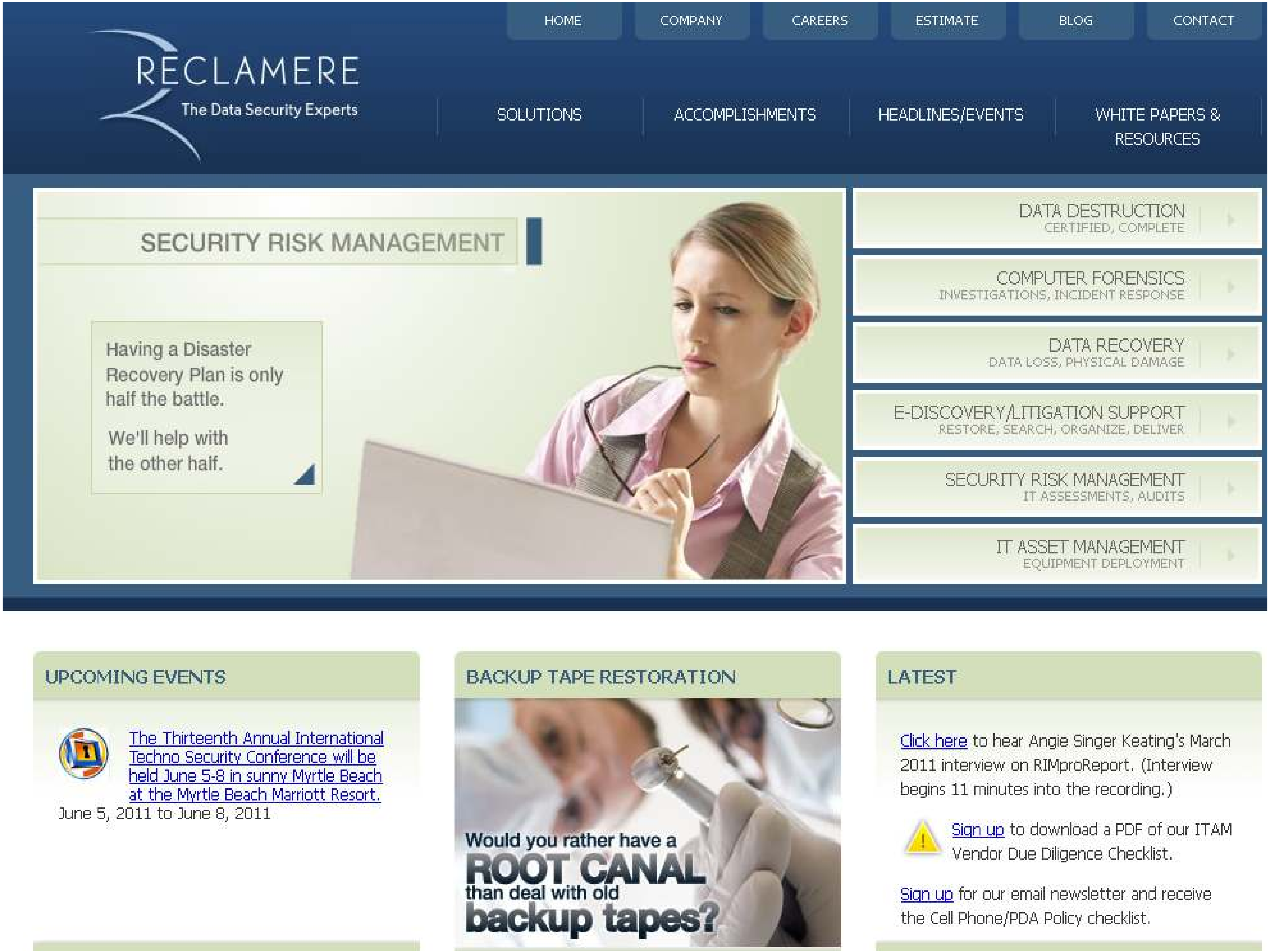
Incident Response

Is Your CSIRT Program Ready for the 21st Century?



RECLAMERE
The Data Security Experts

SECURITY RISK MANAGEMENT

Having a Disaster Recovery Plan is only half the battle.

We'll help with the other half.

UPCOMING EVENTS

The Thirteenth Annual International Techno Security Conference will be held June 5-8 in sunny Myrtle Beach at the Myrtle Beach Marriott Resort.
June 5, 2011 to June 8, 2011

BACKUP TAPE RESTORATION

LATEST

Click here to hear Angie Singer Keating's March 2011 interview on RIMproReport. (Interview begins 11 minutes into the recording.)

Sign up to download a PDF of our ITAM Vendor Due Diligence Checklist.

Sign up for our email newsletter and receive the Cell Phone/PDA Policy checklist.

