Information Security
Incident Management Program

What is an Incident Management Program?

- It is a coordinated program of people, processes, tools and technology, which prevents and manages information security threats, vulnerabilities and incidents in order to minimize their impact on a company or organization.

Why is it needed?

- To protect a company’s brand and reputation
- To protect a company’s intellectual property
- To ensure a company’s uninterrupted ability to conduct business
- To avoid lost customers and revenue
- To avoid the cost of lost productivity
- To avoid the cost of cleaning up the effects of security incidents on the IT infrastructure
Normal
Attack & Response Timeline

- Months/Weeks Before
- Days Before
- weeks Before
- Assessment
- Prevention/Protection
- Time of Extreme danger
- Days After
- weeks After
- Analytics/Forensics
- Detection
- Months/Weeks After
Ideal
Attack & Response Timeline

Assessment

Prevention/Protection

Analytics/Forensics

Detection

Small amount of Danger time
Globally prevent, detect and manage IT security threats, vulnerabilities, and incidents to minimize their impact on your organization.

- Threats
- Vulnerabilities
- Incidents

Operational Management Program Value

- Incident ID and Assessment Standards
- Defined and Shared Policies and Processes
- Defined Roles and Responsibilities
- Knowledge Mgmt.
- Relevant Training
- End User Awareness
- Defined Crisis Management
- Coordinated Mgmt. Reporting
- Defined Escalations/Handoffs
- Consistent Escalation Thresholds
- Continuous Improvement
- Standard Tools
- Program Metrics
- Effective Communications
PHASE 1 – ASSESS & PLAN

- **STAKEHOLDER NEEDS**
  - Identify Stakeholders
  - Define Business Value Drivers

- **CURRENT STATE**
  - Gather information to assess

- **FUTURE STATE**
  - Determine desired state

- **GAP ANALYSIS**
  - Due Diligence; Group & prioritize gaps

- **BUSINESS IMPACT ASSESSMENT**
  - Reinforce obvious gaps & Identify new Prioritize risk; RTO, RPO

- **GAP CLOSURE PLAN**
  - Identify & Prioritize Transformation Projects
  - Prepare Implementation Framework
  - Create Project Plan

PHASE 2 – DESIGN & IMPLEMENT

- **ORGANIZE**
  - Establish Project Management Structure
  - Prepare Detailed Project Work Plans
  - Establish Objectives Program Areas

- **REPORTING**
  - Establish program metrics reporting baseline:
    - Weekly
    - Monthly
    - Annually

- **DESIGN & DOCUMENT**
  - Build Program & Program Area Handbook:
    - Roles & Responsibilities
    - Processes
    - Tools
    - Vendor & Inventory Templates
    - Define Partner & Functional Area Agreements

- **IMPLEMENT**
  - Report Vulnerability correlation
  - Incident reporting
  - Prepare/Implement Program & Program Area Tools:
    - SIM Handbooks
    - Risk Level Matrix (per business impact assessment)
    - Crisis Management Handbook

- **TRAIN/BUILD AWARENESS**
  - Create, develop, deliver training & awareness

- **MAINTENANCE**
  - Develop/implement Maintenance Plan

---

**ORANGE CAPS** = Report/Deliverable

**RTO**: Recovery Time Objective

**RPO**: Recovery Point Objective
Incident Management Program Components

Incident Management Program Areas

- Threat Analysis & Response
- Network Intrusion Detection & Response
- Vulnerability Detection
- Escalation & Crisis Management
- Countermeasures
- Anti-Virus

- Information Security Incident Response Team
- Security Monitoring & Reporting
- Program Administration & Analysis
- Investigations & Forensics
- Patch Management
- Program Rollout & Awareness
Threat Analysis and Response

The Threat Analysis and Response Team:

• Proactively researches and monitors security-related information to identify information security threats that may impact your organization

• Threats are analyzed for their impact to your organization and assigned a risk classification

• Informational alerts and remediation requirements are developed and distributed to the appropriate parties throughout your company

• This process ensures threats are consistently addressed in a timely manner throughout the enterprise
The Network Intrusion Detection and Response Team:

- Proactively monitors the Internet-facing infrastructure for signs of network intrusions and other anomalous activities, traffic, etc. This involves ensuring that network intrusion detection sensor (IDS) alerts are properly addressed.
- Assists the Information Security Incident Response Team (ISIRT) in addressing detected attacks in real time
- Works in close cooperation with the Infrastructure Network Team related to the deployment and tuning of network-based intrusion detection sensors
Vulnerability Detection

The Vulnerability Detection Team:

