior management as appropriate
  - Contacts auxiliary departments and team member as appropriate
  - Ensures evidence gathering, chain of custody, and preservation is appropriate
  - Documents the types of personal information that may have been breached
  - Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
  - Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
  - Looks for signs of a firewall and/or web application firewall breach
  - Prepares a written summary of the incident and corrective action taken
  - Contacts external Internet service provider for assistance in handling the incident
  - Takes action necessary to block traffic from suspected intruder
  - Examines system logs of critical systems for unusual activity
  - Monitors business applications and services for signs of attack
  - Reviews audit logs of mission-critical servers for signs of suspicious activity
  - Contacts the Information Technology Operations Center with any information relating to a suspected breach
  - Collects pertinent information regarding the incident at the request of the Chief Information Security Office
  - Reviews systems to ensure compliance with information security policy and controls
  - Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
Incident Response Policy

• The Incident Response Policy governs the organization’s incident response and is unique to every organization

• The policy includes:
  – Statement of management commitment
  – Purpose and objectives
  – Scope
  – Definition of computer security incidents
  – Organizational structure with definition of roles, responsibilities, and levels of authority
  – Priority or severity ratings of incidents
  – Performance measures
  – Reporting and contact forms
Incident Response Plan

• The Incident Response Plan must tie back to the organization’s mission, size, structure, and functions

• The Incident Response Plan includes:
  – Mission
  – Strategies and goals
  – Senior management approval
  – Organizational approach to incident response
  – Communication plan within the organization and to external entities
  – Metrics for measuring the effectiveness of incident response
  – Roadmap for maturing the incident response capability

• The plan must be reviewed and updated at least annually with management approval
Standard Operating Procedures

- Standard Operating Procedures (SOPs) are the specific technical processes, checklists, and forms used by the incident response team.
- Standardized within an organization to minimize errors.
- SOPs should be tested and validated for accuracy and usefulness.
- All CIRT members should have the latest SOPs documentation at all times.
- SOPs can be used as training for CIRT members.
Incident Response Life Cycle
Preparation

- Preparation requires:
  - Creation and re-defining of the IRP
  - Creation of the Incident Response Team
  - Organization’s security awareness
  - Ensuring that systems, networks, and applications are sufficiently secure

- Although the CIRT is not typically responsible for incident prevention, it is fundamental to the success of incident response programs
Preparation

• Incident Handler Tools and Resources
  – Communication and Facilities
    • Contact information for all parties involved
    • Issue reporting mechanism
    • Issue tracking system
    • War room location
    • Secure storage facilities
  – Incident Analysis Hardware and Software
    • Digital Forensic workstation/laptop and software
    • Malware workstation/laptop
    • Spare workstations, servers, and/or networking equipment
    • Packet sniffers and protocol analyzers for network traffic
    • Removable media
    • Evidence gathering materials
  – Incident Analysis Resources
    • Organization’s documentation
    • Organization’s current network diagrams and list of critical assets
    • Current Infrastructure baseline
    • Port list
  – Incident Mitigation Software
    • Clean OS and application images for restoration and recovery
Preparation

• Most CIRTs create a **Jump Kit**
  - Laptop
  - Appropriate software loaded
  - Blank media (hard drives/flash drives, CDs/DVDs)
  - Basic network equipment (cables, etc.)
  - Evidence gathering materials (pens, paper, etc.)
  - Tools (screwdrivers, screws, etc.)
  - Images
  - Incident Handling procedures
  - Communication / Escalation List

• Key is to facilitate faster response
  1. Never take anything form the jump bag
  2. Audit every quarter to ensure all is up to date
  3. Refresh the bag after use
Preparation

- Although CIRTs are generally not responsible for securing networks, systems, and applications, it is imperative they assist building a sound security practice
  - Risk Management
  - Host and Network Security
  - Malware Protection
  - User Awareness and Training
Detection & Analysis

*Incidents occur in many ways*

- Common Attack Vectors
  - Email
  - Social Engineering
  - External/Removable Media
  - Attrition
  - Web Application
  - Improper Usage
  - Loss or Theft of Equipment
Accurately detecting, assessing, and confirming incidents is the **most challenging** part of Incident Response

Three factors:

- Incidents are detected by various means
  - Automated: IDS/IPS, AV, SIEMs
  - Manual: By users through phone, email, etc.
- High Traffic volume
- Highly specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data
  - *A mile wide and deep!*
Detection & Analysis

Precursors: A sign that an incident may occur in the future

Indicators: A sign that an incident may have occurred or may be occurring now

- Sources of precursors and indicators:
  - Alerts
  - Logs
  - Publicly Available Information
  - People

- Most attacks have no detectable precursors
Detection & Analysis

- The CIRT should work quickly to analyze and validate each incident
  - Follow the Incident Response Plan and Procedures
  - Document all steps taken

- After validation of an incident, perform an initial analysis to determine the incident’s scope
  - Which networks, systems, and applications are affected
  - Where did the incident originate
  - How the incident is occurring or has occurred
  - Who or what originated the incident

- After the initial analysis, prioritize next steps
  - Assign the incident a severity/priority level
  - Deeper analysis
  - Containment, Eradication, and Recovery
### Detection & Analysis

- **Example of Severity / Priority Classifications**

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Description / Categorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Initial event notification</td>
</tr>
<tr>
<td></td>
<td>Verification of alert or incident needed</td>
</tr>
<tr>
<td></td>
<td>Incident is then escalated if necessary</td>
</tr>
<tr>
<td></td>
<td>Corrective Action is not required</td>
</tr>
<tr>
<td>Medium</td>
<td>Potential escalation from a Low Priority Event</td>
</tr>
<tr>
<td></td>
<td>Event verified as an actual or real incident</td>
</tr>
<tr>
<td></td>
<td>System and Facility Integrity maintained</td>
</tr>
<tr>
<td></td>
<td>Corrective Action may be required</td>
</tr>
<tr>
<td>High</td>
<td>Potential escalation from a Low or Medium Priority Event</td>
</tr>
<tr>
<td></td>
<td>Partial Breach of System or Facility</td>
</tr>
<tr>
<td></td>
<td>Partial loss of System or Facility Integrity</td>
</tr>
<tr>
<td></td>
<td>Corrective Action required</td>
</tr>
<tr>
<td>Critical</td>
<td>Potential escalation from a Low, Medium or High Priority Event</td>
</tr>
<tr>
<td></td>
<td>Complete Breach of System or Facility</td>
</tr>
<tr>
<td></td>
<td>Complete Loss of System or Facility Integrity</td>
</tr>
<tr>
<td></td>
<td>Corrective Action required</td>
</tr>
</tbody>
</table>
Detection & Analysis

• Recommendations for easier and more effective incident analysis
  - Profiling networks and systems to understand normal behavior
  - Create a Log Retention Policy
  - Use a SIEM for event correlation
  - Keep all Host Clocks Synchronized using NTP
  - Maintain and use a knowledge base of Information
  - Use publicly available information for research
  - Seek assistance from external sources
Detection & Analysis

- Incident documentation is most effective when using an Issue Tracking System

- Each incident’s documentation should include:
  - The current status of the incident (new/open, in progress, resolved, etc.)
  - Severity of the Incident
  - A summary of the incident
  - Contact information (e.g., system owners, system administrators)
  - Notification Source
  - Indicators and other incidents related to the incident
  - Actions taken by all incident handlers on this incident
  - Chain of custody, if applicable
  - Impact assessments related to the incident
  - A list of evidence gathered during the incident investigation
  - Notes from incident handlers
  - Next steps to be taken (e.g., rebuild the host, upgrade an application)

- All information/documentation must be time stamped and restricted to authorized personnel
Detection & Analysis

- After analysis, the CIRT must notify appropriate personnel
- The IRP should have documented
  - What must be reported
  - To who must it reported to
  - How to communicate (email, phone, daily briefings)
  - At what times to report it
- Parties include:
  - CIO
  - CISO
  - System Owners
  - HR
  - Legal
  - US-CERT (required for Federal agencies)
Containment, Eradication, & Recovery

• A vital part of containment is **decision-making**
• Containment decisions are much easier if there are predetermined strategies and procedures documented in the IRP
• Strategies should be tailored based on incident type
• Criteria for determining strategy is based on:
  – Potential damage to and theft of resources
  – Need for evidence preservation
  – Service availability time and resources needed to implement the strategy
  – Effectiveness of the strategy
  – Duration of the solution
Containment, Eradication, & Recovery

