Incident Response

Richard Starnes, CISSP, MSc,MCSE
Incident Response Team Leader
Richard.Starnes@exodus.net

Martin Pfeilsticker, CISSP
Security Engineer
Martin.Pfeilsticker@exodus.net

Agenda

- **What is CATT ?**
- **What is Incident Response?**

Q & A

Cyber Attack Tiger Team
C.A.T.T.

THE INFRASTRUCTURE FOR THE DIGITAL ECONOMY™

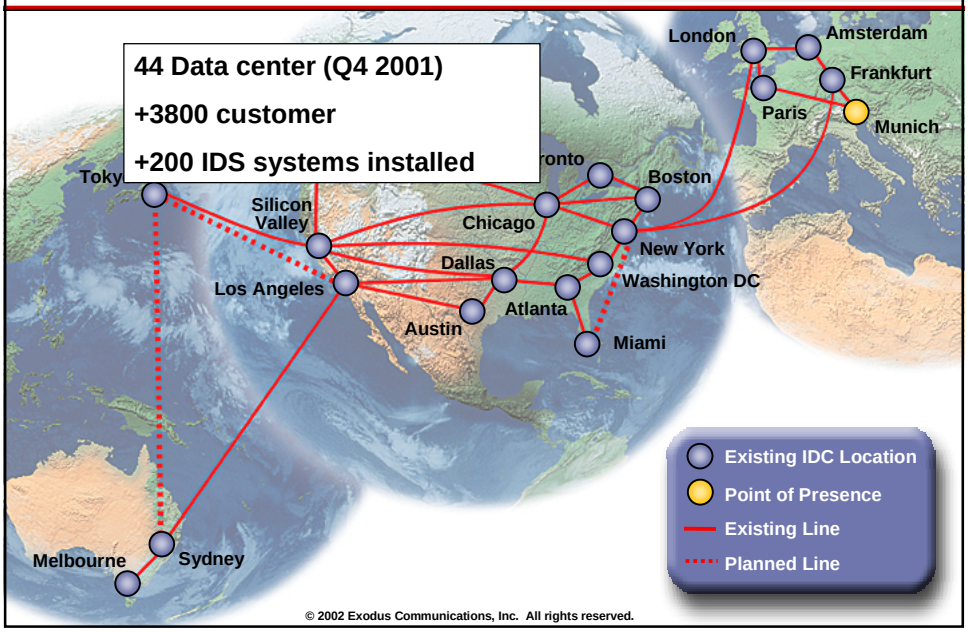
EXODUS®

The Challenge:

44 Data center (Q4 2001)

+3800 customer

+200 IDS systems installed



What does CATT do?

- **Provides various levels of Incident Response (IR)**
- **Triage IR**
- **24/7 On-call IR**
- **Support for Criminal Investigations**
- **CAMS – Intrusion Detection (IDS)**
- **CIMS – Content Integrity Monitoring**
- **Forensic Analysis**
- **Intelligence**

Who and What is CATT?

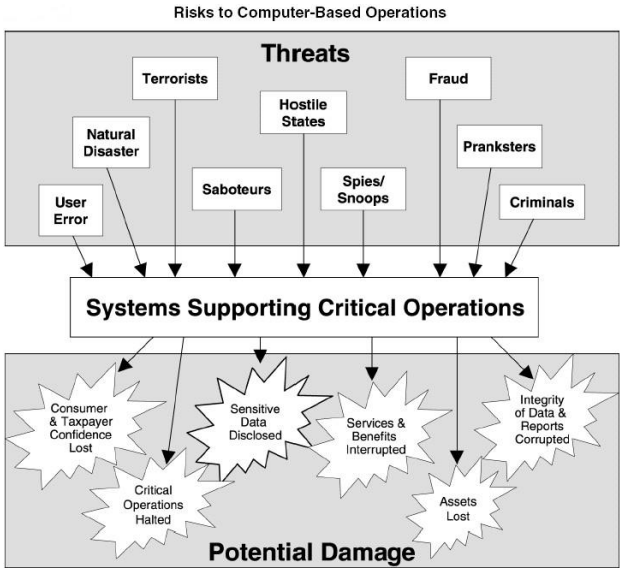
- **The Digital Firemen®**
- **Incident Responders**
  - Former Police/Military (FBI, DCIS, AFOSI)
  - Security Engineers
- **Big Case Experience**
  - Kevin Mitnick
  - Mafiaboy
- **First Undercover Op Undercover hackers**
- **“We don’t hire the ethically challenged.”**

