Incident Response Program Guidelines

Introduction

An incident response program is an organized approach to addressing and managing the aftermath of a security breach of customer information or technological attack. All business customers should develop procedures for assessing security incidents that have occurred, identifying the customer information and information systems that have been accessed or misused and containing and controlling the security incident. The Customer should also establish notification procedures for appropriate law enforcement agencies and affected customers.

The Bank has created the following guidelines defining what should be included in an Incident Response Program to assist our customers in managing an incident.

Develop an Incident Response Report Form

This form should include/not limited to the following:
a. **Incident Details** – time and date of incident, type of incident
b. **Customer Information** – Customer contact information, account numbers
c. **Suspect Information** – if known
d. **Detailed description of incident** – chronological order of events that occurred
e. **Immediate Corrective Actions** – immediate actions to contain the incident
f. **Long Term Corrective Actions** – long term actions to correct the incident and mitigate future risks
g. **Incident Response Team Members** – list of members assembled with data and time
h. **Management Notified** – who was notified with date and time
i. **Agencies contacted** – what agencies were notified with date and time
j. **Person Reporting the Incident**
k. **Person Completing the Form**
l. **Management Review and Signature**

Immediate Actions

The person or employee identifying the event should take immediate action. Possible immediate actions to be taken:
a. Identify the volume and type of information that has been lost
b. Create a list of customers that were probably included in the compromised data
c. Determine the likelihood that the information has been used or may be misused
d. Contact network security consultants, if applicable
e. Halt internet traffic, if necessary

f. Isolate segments of the network
g. Take servers, routers or other critical equipment offline
h. Take any steps necessary to preserve forensic evidence
i. Notify the Incident Response Team

Secondary Actions

Possible secondary actions to be taken:
a. Report incident to the management
b. Take any additional steps needed to gather and retain intrusion forensic information
c. Contact law enforcement agencies
d. Contact insurance carriers
e. Make a decision on whether or not to notify the customers that were affected

Compile & Analyze

a. How was the data compromised
b. Has the information been used or may it be misused
c. Method used to gain access to the sensitive customer information or system
d. The extent of the intruder's access to systems or customer data
e. The intruders past and current activities

Preservation of Evidence

All data concerning the event should be written to a tamperproof device such as a write-once CD ROM. Backup tapes may be used if data volume dictates. All paper reports compiled along with computer storage media pertaining to the event should be placed in the control of the Incident Response Team leader and/or their designee.

Eradicate the Event

If a system has been compromised, the event should be cleaned from the system by removing potential contaminants, infected or breached systems or areas and restoring from backups made before the event.