

# ISACA Vancouver Chapter

## Trends and Hot Topics in Forensics\*

May 6, 2008

James Crooks CISA, CISSP, GCFA, GCIH, ISP



\*connectedthinking

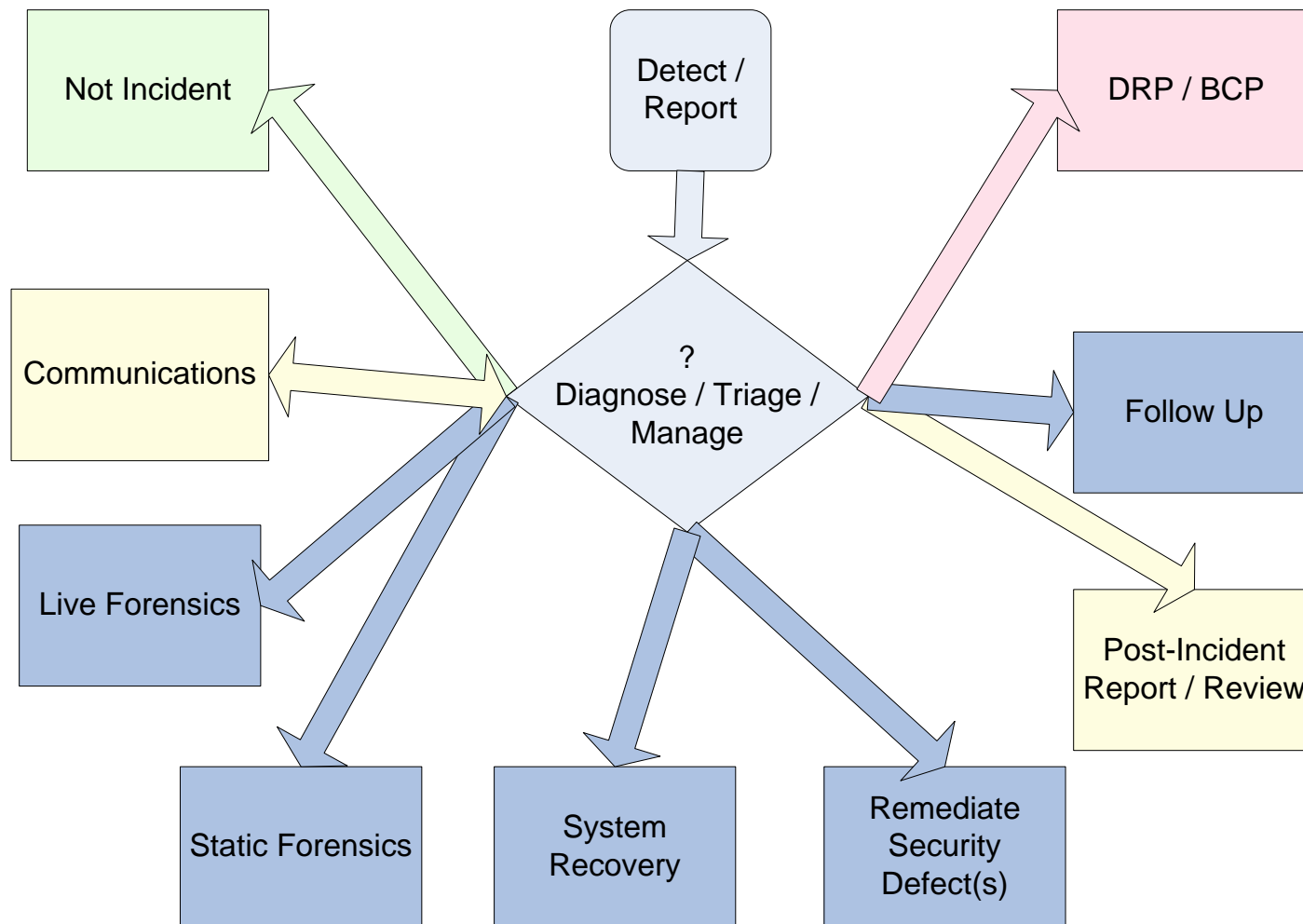
PRICEWATERHOUSECOOPERS 

# Outline



- Incident Flow and Universe
- Incident Response Steps
- Technical Responses
- Non-Technical Responses
- Basic Forensics
- Forensic Targets
- Advanced Forensics
- Live Forensics
- Firewire Tricks
- Anti-Forensics
- Forensic Training

# Incident Flow and Universe



# Incident Response Steps



- Pre-incident preparation
- Detection of incidents
- Initial response / Triage
- Response strategy selection + procedure customization
- Forensic collection and investigation
- Recovery and security measure enhancement
- Reporting
- Follow-up

# Technical Responses



- Pre-Incident Preparation (toolkit)
- Initial Response / Triage / Verify Incident
- Live Forensics
- Forensic Data Collection
- Disaster Recovery and Business Continuity
- Recovery and Remediation
- Follow-Up

# Non-Technical Responses

- Strategy / Response Selection
- Communications
- Reporting



# Basic Forensics



- Static Forensic Imaging (not your usual backup)
- Validation (cryptographic checksums)
- Documentation and chain of custody
- Collect and correlate external logs (firewalls, IDS, etc.)
- Analysis of collected data
- Collect evidence and notes in case file

# Forensic Targets

- Allocated files
- File change timeline
- Deleted files (in recycle bin or unallocated space)
- Browser history
- Cookies
- Browser cache
- Temporary files
- Data in slack space



# Advanced Forensics



- Live forensics to capture volatile data
- Firewire memory tricks
- Icy RAM: chilled chips retain data with power off
- Portable devices (everything has memory: PDAs, phones, MP3 players, cameras, flash memory, cars)
- Forensics in Virtual Systems
- Massive data stores: SAN etc.

# Live Forensics for Volatile Data



- Network state
- Process state
- Memory
- Disk arrays
- Disk imaging on unstopppable system
- Firewire memory access

# Firewire Tricks



- Memory capture
  - No logon needed
  - No keyboard or mouse
  - No privilege issues
- Collect BIOS password on some systems
- Process info
- Can read AND write memory
- Make registry entries
- Remove XP SP2 keyboard lock password

# Anti-Forensics

- Hidden directories
- Hidden partitions
- Full disk encryption
- EFS and directory encryption
- Vista bit locker
- Sanitization tools and techniques (including cipher /w)
- Disk defragment

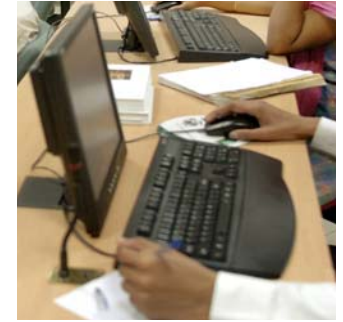


# Questions?



# Thank you.

# Some Related PwC Services



Fraud Investigation

Forensic Accounting

Fraud Risk Management

Computer Forensics

Electronic Discovery

Intelligence Screening

Money Laundering Investigation

Incident Response Consulting

Incident Response Support

DRP/BCP Consulting

Vulnerability Scans

Penetration Testing

Compliance Assessments

IT Advisory

Advisory Services Web Site:

<http://www.pwc.com/extweb/service.nsf/docid/757F3D926EF5CCA9852570CA00176FCE>