Traditional Response Concepts

Technical Incidents Requiring Technical Responses

Virus/ Malware

- Contain
- Prevent Spreading
- Analyze Impact

Network Intrusion

- Secure the Perimeter
- Harden the Perimeter

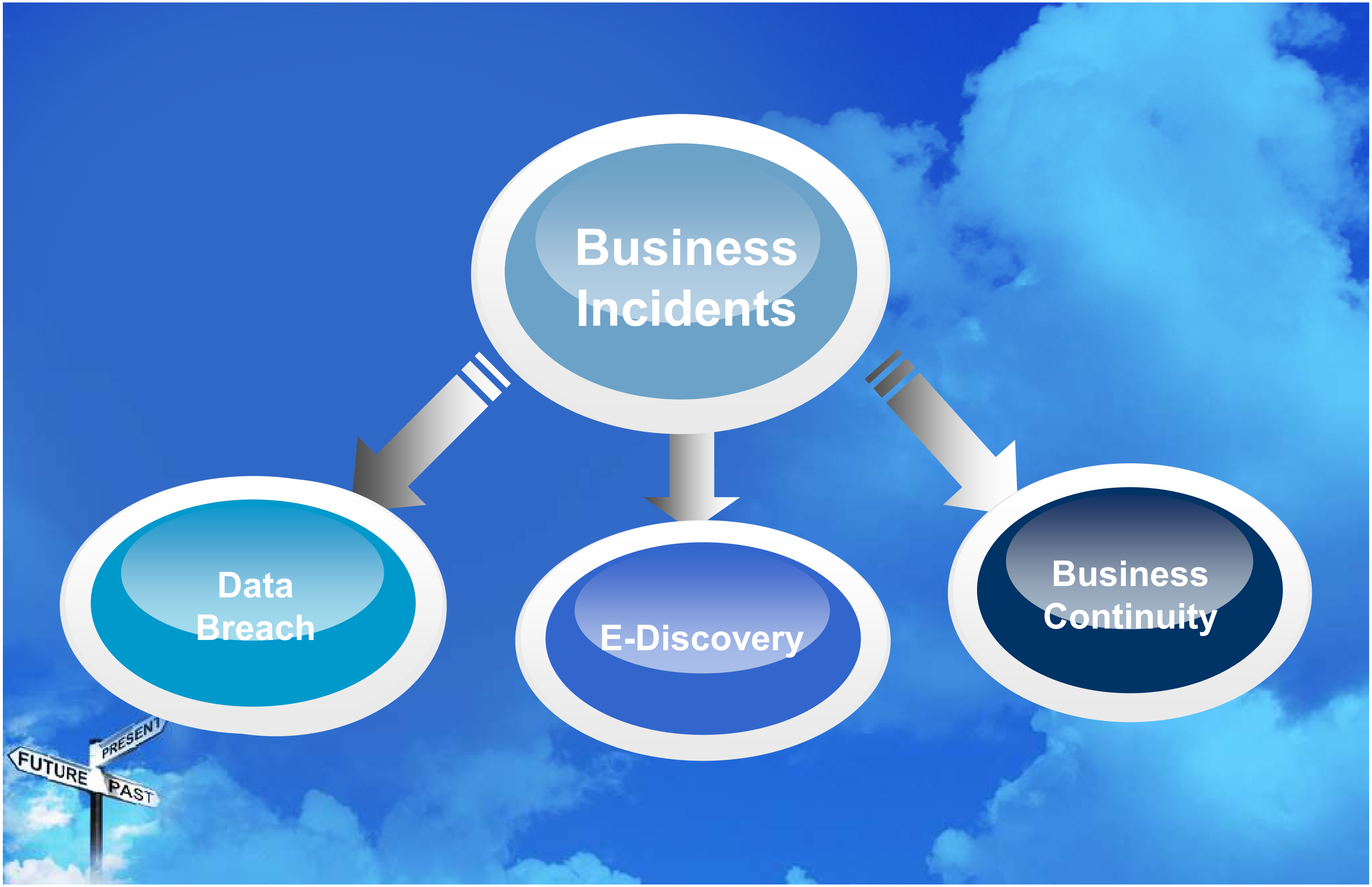
Disaster Recovery

- Hot/Warm Cold Sites
- Recovery Point Objectives

Equipment Issues

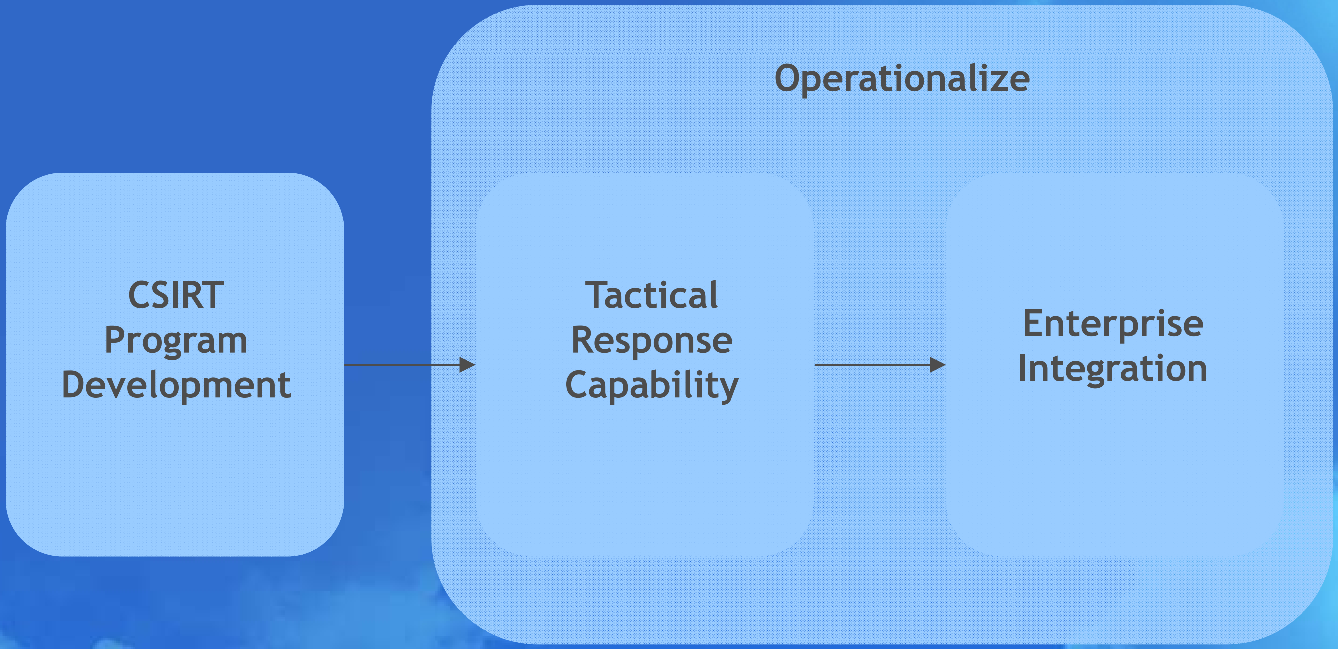
- Lost/ Stolen Equipment
- Employee Misconduct

Today's Response Concepts



Phase Overview

- An incident response program should be assembled in phases that when completed will produce a holistic capability that can service organizational requirements.



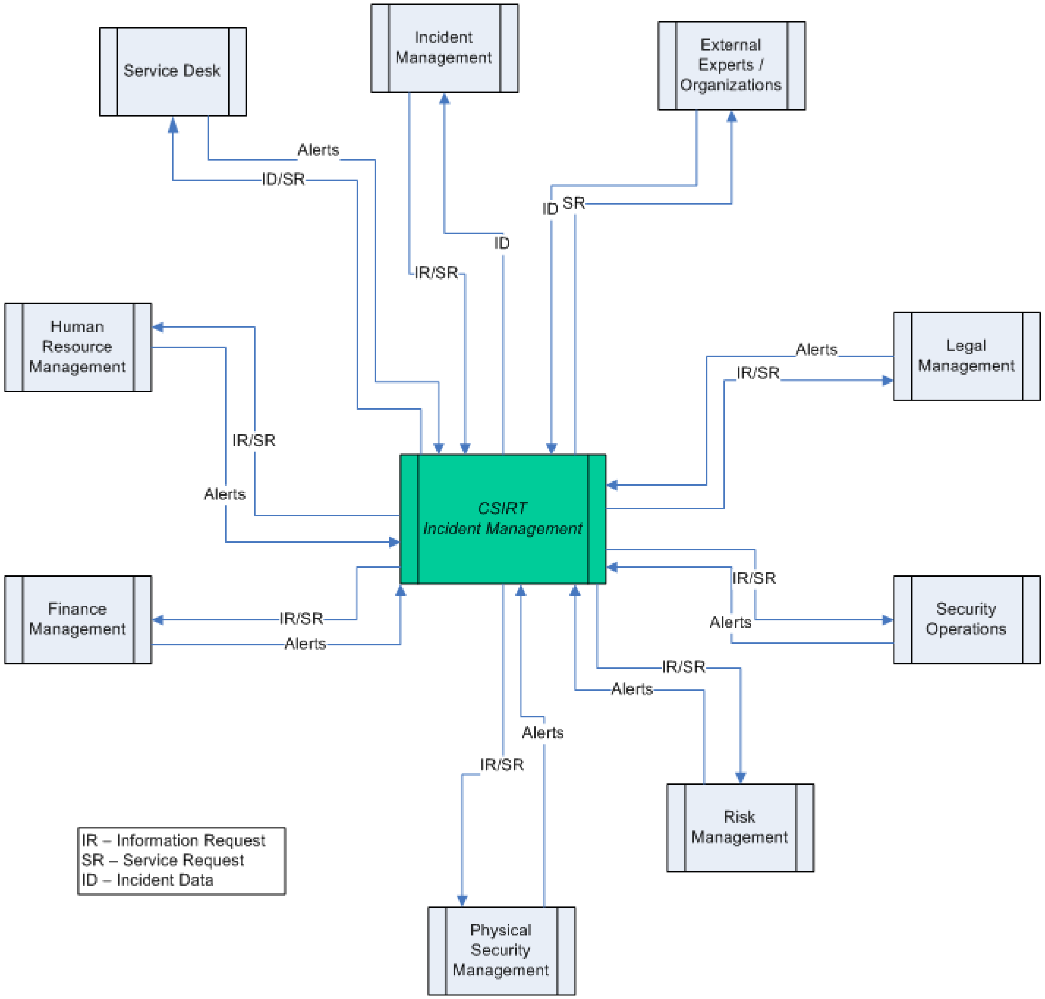
Operationalize

CSIRT Program Development

Tactical Response Capability

Enterprise Integration

PHASE 1: CSIRT program development - process integration



A CSIRT incident management process must describe the relationship with:

- Current corporate incident management process; and
- Other corporate business processes that will require interaction.