CATT is worldwide: Anywhere, everywhere

- **US**
  - East Cost Team
    - HQ in Washington DC
  - West Coast
    - HQ in Los Angeles
- **EMEA Team**
  - London
  - Frankfurt
- **Asia Pacific**
  - Sidney

Incident Response Fundamentals

Know The Enemy



Who are the Threats?

- **49% insiders**
- **17% remote**
  - More money is lost via internal hacking and exploitation (by a factor of 30 or more)
  - Most of the hacking that is done is from technical personnel in technical positions within the company

- **34% Internet or an external connection**

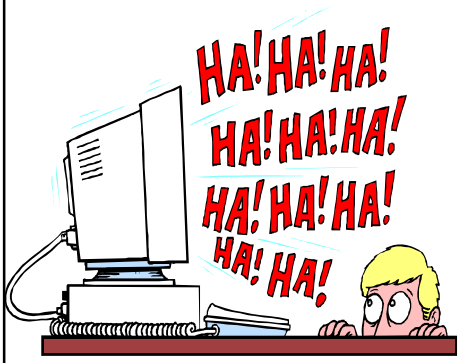
Threat Motivations

- **There are many different motivations to hack**
  - Experimentation and desire to learn
  - “Gang” mentality
  - Psychological needs
  - Misguided trust in other individuals
  - Altruistic reasons
  - Self-gratification
  - Revenge and maliciousness
  - Emotional issues
  - Desire to embarrass the target
  - “Joyriding”
  - “Scorekeeping”
  - Espionage (corporate, governmental)

Extremists and Radicals

- **Political**
  - Sri Lanka Tamil Tigers
  - “Free China”
  - Muslim and Indian Hacker
- **Business**
  - Animal Rights League
- **Statement**
  - “Free Kevin”

What Makes You a Target?



- Good “scorekeeper” site due to your visibility in the world
- Available resources that can be used by the hacker to provide services to other hackers
- Embarrassment factors allow high visibility to other companies and the world
- Target of extremist or activist groups due to corporate or personal focus
- Lax security measures (allows spam relay, web site hosting, etc.)

How Bad Is It?

“If it ain’t hardened, it’s hacked.”

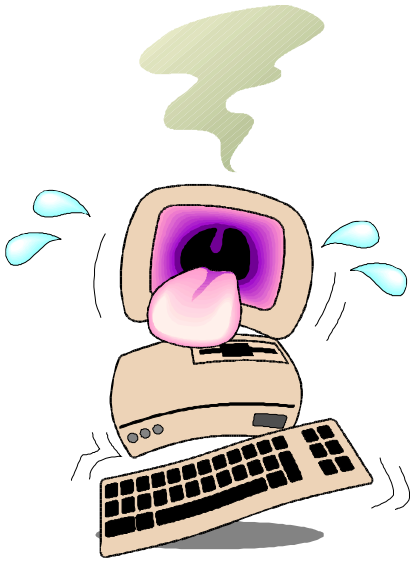
Typical Attacks

- Insider attack
- Social engineering
- Virus infiltration
- Denial of Service
- OS or application bug
- Infiltration via passwords
- Infiltration via “no security”
- Spoofing
- Trojan horse
- Brute force
- Stealth infiltration
- Protocol flaw or exploit

Social Engineering

- The most common type of attack
- Preys upon basic intra-organizational trust
- Advanced technical skills not required

Attack Levels



- **Obvious attacks**
  - Denial of Service
  - Router table attack
  - Common external attacks
  - Unusual activity for specific user accounts that are typically low-use or non-use
  - Bug exploits
- **Not-so-obvious attacks**
  - Aperiodic “network trash”
  - No alarms, but high valid user activities on specific accounts
  - Session hijacking
- **Low-level stealth attacks**
  - Single probes from various source addresses over a long period of time