- Conducts regular ongoing vulnerability scans/probes of the Internet-facing infrastructure to identify key high-risk vulnerabilities
- Provides vulnerability data to the Information Security Incident Response Team (ISIRT) so that the vulnerabilities are addressed
- Conducts “special request” scans of the infrastructure
- Rescans vulnerable systems to assess remediation status
- Assists in the management of exception requests related to vulnerability remediation
Escalation & Crisis Management

The Information Security Escalation & Crisis Management Team:

• Prepares for and addresses those unique information security-related incidents that are anticipated to cause significant impact or have caused enterprise-wide severe impact or interruption.
Countermeasures

The Information Security Countermeasures Team:

- Conducts regular and targeted scanning for specific critical information security vulnerabilities and/or compromised systems
- Delivers a customized payload to the impacted system which results in the mitigation of the vulnerability and/or the remote shut-down/disabling of the impacted system
Anti-Virus

The Information Security Anti-Virus Team:

- Plans and implements the company’s AntiVirus strategy (e.g., choice of tools, tool deployment, etc.)
- Obtains and tests new versions of AntiVirus tools when they are made available
- Facilitates the communication of AntiVirus strategy, directions and tools available
The Information Security Incident Response Team (ISIRT):

- Is a global team with corporate-wide responsibilities pertaining to receiving, assessing, responding to, addressing and managing information security incidents.
- Depending on the severity of incidents, ISIRT will own, hand-off, address, or escalate security incidents, thus ensuring incidents are handled commensurate with their level of risk.
Infosec Security Monitoring and Reporting

The Information Security Monitoring and Reporting Team:

- Monitors patching compliance related to high-risk vulnerabilities for internal systems where these conditions can be remotely detected.
- Works closely with regional and business security teams, IT delivery teams, and other teams within Information Security and the Information Security Incident Management Program.
Program Administration and Analysis

The Program Administration and Analysis Team:

- Collects, consolidates, analyzes and provides specific audience-based reports related to the functional programs within the Information Security Threat, Vulnerability and Incident Management Program.

- This Team also conducts strategic planning and budgeting and leads the program/project management and maintenance activities within the Program.
Investigations and Forensics

The Information Security Investigations & Forensics Team:

- Addresses serious information security related incidents which involve civil, criminal, administrative, disciplinary, brand and/or financial implications
- Works closely with internal partners such as Legal, HR/ER, Media Relations and Security and external parties such as law enforcement and government authorities
- Has ability to recover, decrypt, and analyze IT-related data and report, present, and represent such data in civil, criminal, and administrative proceedings
Patch Management

The Information Security Patch Management Team:

- Works in conjunction with Threat Analysis and Response and Vulnerability Detection program areas
- Provides system owners with remediation information related to high-risk vulnerabilities affecting the company’s infrastructure
- Creates weekly reports which track number of vulnerable systems detected and number of systems remediated
InfoSec Program Rollout and Awareness

The Information Security Program Rollout and Awareness Team:

- Develops and delivers end-user and partner-focused communications and awareness activities to increase understanding, use of, and compliance related to the Information Security Threat, Vulnerability and Incident Management Program.
Typical Lifecycle
(Primarily Depicting Reactive Processes)

Triggers
- Incident Initiation
- Incident Management

- Intrusion Detection
- Vulnerability Detection
- Threat Analysis
- Anti-Virus
- Countermeasures
- Compliance Monitoring

- Crisis Management
- Investigations & Forensics
- Incident Response Team
- Countermeasures
- Countermeasures

Authorized New System/Application
New Threat/Vulnerability
Incident Report
Unauthorized Device
Unauthorized Action
Investigation Request

Incident Detection
Proactive Threat Discovery
Receive Report of Incident
System/Network Monitoring
Compliance Monitoring
Incident Resulting from Investigation
Targeted Vulnerability Testing
Threat and Vulnerability Database
Threat Severity Assignment
Threat Investigation/Analysis
Build Configuration

Dashboard
Monitoring/Reporting
Crisis Management
Remediation Actions
Investigation
Compliance Testing
Post Mortem

Incident Resulting from Investigation
Investigation
Incident Response
Remediation Actions
Crisis Management
Compliance Testing
Post Mortem

Receive Report of Incident

Crisis Management
Remediation Actions
Investigation
Compliance Testing
Post Mortem

Information Security
Incident Management Program

Incident Management Tools

• An effective Incident Management Program requires specific tools be developed. Examples include:
  − Security Incident Cost Calculator
  − Risk Assessment Matrix
  − Crisis Management Manual
  − Incident Management Handbook

• Each tool must be customized for the specific business structure and IT infrastructure of a given company

• It is difficult for a company to develop these tools without outside help
## Incident Management Tools