PHASE 1: CSIRT program development - CSIRT process

INCIDENT INGRESS

Incident Identification

Logging & Categorization

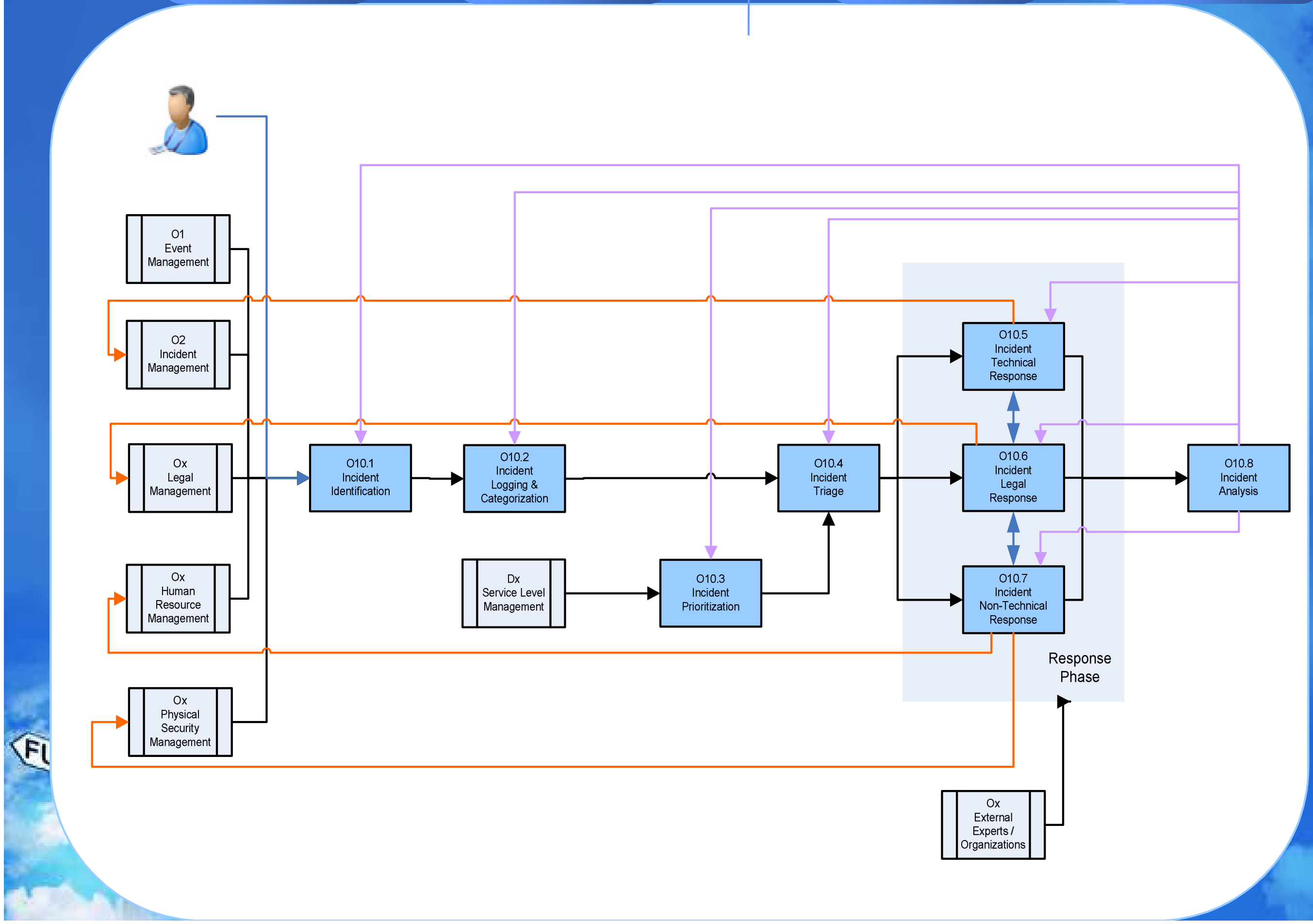
INCIDENT HANDLING

Incident Triage

Incident Response

PROCESS IMPROVEMENT

Incident Analysis



O1 Event Management
O2 Incident Management
Ox Legal Management
Ox Human Resource Management
Ox Physical Security Management
O10.1 Incident Identification
O10.2 Incident Logging & Categorization
Dx Service Level Management
O10.3 Incident Prioritization
O10.4 Incident Triage
O10.5 Incident Technical Response
O10.6 Incident Legal Response
O10.7 Incident Non-Technical Response
O10.8 Incident Analysis
Response Phase
Ox External Experts / Organizations

The major elements of a CSIRT process must be defined, with each of the elements having accompanying detailed procedures.

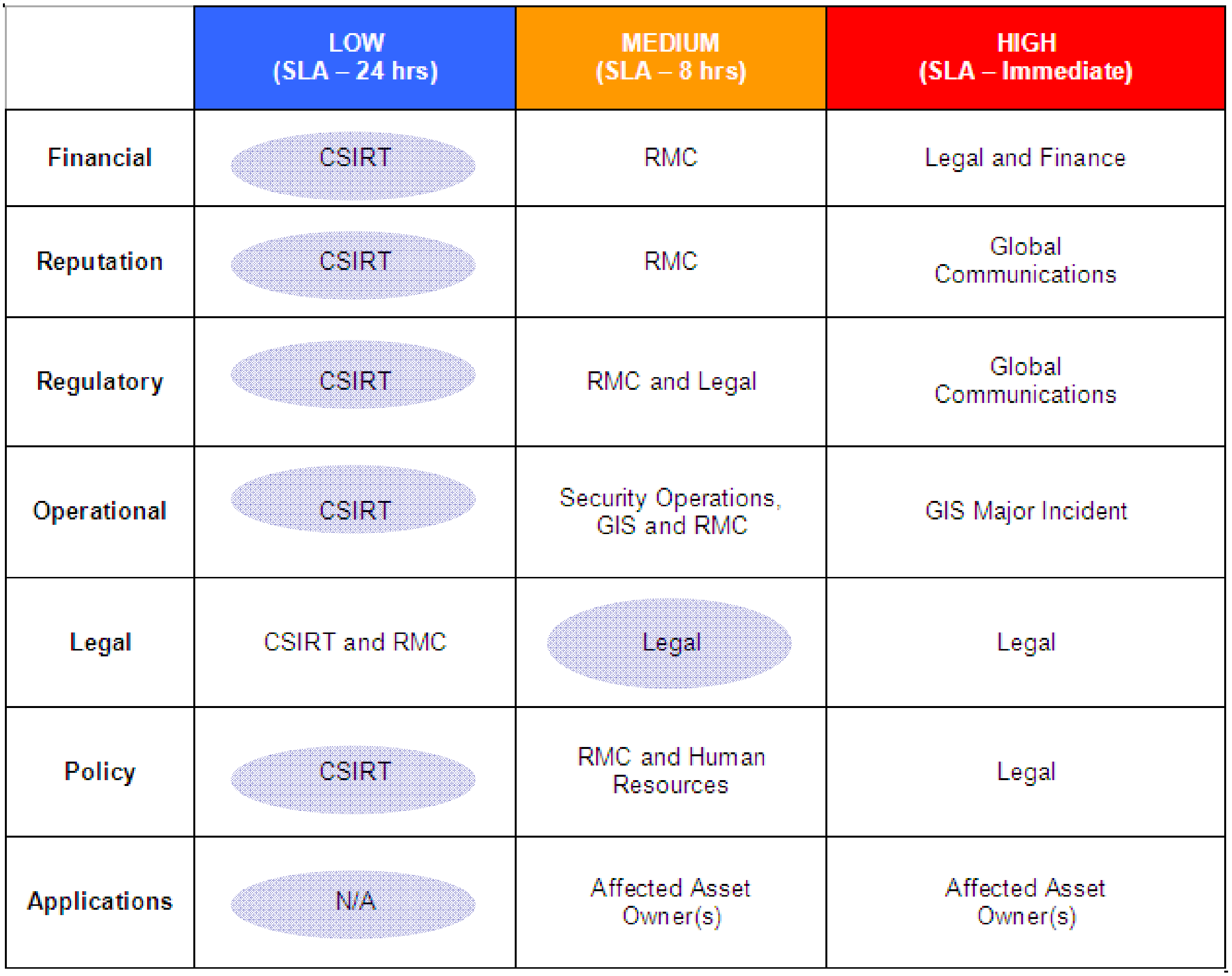
PHASE 1: CSIRT program development - incident ingress process

An incident's priority can be determined by establishing the highest level of impact on the organization using an established matrix.