• Gathering evidence during containment is important as it may be needed for legal investigations
• The IRP should describe the policy on handling evidence
• Chain of Custody must be kept at all times

• Evidence should include:
  – Identifying Information
  – Name, title, and phone number of each individual who collected or handled the evidence
  – Time and date of each occurrence of evidence handling
  – Locations where evidence was stored
Containment, Eradication, & Recovery

- **Eradication** is necessary to eliminate components of the incident
  - Deleting malware
  - Disable breached user accounts
  - Identifying and mitigating all vulnerabilities that were exploited

- **Recovery** restores systems to normal operations and confirms that systems are functioning normally
  - Restoring from clean backups
  - Rebuilding systems from scratch
  - Replacing compromised files with clean versions
  - Patching
  - Changing passwords
  - Tightening network perimeter security
Post-Incident Activities

- A “lessons learned” should be conducted after all major incidents

- Goals of lesson learned meetings:
  - Improves the organization’s security posture
  - Improves incident handling process and trains team members
  - Provides closure to incidents
  - Information sharing across teams throughout the organization

- The lessons learned meeting answers:
  - What went right
  - What went wrong
  - Corrective action plans to prevent similar incidents
  - How well did the staff perform
  - What tools/resources are needed to detect and mitigate future incidents
Post-Incident Activities

• Creation of a follow-up report for each incident
  – Reference used to assist in handling similar incidents
  – Chronology of incident events (including timestamps)
  – Monetary estimate of the amount of damage the incident caused
  – The reports should be in compliance with the organization’s retention policy

• Metrics
  – Show trends
  – Checks performance of CIRT
  – Sways senior management to make decisions and provide guidance
  – Rationale for new tools and more resources
IR Life Cycle Summary

Source: NASA
Incident Taxonomy
## Cyber Security Evolution

<table>
<thead>
<tr>
<th>Reactive</th>
<th>Proactive</th>
<th>Predictive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Response, Notification, Tracking, Analysis, Containment, Eradication, and Remediation</td>
<td>Network Vulnerability Scanning: Network, systems,</td>
<td>Strategic Analysis</td>
</tr>
<tr>
<td>Incident Detection Systems (IDS)</td>
<td>Vulnerability Handling</td>
<td>Threat Management &amp; Correlation System</td>
</tr>
<tr>
<td></td>
<td>Email Filtering &amp; Blocking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Sinkhole</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Tracking, Monitoring, &amp; Mitigation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patch/Asset Management</td>
<td></td>
</tr>
<tr>
<td>Situational Awareness: Log Monitoring, Event Aggregation and Correlation (SIM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow/Network Behavior Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Based Monitoring System (HBSS): Antivirus, Firewall, Anti-Malware, Application White listing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Protection: Intrusion Prevention System (IPS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web &amp; Application Scanning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Scope Analysis &amp; Remote Forensics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Monitoring/Data Loss Prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Team/Blue Team</td>
<td></td>
</tr>
</tbody>
</table>

Source: NASA
ReadyOp

• ReadyOp by Collabria Software
  – Next gen “Incident Command, Communication & Collaboration System”
• Web-based application designed specifically for Incident Command Response
• Integrates all communication onto one unified platform
• Secure and encrypted method of communication
• Capabilities:
  – Develop, store, and institutionalize your IRP
  – Develop, manage, and execute BCP
  – Build a visual DB of your organizational team, assets, and procedures
  – Communicate simultaneously and instantly with any team member
Conclusion

- Incidents will happen
- IRP prepares organizations to handle incidents
- CIRT is responsible to carry out the Incident Response Plan
- Incident Response Program
  - Policy
  - Plan
  - SOPs
- Hold Lessons Learned meetings after major incidents to improve your organization’s security posture
- Audit and re-fine your incident response plan

Move your organization from Reactive to Predictive
References


Building an Effective Incident Response Plan

For further information please contact:

Alex Rodriguez-Triana
Information Security Consultant
GSEC, ITILv3
Enterprise Risk Management, Inc.

305-447-6750 (o)
305-608-4913 (m)
arodriguez@emrisk.com
www.emrisk.com