Security Manager’s Motto: *Be Paranoid*

Terminology

- **Anomaly**
  - Unanticipated or unexpected occurrence

You detect it

- **Incident**
  - anomaly that violates the organization's security policy

You know what is

- **Incident Response**
  - timely marshalling of resources in response to an incident

You know how to handle it

The Three R's of Incident Response

- **REACT**
- **RESPOND**
- **RECOVER**

React, Respond, Recover

- **REACT**
  - *R*eview policy and procedures
  - *E*valuate the situation
  - *A*void panic
  - *C*ollect information
  - *T*ake appropriate action

React, Respond, Recover

- **RESPOND**
  - Request information
  - Evaluate the situation
  - Stop the “attack” and Secure the “crime scene”
  - Preserve evidence
  - Organize forensic examination
  - Note findings
  - Determine cause

React, Respond, Recover

- **RECOVER**
  - Raise security expectations
  - Evaluate current security posture
  - Create implementation plan
  - Order it to be done
  - Validate the implementation
  - Expect the unexpected
  - RECOVER on a regular basis

Incident Response Inputs

- **Security Policy**
- **Security Procedures**
- **Risk Assessment**
- **Logs**

Different Countries, Different Law Enforcement Structures

- **Some countries have a centralized, "federal" cybercrime structure for computer crime enforcement**
- **Some countries have multiple jurisdictions:**
  - Local authorities
  - Regional authorities
  - Federal authorities
- **Some are complex (e.g. U.S.A.)**
  - Local city-based police department cybercrime officials
  - County-based sheriff department cybercrime officials
  - State-level agencies (e.g. Department of Public Safety in Texas)
  - Federal:
    - Child pornography - Customs Service
    - Financial crimes and counterfeiting - Secret Service
    - Computer crime that is conducted over state or international lines: Federal Bureau of Investigation
    - Defense-related: Defense Investigative Service
    - Embassy and State Department: Diplomatic Protection Service

Determining Damage Costs

- **Damage must be expressed in monetary value**
  - Cost of repairing cyber-damage
  - Cost of personnel involved in the cleanup
  - Lost productivity by staff
  - Lost customers due to inability to service their needs
  - Lost product or lack of ability to manufacture

REACT

REACT

- **R**eview policy and procedures
- **E**valuate the situation
- **A**void panic
- **C**ollect information
- **T**ake appropriate action

Review Policies and Procedures

REACT
- *Review policy and procedures*
- *Evaluate the situation*
- *Avoid panic*
- *Collect information*
- *Take appropriate action*

- **Locate IR policies and procedures**
- **Notify Incident Response Team**
  - Internal
  - External
- **Determine applicable actions**

IR Procedures

REACT
- *Review policy and procedures*
- *Evaluate the situation*
- *Avoid panic*
- *Collect information*
- *Take appropriate action*

- **Describe the who, what, when of organization's Incident Response process**
- **Prioritized activities based on organization's goals**
  - Recover and move on
  - Pursue and prosecute
- **Policy and Procedures should "do the thinking for you"**

Security Policy

REACT

- Review policy and procedures
- Evaluate the situation
- Avoid panic
- Collect information
- Take appropriate action

- **Define incident**
- **Identify roles and responsibilities**
- **Formulate a plan of action**

Policies in General

- **Difficult to change**
- **Transcend time and technology**
- **Require management intervention to modify or augment**
- **Not trivial**
- **Short and to the point**
- **Reflect management thought**

A Policy is NOT a Procedure

Procedures in General

- **Easy to change**
- **Specific to technological issues and products**
- **An implementation of policies and management mandates**
- **Do not require a committee to change or implement**
- **Technical in nature**

A Procedure is NOT a Policy

Information Systems Security Policies

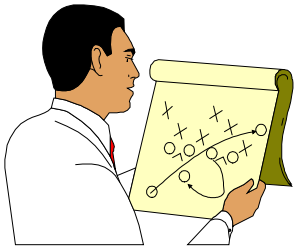
- **Incident Detection**
  - Monitoring, auditing, and logging
    - Use of tools
    - Responsibility
    - Frequency
  - Raising employee awareness
- **Incident Reporting**
  - Who should be notified, and how
    - Business partners
    - Other company sites
    - Vendors
    - Customers
    - Law Enforcement

What if No Policies/Procedures Exist?