	LOW (SLA – 24 hrs)	MEDIUM (SLA – 8 hrs)	HIGH (SLA – Immediate)
Financial	Little to None	$100K to $250K	> $250K
Reputation	Little to None	Localized	Widespread
Regulatory	Minor to No Infringement	Significant Infringement without PII of PCI Data Disclosure	Disclosure of PII or PCI Information, Requiring Either Internal or External Notification
Operational	Little to None	Localized and/or Moderate Impact	Widespread and/or Severe Impact
Legal	Little to None	Legal Action (civil and/or criminal) Unlikely Direct Request by Legal Department	Legal Action (civil and/or criminal) Likely
Policy	Minor to No Infringement	Inappropriate but Not Malicious	Suspected Malicious Intent
Application	N/A	N/A	PCI, PII Data Bearing

PHASE 1: CSIRT program development - incident ingress process

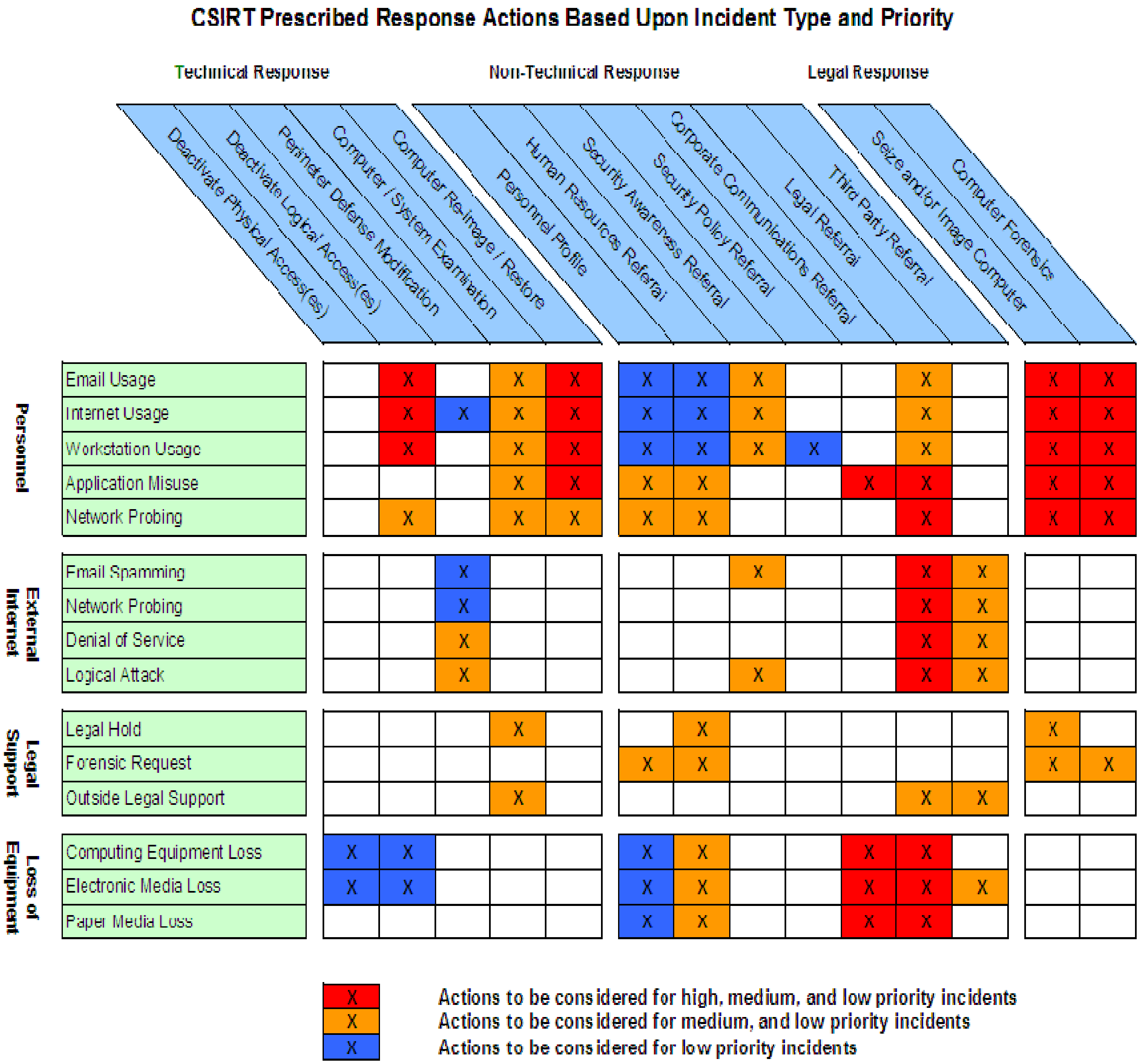
Now a CSIRT process can effectively utilize a Reporting Escalation Matrix to ascertain which departments should receive immediate alerts about an incident.



	LOW (SLA – 24 hrs)	MEDIUM (SLA – 8 hrs)	HIGH (SLA – Immediate)
Financial	CSIRT	RMC	Legal and Finance
Reputation	CSIRT	RMC	Global Communications
Regulatory	CSIRT	RMC and Legal	Global Communications
Operational	CSIRT	Security Operations, GIS and RMC	GIS Major Incident
Legal	CSIRT and RMC	Legal	Legal
Policy	CSIRT	RMC and Human Resources	Legal
Applications	N/A	Affected Asset Owner(s)	Affected Asset Owner(s)

PHASE 1: CSIRT program development - incident handling process

Once an incident has been properly categorized, utilizing a response matrix ensures that incidents are handled in a standard and repeatable fashion.

