TRANSPERFECT
LEGAL
SOLUTIONS

Incident Response: Triggers • Steps • Preparation

Welcome!

Threat Environment






APT's
Malware
External Actors
Insider Threats
Negligence/Accident

Normal State

Normal State - Policy

Acceptable Use

Basic Security Features

Provision/De-provision

Data Lifecycle

Baseline & Monitoring

Normal State - Devices

Known State

Operating Within Parameters

Meeting Business Purpose

Help Desk Statistics

Normal State - Servers

Known State

Operating Within Parameters

Meeting Business Purpose

Normal Log Statistics

Standard Performance

Normal State - Network

Known State

Operating Within Parameters

Meeting Business Purpose

Normal Traffic Statistics

Standard Performance

Normal State - People

Help Desk Statistics

Informal Complaint Level

Normal Intelligence Indicators

Trained Staff & User Base

Alert!

Alert! - Policy

Reporting Mechanism

Defined Parameters

Flexible to Threat Landscape

Clear Responsibility

Initial Response Plan

Alert!- Devices

Ambiguous State

Problem Reports

Business Purpose Degraded

Help Desk Statistics

Alert!- Servers

Ambiguous State

Performance Degradation

Operating Profile Changes

Log Indicators Outside Parameters

Alert! - Network

Ambiguous State

Performance Changes

Abnormal Traffic Statistics

Alert!- People

Intelligence Indicators

Help Desk Statistics

Informal Complaints

Outside Information Sources

Respond!

Respond! - Policy

Clear Response Plans

Defined Responsibilities

Clear Outcome Goals

Damage Assessment

Budget/Equipment/Services

Respond!- Devices

Forensic Preservation?

Infection/Attack Vector

Gold Image Reload

Prevent Recurrence

Respond!- Servers

Damage Assessment
Terminate/Prevent
Log Analysis
Infection/Attack Vector
Resume Operations

Respond! - Network

Damage Assessment
Network Log Analysis
Regain Control
Re-Tune Controls & Monitoring

Respond!- People

Communications Plan

Training

Lessons Learned

Disclosures/Reporting

Final Thoughts






Indicators Clear in Retrospect

Prior Planning = Effective Response

Establish Metrics

Clearly Defined Tripwires

Establish Relationships Now!

QUESTIONS?

Andrew Neal

Regional Director, Forensic Technology and Consulting

ANeal@TransPerfect.com

214-436-7999