- **Notify senior management**
- **Get management support and buy-in**
- **Form an ad hoc IRT**
  - Director (required)
  - Lead investigator (required)
  - Other
- **Follow REACT/RESPOND/RECOVER process**

Evaluate the Situation

REACT
- *R*eview policy and procedures
- *E*valuate the situation
- *A*void panic
- *C*ollect information
- *T*ake appropriate action



- **What is the urgency of the situation?**
- **How critical are the affected systems?**
- **What is the supporting evidence?**
  - Rule out:
    - Improper configuration
    - Bad assumptions
    - Operator error
  - Examine recent changes to site's configuration
  - Talk to systems administrators
- **Determine if continued operation is possible and/or required?**

Avoid Panic

REACT
- *R*eview policy and procedures
- *E*valuate the situation
- *A*void panic
- *C*ollect information
- *T*ake appropriate action

- **Evaluate calmly and objectively**
- **Don't**
  - Trash the "crime scene"
  - Log in and poke around
  - Run probes to determine if site is vulnerable to particular attacks
  - Halt systems via an unapproved or abnormal procedure
  - Engage the attacker
  - Probe involved networks

Collect Information

REACT
- *R*eview policy and procedures
- *E*valuate the situation
- *A*void panic
- *C*ollect information
- *T*ake appropriate action

- **Preserve crime scene**
- **Gather configuration details**
- **Collect information without modifying the target system**
  - Host names and addresses
  - Machine and OS types
  - Backup servers
  - Network topology diagram

Practice Good Operations Security

- **Maintain "need to know"**
  - Attacker may be among you
  - Attacker may monitor you
    - Flurry of email or other in-band communication
    - Buzz in the air
    - Change established daily routines

"Loose lips sink ships"

Safeguard Evidence

- **Log Book**
  - Date and Time
  - Hostname, IP address, machine & OS type
  - System administrators and user names
  - Interviewees
  - Observations
  - Actions taken
  - Assumptions
- **Establish and maintain Chains of Custody**
  - Verifiable
  - Witness

Record Keeping: Before and After

- **Keep accurate and detailed records of before and after events**
- **Records are critical in a real investigation where incident causes damage or loss**

Chain of Custody

- **Lead Investigator**
  - Evidence Handler
    - Engineer's notebook and ink
    - Evidence labels and transmittals
    - Digital signatures and checksums
    - Two Person Integrity

Take Appropriate Action

REACT
- *R*eview policy and procedures
- *E*valuate the situation
- *A*void panic
- *C*ollect information
- *T*ake appropriate action

- **Determine appropriate response**
  - Protect, rebuild, and proceed
  - Pursue and prosecute
    - Get subject matter expertise
    - Get legal advice
- **Estimate level of effort**
  - External support required?
    - System administrators
    - Network engineer
    - Security expertise
    - Investigators

Consider Legal Ramifications

- **Employee/Customer rights**
  - Consent forms
  - Warning banners
- **State and Federal Laws**
  - Data Protection Act
    - Monitoring requires one of following conditions:
      - Court order
      - Regular course of business
      - Consent
    - System warning banner required for monitoring

EXODUS

Will the Law Help?

- Severity of the crime
- "Harm factor" to the individual, company or general public
- Statutory language
- What, politically, is attractive to prosecution efforts
- Amount of financial loss
- Manpower constraints imposed on law enforcement and legal prosecution groups
- "Victim's" dedication

EXODUS

Getting The Law Interested

- Have to show definitive law violation and damages
- Need to have information well organized and intelligible
- Most law enforcement organizations do not have many (if any) computer crime experts
- Most attorneys have very little cyberlaw expertise and background

RESPOND

EXODUS®

RESPOND

- ***R*equest information**
- ***E*valuate the situation**
- ***S*top the “attack” and *S*ecure the “crime scene”**
- ***P*reserve evidence**
- ***O*rganize forensic examination**
- ***N*ote findings**
- ***D*etermine causes**