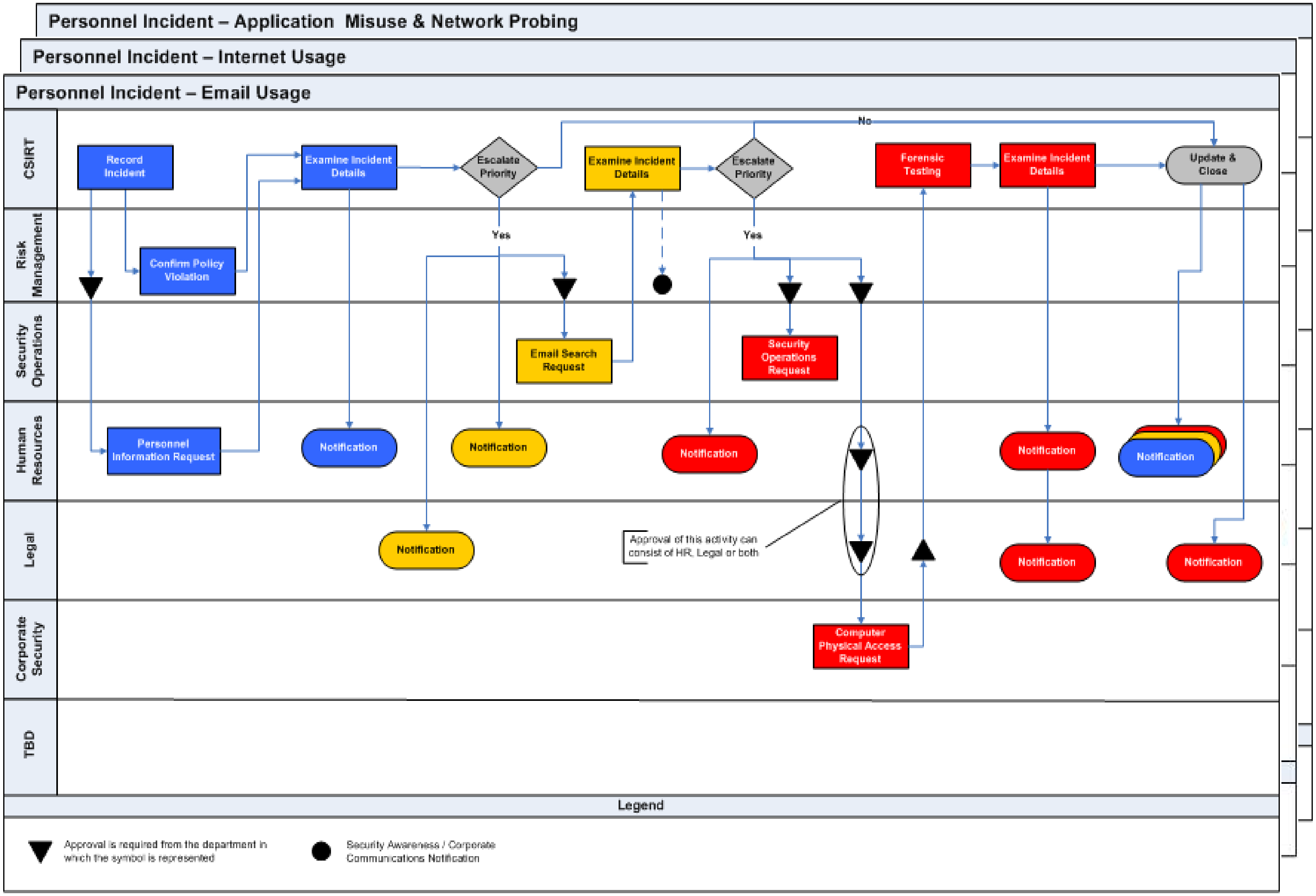


CSIRT Prescribed Response Actions Based Upon Incident Type and Priority

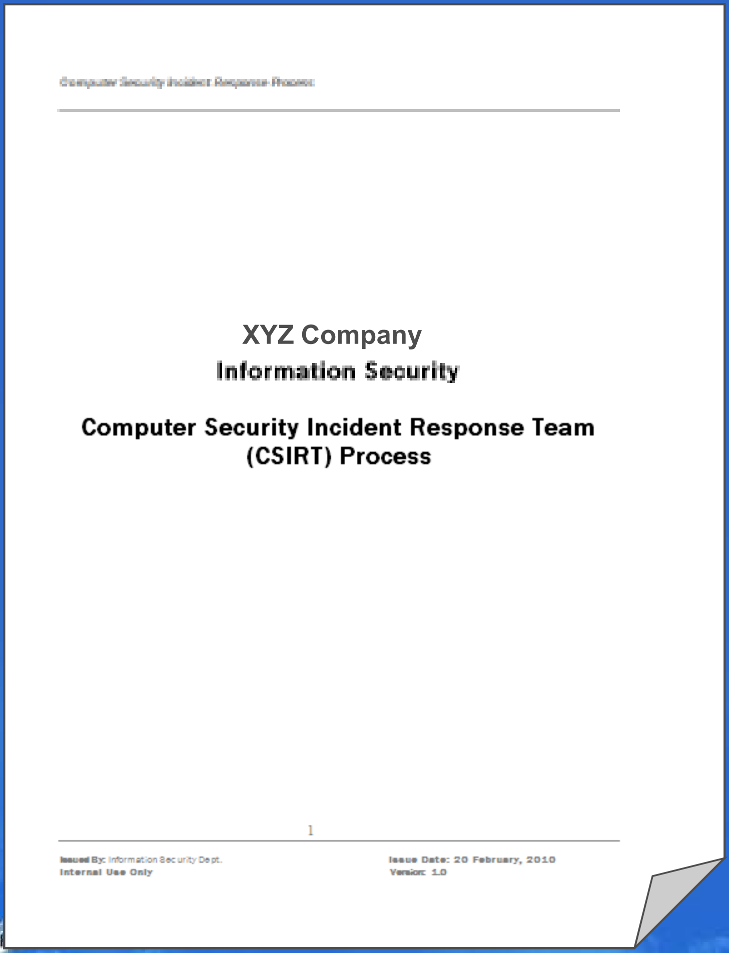
		Technical Response					Non-Technical Response							Legal Response	
		Deactivate Physical Access(es)	Deactivate Logical Access(es)	Perimeter Defense Modification	Computer / System Examination	Computer Re-image / Restore	Personnel Profile	Human Resources Referral	Security Awareness Referral	Security Policy Referral	Corporate Communications Referral	Legal Referral	Third Party Referral	Seize and/or Image Computer	Computer Forensics
Personnel	Email Usage		🟥 X		🟧 X	🟥 X	🟦 X	🟦 X	🟧 X			🟧 X		🟥 X	🟥 X
	Internet Usage		🟥 X	🟦 X	🟧 X	🟥 X	🟦 X	🟦 X	🟧 X			🟧 X		🟥 X	🟥 X
	Workstation Usage		🟥 X		🟧 X	🟥 X	🟦 X	🟦 X	🟧 X	🟦 X		🟧 X		🟥 X	🟥 X
	Application Misuse				🟧 X	🟥 X	🟧 X	🟧 X			🟥 X	🟥 X		🟥 X	🟥 X
	Network Probing		🟧 X		🟧 X	🟧 X	🟧 X	🟧 X				🟥 X		🟥 X	🟥 X
External Internet	Email Spamming			🟦 X					🟧 X			🟥 X	🟧 X		
	Network Probing			🟦 X								🟥 X	🟧 X		
	Denial of Service			🟧 X								🟥 X	🟧 X		
	Logical Attack			🟧 X					🟧 X			🟥 X	🟧 X		
Legal Support	Legal Hold				🟧 X			🟧 X						🟧 X	
	Forensic Request						🟧 X	🟧 X						🟧 X	🟧 X
	Outside Legal Support				🟧 X							🟧 X	🟧 X		
Loss of Equipment	Computing Equipment Loss	🟦 X	🟦 X				🟦 X	🟧 X			🟥 X	🟥 X			
	Electronic Media Loss	🟦 X	🟦 X				🟦 X	🟧 X			🟥 X	🟥 X	🟧 X		
	Paper Media Loss						🟦 X	🟧 X			🟥 X	🟥 X			

🟥 X Actions to be considered for high, medium, and low priority incidents
🟧 X Actions to be considered for medium, and low priority incidents
🟦 X Actions to be considered for low priority incidents

PHASE 1: CSIRT program development - incident handling process


Personnel Incident – Application Misuse & Network Probing
Personnel Incident – Internet Usage
Personnel Incident – Email Usage
CSIRT
Risk Management
Security Operations
Human Resources
Legal
Corporate Security
TBD
Record Incident
Examine Incident Details
Escalate Priority
Examine Incident Details
Escalate Priority
Forensic Testing
Examine Incident Details
Update & Close
No
Yes
Yes
Confirm Policy Violation
Email Search Request
Security Operations Request
Personnel Information Request
Notification
Notification
Notification
Notification
Notification
Notification
Notification
Approval of this activity can consist of HR, Legal or both
Notification
Notification
Computer Physical Access Request
Legend
▼ Approval is required from the department in which the symbol is represented
● Security Awareness / Corporate Communications Notification