### Security Incident Cost Calculator

#### Incident Management Program

**Per Incident Cost**

**Instructions** - Please fill in all fields highlighted in yellow.

<table>
<thead>
<tr>
<th>Productivity Loss</th>
<th>Total</th>
<th>AP</th>
<th>Japan</th>
<th>EMEA</th>
<th>Latin America</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Servers Affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average # of Hours of Server Downtime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average # of Users on Server During This Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Clients or PCs Affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average # of Hours of Client or PC Downtime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average # of Users on Clients or PCs During This Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Employees Reading Messaging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Hours Reading Messaging per Employee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Employees Required to Perform Actions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Hours Implementing Required Actions per Employee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hourly Rate per Employee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Productivity Loss Subtotal**

| #VALUE! | #VALUE! | #VALUE! | #VALUE! | #VALUE! |

#### Call Center Costs

<table>
<thead>
<tr>
<th># of Support Calls</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Length of Call (in Hours)</td>
<td>0</td>
</tr>
</tbody>
</table>

| Cost per Call or Hour | | | | | |
Considerations for calculating the cost of security incidents

Know your downtime cost: per hour, per day, per Business Unit…

Productivity
- Number employees impacted x hours out
  x burdened hours =

Revenue
- Direct loss
- Compensatory payment
- Lost future revenues
- Billing losses
- Investment losses

Financial performance
- Revenue recognition
- Cash flow
- Payment guarantees
- Credit rating
- Stock price

Damaged reputation
- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Other expenses
- Temporary employees
- Equipment rental
- Overtime & travel costs
- Extra shipping expenses
Incident Management Tools

Risk Assessment Matrix

• A Risk Assessment Matrix provides a quick and consistent way to evaluate the risk severity of an information security threat, vulnerability or incident. It standardizes escalation triggers, thresholds and actions across the Incident Management Program.

• The Risk Assessment Matrix serves as a strong guideline for the initiation of a crisis or escalation and contains a series of metrics to help users identify the level of escalation. Scores are assigned in the areas of:
  • The likelihood of an information security threat, vulnerability, or incident impacting the IT Infrastructure and
  • The potential impact if the threat, vulnerability, or incident begins to impact the IT Infrastructure (including, but not limited to brand, financials, employees, customers, data/information loss, etc.)
Incident Management Tools

Risk Assessment Matrix

- The likelihood score is multiplied by the potential impact score, giving a Risk Score which is used to identify the predetermined actions to be undertaken.

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk Score</th>
<th>Action/Response</th>
<th>Deadlines for required actions</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis</td>
<td>16-20</td>
<td>Action A</td>
<td>Deadline A</td>
<td>Example A</td>
</tr>
<tr>
<td>High</td>
<td>12-15*</td>
<td>Action B</td>
<td>Deadline B</td>
<td>Example B</td>
</tr>
<tr>
<td>Medium</td>
<td>5-11</td>
<td>Action C</td>
<td>Deadline C</td>
<td>Example C</td>
</tr>
<tr>
<td>Low</td>
<td>1-4</td>
<td>Action D</td>
<td>Deadline D</td>
<td>Example D</td>
</tr>
</tbody>
</table>

Likelihood Matrix

<table>
<thead>
<tr>
<th>Likelihood Rating</th>
<th>Likelihood</th>
<th>Impact Event Impacting</th>
<th>Threat Assessment</th>
<th>Vulnerability Remediaion is exploit available?</th>
<th>Risk Mitigation Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Immediate:</td>
<td>Currently</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Imminent:</td>
<td>Very attractive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Likely:</td>
<td>Attractive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Not likely:</td>
<td>Somewhat attractive</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Impact Matrix

<table>
<thead>
<tr>
<th>Impact Rating</th>
<th>Systems</th>
<th>Data and Information</th>
<th>Financial ($)</th>
<th>Brand</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>External (I)</td>
<td>Internal (I)</td>
<td>Access</td>
<td>XXXX Proprietary Information</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incident Management Tools

Crisis Management Manual

• The Crisis Management Manual is a tool to assist on-call crisis managers in the event of an Information Security related crisis.

• The Manual creates a standard process for managing high-profile incidents to ensure an immediate, appropriate, and consistent response to a geographic or worldwide crisis situation. This enables the Crisis Manager to take control of the crisis environment and manage the flow of information to most effectively protect the organization.

• In addition to aiding the Crisis Manager, the Manual contains tools, templates, flow charts, checklists and processes and outlines the responsibilities of other critical parties in the management of a crisis.
Incident Management Tools

Incident Management Program Handbook

- The Handbook is a tool utilized by all members of the Incident Management Program. It contains all job descriptions, roles and responsibilities, processes and tools documentation for each of the Program components.

- The Handbook provides a standard, easily accessible repository for securing all important Program documentation which lends consistency and stability to the IM Program.

- The Handbook is primarily utilized in a virtual manner with all documents undergoing regular scheduled review and update.