Request Information

RESPOND

- *Request information*
- *Evaluate the situation*
- *Stop the attack and Secure the crime scene*
- *Preserve evidence*
- *Organize forensic examination*
- *Note findings*
- *Determine causes*

- **Talk to users and system administrators**
- **Review the evidence**
  - Many types of logs
    - **IDS**
    - **Firewall**
    - **Router**
    - **WWW**
    - **RADIUS**
    - **Email**
    - **Workstation**
    - **Databases**
  - Email messages
  - Etc.
- **Determine where attack originated**
  - Internal
  - External

Evaluate the Situation

RESPOND

- *Request information*
- *Evaluate the situation*
- *Stop the attack and Secure the crime scene*
- *Preserve evidence*
- *Organize forensic examination*
- *Note findings*
- *Determine causes*

- **Determine the source of the problem**
- **Estimate required level of effort**
- **Identify need for subject matter experts**
- **Create initial plan of action**

Determining the Problem

Passive techniques

- Interviews
- Monitoring
  - Network traffic
  - Host activity
  - Video surveillance
- Phone records
- Timecards
- Building entry/exit logs
- Honey pot

Active techniques

- Scan network/host for known vulnerabilities
- Retrieve log files and other critical data
- Contact ISPs
- Engage suspected attacker

Stop the "Attack"

RESPOND

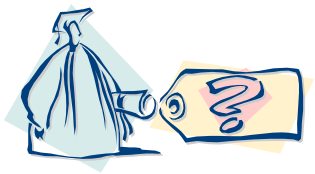
- *R*equest information
- *E*valuate the situation
- Stop the attack and *S*ecure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes

- **Immediate actions**
  - Power down
  - Modify firewall/router rules
  - Change network address
  - Increase bandwidth
  - Apply system patches
- **Long term actions**
  - Identify and eliminate root causes
    - Hardware
    - Software
    - Configuration
  - Configuration errors
    - Network/host
  - Locate attacker
  - Update operational procedures

Secure Crime Scene

RESPOND

- *R*equest information
- *E*valuate the situation
- Stop the attack and Secure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes



- **Enforce equivalent of yellow police tape**
- **Tag and seal *ALL* evidence taken into custody**
  - Date and time
  - Unique evidence number
  - Item name
  - Description of suspected contents
  - Signature of technician
  - Signature of witness (if available)
  - Location obtained

Secure the "Crime Scene"

RESPOND

- *R*equest information
- *E*valuate the situation
- Stop the attack and Secure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes

- **Coordinate with knowledgeable "trusted" technical contact**
- **Emergency Kits**
  - Important contact information
  - Forensics tools (software, hardware)
  - Notebook and pen

Preserve Evidence

RESPOND

- *R*equest information
- *E*valuate the situation
- *S*top the attack and *S*ecure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes

- **Goal**
  - Collect all relevant evidence
- **Objectives**
  - Preserve the scene
  - Preserve data integrity
  - Preserve legal integrity
  - Establish a chain of custody

The criminal always takes something from the scene and always leaves something behind.

Evidence Preservation Issues

RESPOND

- *R*equest information
- *E*valuate the situation
- *S*top the attack and *S*ecure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes

- **Diligence & Patience vs. Speed & Accuracy**
- **Dangers**
  - Destruction or modification of evidence
  - False evidence creation

Evidence Types

RESPOND

- *R*equest information
- *E*valuate the situation
- Stop the attack and *S*ecure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes

- **Volatile**
  - Memory
    - RAM
    - Witnesses
  - Active Processes
  - Active network connections
  - Screen contents
- **Non-Volatile**
  - Physical equipment
  - Tapes, hard drives, floppies
  - Printouts
  - Recorded video surveillance

Note Findings, Determine Causes

RESPOND

- *R*equest information
- *E*valuate the situation
- Stop the attack and *S*ecure the crime scene
- *P*reserve evidence
- *O*rganize forensic examination
- *N*ote findings
- *D*etermine causes

- **Analysis**
- **Incident Report**
  - Systems/networks affected
  - How compromise occurred
  - Other sites affected
  - Impact to operations
- **Brief management**