PHASE 1: CSIRT program development – documentation



Computer Security Incident Response Process

XYZ Company

Information Security

Computer Security Incident Response Team (CSIRT) Process

1

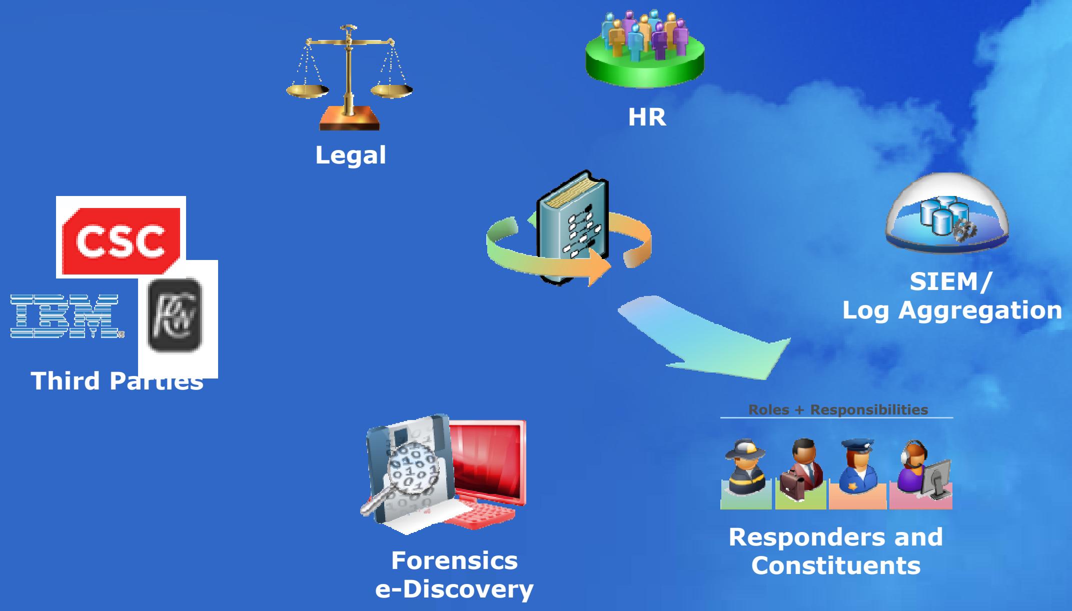
Issued By: Information Security Dept.
Internal Use Only

Issue Date: 20 February, 2010
Version: 1.0

The result is a codified, documented process guide that serves multiple functions.

- ❑ Reference for both incident responders and various organizational departments
- ❑ Satisfies regulatory requirements
- ❑ Evidence documentation for internal and external audits

PHASE 2: Tactical response capability - relationships



Legal

HR

Third Parties

SIEM/
Log Aggregation

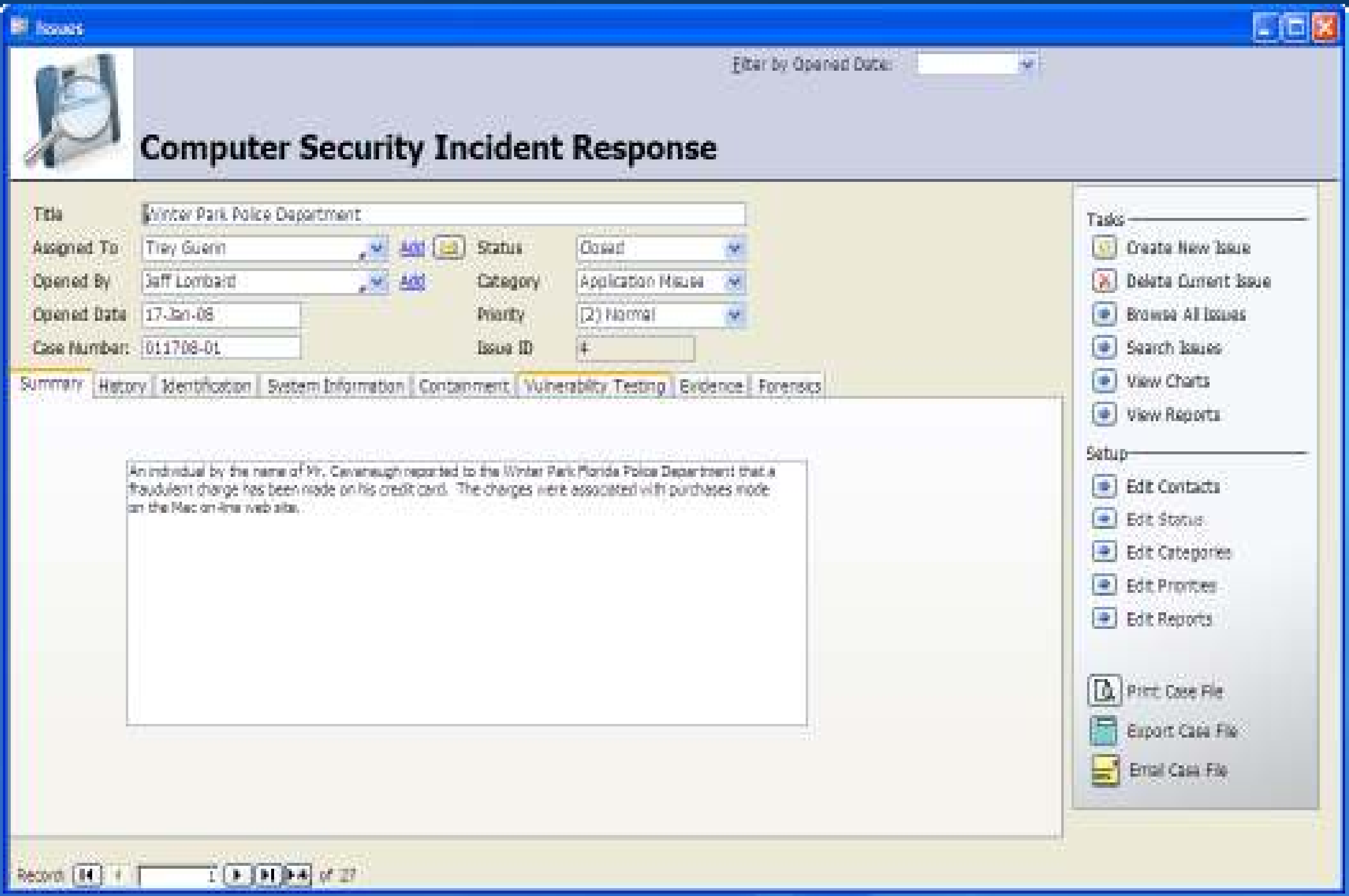
Roles + Responsibilities

Responders and
Constituents

Forensics
e-Discovery

Once an organization develops its response program, it will find it necessary to establish relationships with key departments and third parties. Communication with these entities must be governed by processes and necessary approvals to ensure that sensitive information is handled appropriately.

PHASE 2: Tactical response capability – logging and tracking



Computer Security Incident Response

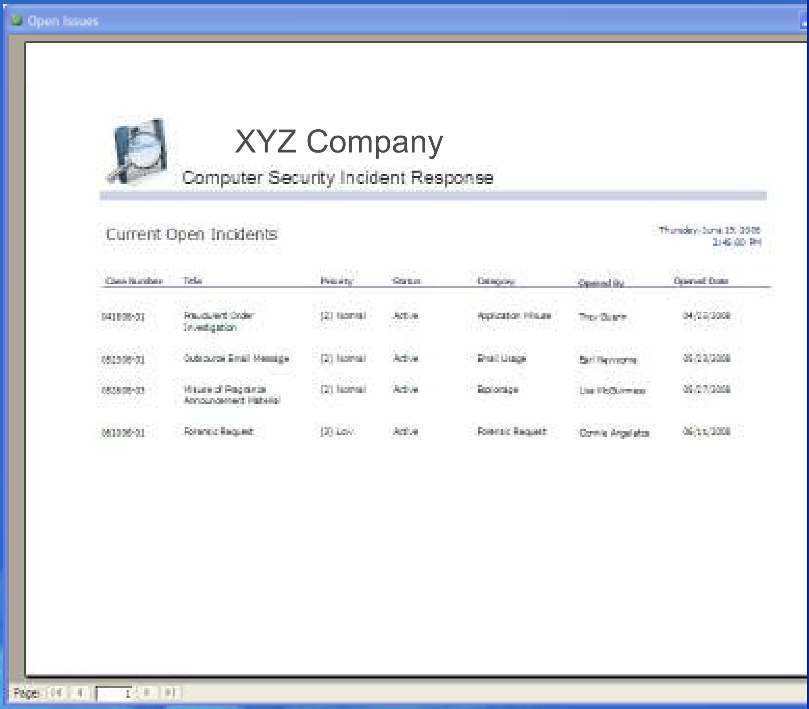
Title	Winter Park Police Department		
Assigned To	Trey Guerin	Status	Closed
Opened By	Jeff Lombard	Category	Application Misuse
Opened Date	17-Jan-08	Priority	(2) Normal
Case Number:	011708-01	Issue ID	4

An individual by the name of Mr. Cavenaugh reported to the Winter Park Florida Police Department that a fraudulent charge has been made on his credit card. The charges were associated with purchases made on the Mac on-line web site.

An organization should establish at least a basic mechanism to document computer security related incidents. Additionally, any captured or stored evidence should be tracked to facilitate compliance with record retention policies.

PHASE 2: Tactical response capability – reporting

Basic status and trending reports should be made available to appropriate management personnel.



Open Issues

XYZ Company

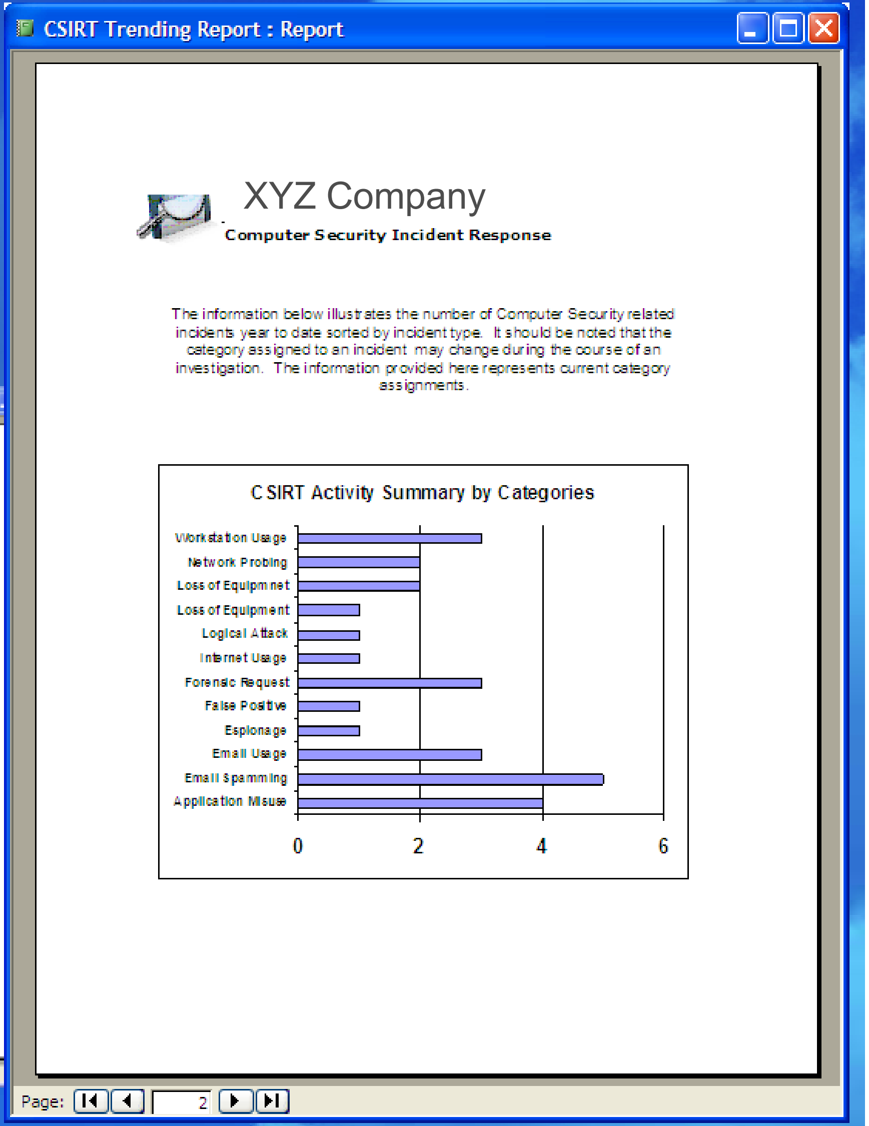
Computer Security Incident Response

Current Open Incidents

Thursday, June 15, 2006
3:46:00 PM

Case Number	Title	Priority	Status	Category	Opened By	Opened Date
041808-01	Fraudulent Order Investigation	(2) Normal	Active	Application Misuse	Troy Quarm	04/22/2008
052308-01	Outsource Email Message	(2) Normal	Active	Email Usage	Earl Remmons	05/23/2008
052508-03	Misuse of Plagiarize Announcement Material	(2) Normal	Active	Espionage	Lisa McGuinness	05/27/2008
061308-01	Forensic Request	(3) Low	Active	Forensic Request	Connie Angelatos	06/11/2008

Page: 1



CSIRT Trending Report : Report

XYZ Company

Computer Security Incident Response

The information below illustrates the number of Computer Security related incidents year to date sorted by incident type. It should be noted that the category assigned to an incident may change during the course of an investigation. The information provided here represents current category assignments.

CSIRT Activity Summary by Categories

Page: 2

PHASE 3: Enterprise incident management

While not necessary for an organization’s CSIRT to be effective, maximum efficiency can be achieved by employing an enterprise solution; one that is specifically designed to support incident response case management. Key benefits include:

❑ Electronic manifestation of documented CSIRT process

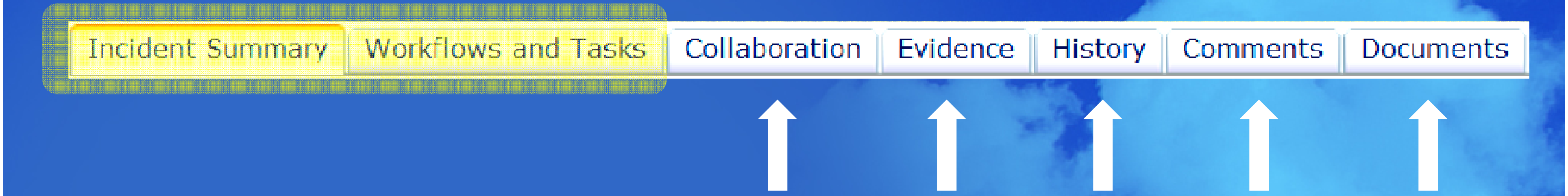
❑ Promotes and ensures proper approvals for CSIRT member actions

❑ Facilitates inter-departmental and team communications

❑ Centralized repository for case information

❑ Real time documentation associated with all actions taken

PHASE 3: Enterprise incident management



Serving as the central repository for all CSIRT incidents, an application has the ability to capture a variety of case related information including:

- ❑ **Collaboration** – dialogs initiated from within the application, whether email or chat, can be included in the case archives
- ❑ **Evidence** – Automatically document all collected evidence
- ❑ **History** – A complete case history is assembled in real time
- ❑ **Comments** – Case coordinators have the ability to append comments at any time to the case file
- ❑ **Documents** – Files can be uploaded and stored within the case file

NIST SP 800-61

National Institute of Standards and Technology

Computer Security Incident Handling Guide

Revision 2 – August 2012

Organizing a response capability

- Establish a formal incident response capability.
- Create an incident response policy.
- Develop an incident response plan based on the incident response policy.
- Develop incident response procedures.
- Establish policies and procedures regarding incident-related information sharing.

Organizing a response capability (con’t)

- Provide pertinent information on incidents to the appropriate organization.
- Consider the relevant factors when selecting an incident response team model.
- Select people with appropriate skills for the incident response team.
- Identify other groups within the organization that many need to participate in incident handling.
- Determine which services the team should offer.