RECOVER

RECOVER

- **Raise security expectations**
- **Evaluate current security posture**
- **Create implementation plan**
- **Order it to be done**
- **Validate the implementation**
- **Expect the unexpected**
- **RECOVER on a regular basis**

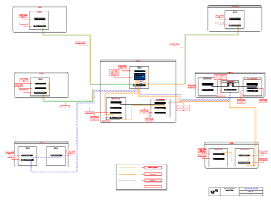
Raise Security Expectations

RECOVER
- Raise security expectations
- Evaluate current security posture
- Create implementation plan
- Order it to be done
- Validate the implementation
- Expect the unexpected
- RECOVER on a regular basis

- **It's not good enough to say "we need security"**
  - Resource commitment
  - Management support
- **Security budgeting**
  - Security tools and patches
  - Training classes and resources
  - 3rd party consulting
    - Tiger teams
    - Security auditors
  - Long term staffing requirements

Evaluate Current Security Posture

RECOVER
- Raise security expectations
- Evaluate current security posture
- Create implementation plan
- Order it to be done
- Validate the implementation
- Expect the unexpected
- RECOVER on a regular basis

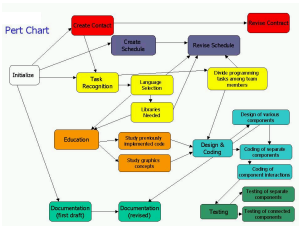


- **Determine and document current configuration**
- **Conduct risk assessment**
  - Threats
  - Vulnerabilities
  - Impacts

Nessus

Create Implementation Plan

RECOVER
- Raise security expectations
- Evaluate current security posture
- Create implementation plan
- Order it to be done
- Validate the implementation
- Expect the unexpected
- RECOVER on a regular basis



- **Revise policy and procedures**
  - Address corporate goals
  - Define acceptable use
- **Areas of concentration**
  - Deficiencies that occurred during this response
  - Baselining
  - Basic system installation and configuration
  - Security configuration
  - Backups
  - Security audits
  - Incident response

Create Implementation Plan

- **Reload system from trusted media**
  - Why can't we just fix the problem?
  - Why can't we user our last backup?
- **Apply known approved patches**
  - Unverified patches may introduce new vulnerabilities

Create Implementation Plan

- **Tighten system/network configurations**
  - Per host service matrix
  - Per host protocol matrix
  - Enable auditing
  - Boundary controls
  - Disable unused and unnecessary accounts
  - Enforce strict password controls

Create Implementation Plan

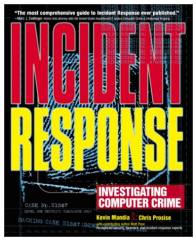
- **Baseline it**
  - Disk image
  - Backups
  - Create a system profile
- **Consider installing intrusion detection sensors and network monitors**
  - Do you have someone who has the responsibility of reviewing audit logs?

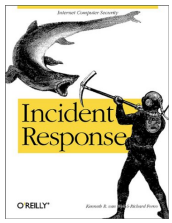
Order and Validate Implementation

RECOVER
- Raise security expectations
- Evaluate current security posture
- Create implementation plan
- Order it to be done
- Validate the implementation
- Expect the unexpected
- RECOVER on a regular basis

- **Require regularly scheduled status reports**
- **Hold individuals accountable for doing their job**
- **Employ 3rd party security audits**
  - Independent verification tool
  - Audits
  - Regular scanning
  - Penetration testing

Recommended Reading





- **"Incident Response"**
  - Kevin Mandia & Chris Prosise
  - Osborne/McGraw Hill
  - 0-07-213182-9
- **"Incident Response"**
  - Kenneth R. Van Wyk & Richard Forno
  - O'Reilly & Associates
  - 0-596-00130-4
- **SANS website**
  - www.sans.org/infosecFAQ/incident/incident_list.htm
- **"Intranet Security"**
  - @@@

Questions?

Martin Pfeilsticker
Security Engineer
CATT EMEA
Martin.Pfeilsticker@exodus.net

+49 69 38777 227 (office)
+49 173 7066139 (cell phone)