Events and incidents

Event –

- any observable occurrence in a system or network
- Examples of events?

Computer security incident –

- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
- Examples of incidents?

Policy vs. Plan vs. Procedure

Policy –

- Governs the response capability

Plan –

- How the organization responds to an incident

Procedure –

- SOP documents specific tactics

Team Structure

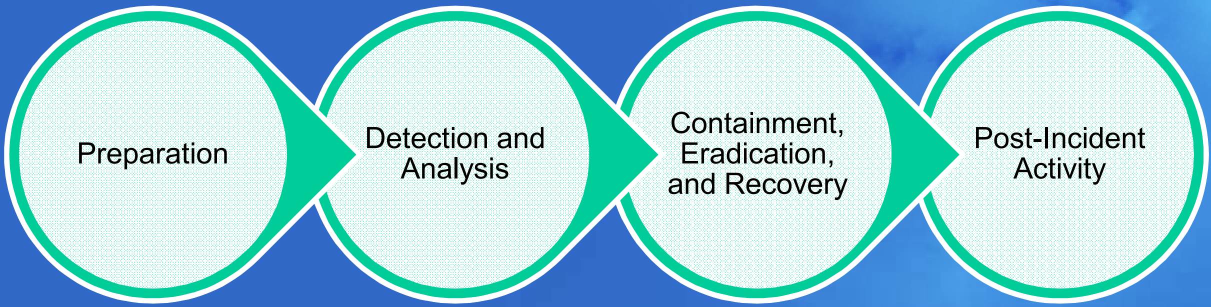
Three organizational models

- Centralized team
- Distributed team
- Coordinating team

Three staffing models

- Employees
- Partially outsourced
- Fully outsourced

Handling an Incident



Preparation

Two main preparation activities:

- Preparing to handle incidents
- Preventing incidents

Detection and Analysis

- Be prepared to handle incidents from common attack vectors.

Understand Signs of an Incident

Precursors

- Web server log entries showing usage of a vulnerability scanner
- New exploit targeting your mail server

Indicators

- IDS alerts
- Antivirus alerts
- Sysadmin sees suspicious activity

Incident Analysis Recommendations

- Profile networks and systems
- Understand normal behaviors
- Create a log retention policy
- Perform event correlation
- Keep all hosts clocks synchronized
- Maintain and use a knowledge base of information
- Use Internet search engines for research
- Run packet sniffers
- Filter the data
- Seek assistance from others

Document, document, document

Incident Prioritization

- Functional impact of the incident
- Information impact of the incident
- Recoverability from the incident

Notification

Your plan should detail who gets status updates and when

- CEO
- Head of security
- Law enforcement
- Users

Containment, Eradication, and Recovery

- Choose a containment strategy
- Evidence gathering and handling
- Identifying the attacking hosts – CAUTION
- Eradication and recovery

Post Incident Activity

- Lessons Learned
- Using collected incident data
- Evidence retention

Coordination and Information Sharing

- Plan coordination with external parties before incidents occur.
- Consult with the legal department before initiating any coordination efforts.
- Perform incident information sharing throughout the incident response life cycle.
- Attempt to automate as much of the information sharing process as possible.
- Balance the benefits of information sharing with the drawbacks of sharing sensitive

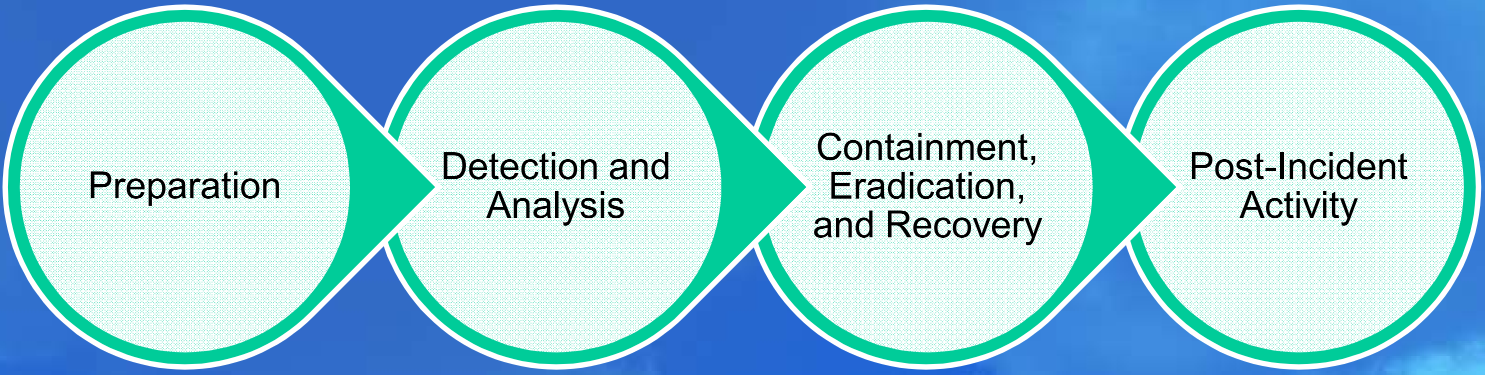
- information.

Coordination and Info. Sharing (con’t)

- Share as much of the appropriate incident information as possible with other organizations.

Scenario 1

On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.



Preparation

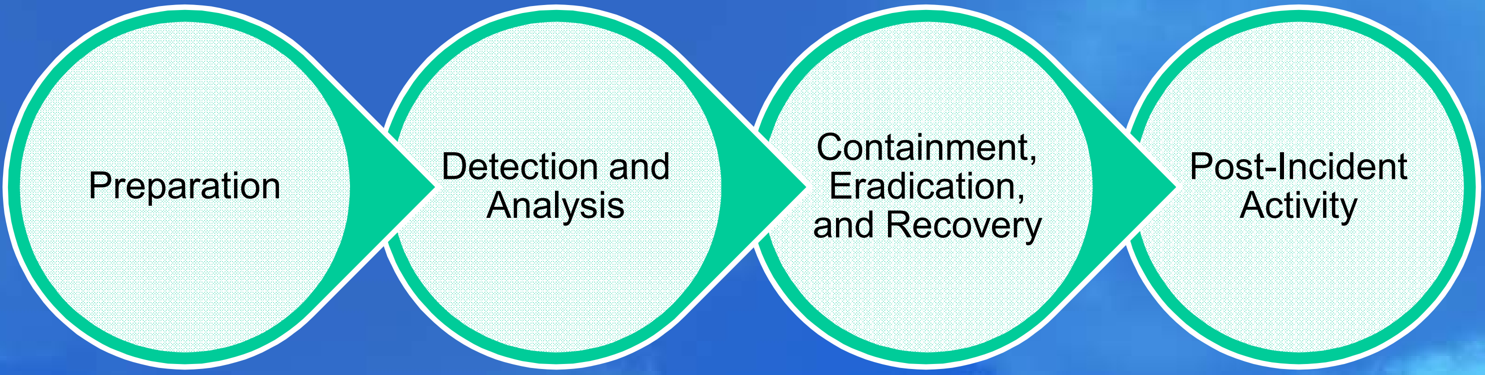
Detection and Analysis

Containment, Eradication, and Recovery

Post-Incident Activity

Scenario 2

On a Sunday night, one of the organization’s network intrusion detection sensors alerts on anomalous outbound network activity involving large file transfers. The intrusion analyst reviews the alerts; it appears that thousands of .RAR files are being copied from an internal host to an external host, and the external host is located in another country. The analyst contacts the incident response team so that it can investigate the activity further. The team is unable to see what the .RAR files hold because their contents are encrypted. Analysis of the internal host containing the .RAR files shows signs of a bot installation.



Preparation

Detection and Analysis

Containment, Eradication, and Recovery

Post-Incident Activity

Thank You!

Contact Info

Angie Singer Keating

CEO

CISA, CIPP, CISM, CRISC

angie@reclamere.com

http://www.linkedin.com/in/angiesingerkeating

Follow me on Twitter @VeepGeek