

Corporate Incident Response: Wait! I should have written that down!

16th Annual New York State Cyber Security Conference

Jeffrey Isherwood

Exelis Inc.

Senior Security Analyst, Trainer
& Vulnerability Mgmt. Specialist
CISSP, C|EH, CRISC, LINUX+, NCLA, LPIC 1
I-Safe Internet Safety Trainer

Overview

- The Goal of Incident Response (IR)
 - > Law Enforcement vs. Corporate IT
- IR Methodology
 - > Law Enforcement
 - > Corporate IT
- Gaps in Corporate IR
- Why do the Gaps Matter?
- Developing Solutions

The Goal of Law Enforcement

- In General
 - > Prevent the occurrence of a crime that in some way damages another human being, group, agency or society as a whole.
 - > Ensure suspected criminals are tried in a manner that is in compliance with the applicable laws.
- Incident Response
 - > Preserve safety and prevent loss of life.
 - > Properly identify the perpetrators and build a prosecutable case.



The Goal of Corporate IT

- In General
 - > Ensure the smooth operation of IT assets, data and infrastructure.
 - > Enable the organization to perform its mission/business in accordance with policy.

- Incident Response
 - > Preserve security of IT assets, data and infrastructure.
 - > Prevent loss or compromise of organizational data.
 - > Maintain continuity of operations.
 - > Identify the source of the incident to prevent future losses from occurring.



The Differences in IR?

Law Enforcement

- Primarily concerned with:
 - > Detection
 - > Containment
 - > Recovery
 - > Prosecution
 - Investigate, Log, Certify
 - Maintain chain of custody

Corporate IT

- Primarily concerned with:
 - > Detection
 - > Containment
 - > Recovery
 - > Prevention
 - Identify the gaps
 - Remediate attack vectors

The Challenge



Law Enforcement Methodology



- Forensically sound investigations
 - > Trained investigators
 - > Documented procedures
 - > Time stamps
 - > Hashes
 - > Activity logging
 - > Chain of custody
 - > Secure evidence storage
 - > Timeline analysis
- Toolkits
 - > Documented in court
 - > Rigorously tested
 - > Automatic hashing
 - > Automatic activity logs
 - > Secure evidence storage
 - > Occasionally
 - Restricted
 - Require special training

Corporate Methodology

- 
- Toolkits
 - > Free or low cost Tools
 - Open Source
 - Command line tools
 - Operating System dependent
 - > Menagerie of methods
 - > Haphazard logging (at best)
 - > Manual hashing (maybe)
 - > Insecure evidence storage
 - Ad-Hoc investigations
 - > Local IT Support Staff
 - First on scene IR
 - > Lacking in policy
 - > Not trained in IR
 - > Lack of timelines
 - > Lack of activity log

Bad Elements have the upper hand...

Criminals have the “advantage”

- Sophisticated technological skills and/or equipment
- Distance
- Time
- Practiced tactics
- Lawlessness
- Anonymity
- Information sharing



There's No Need to Fear! The IT Staff is here...

IT Staff is often the first responder due to end user calls to the help desk

- It starts as a trouble ticket, turns out to be an incident!
- IT staff not trained to protect the crime scene



Gaps in Corporate IR

IT Staff have many functions prior to discovering an incident

- They try to restore continuity and please the user
- Use tools they are familiar with
- Get called away by customers
- Often muddy the evidence
 - > Difficult to prosecute
 - > OS Dependent tools
 - > “Poking around”
 - > **Poor to zero logging of actions**



Corporate IR Policy

Corporate IR Policy doesn't generally include prosecution

- Public Relations
- Liability
- Stock Prices
- Corporate Intelligence



Why Should Corporations Want to Prosecute?

- Corporations are traditionally risk averse when it comes to IT Data Breaches
- They may not understand the risks that come with not reporting
 - Regulatory and Compliance issues
 - Business Continuity
 - Liability
 - Brand Protection

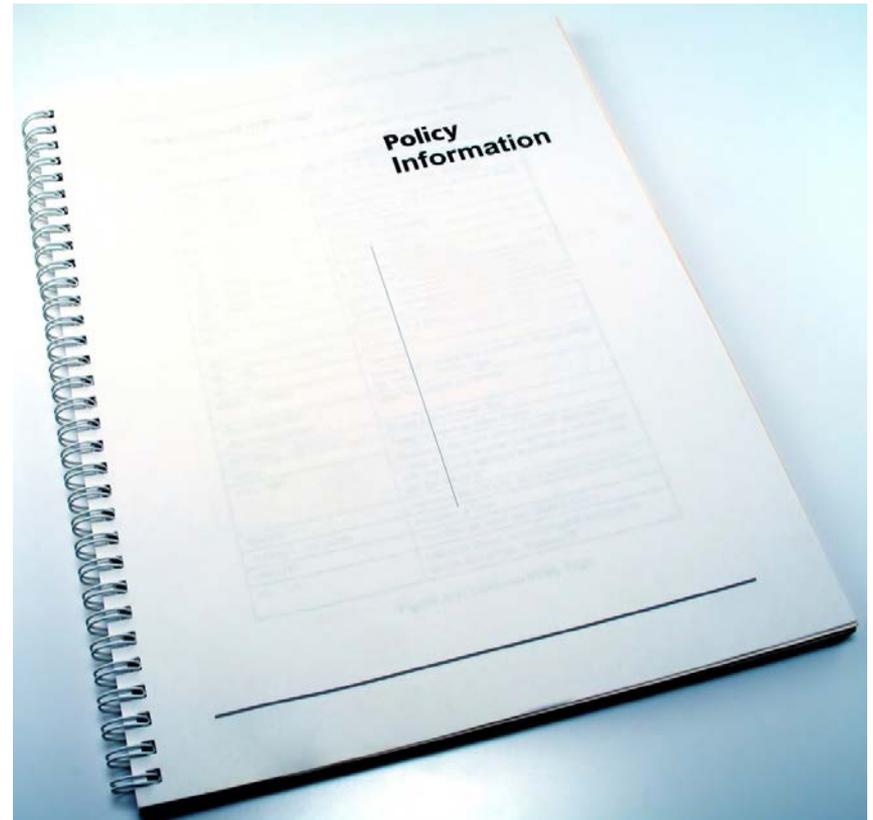
Cybercrime Concerns for Law Enforcement

- Jurisdictional Issues
 - > International Cooperation
 - > Across Borders
- Digital Forensics
 - > The “SODDI” Defense
 - > Presenting Digital Evidence
- Charging the Case correctly
 - > Nature of the evidence
 - > Type of case



Cybercrime Concerns for Corporate IT

- Identifying an Incident
 - > Policy, Procedures, Training
- Capturing an incident
 - > Accurate logging
 - > Preserving digital evidence
- Recovering
 - > Identify the gaps
 - > Remediate attack vectors
 - > Report to Law Enforcement



Current Standard Corporate IT Tools Are Lacking

Open Source & Free Tools:

- > Generally windows based
- > Network useable tools are command line based
- > Collection of scripts that use other tools

Problems:

- > Create multiple outputs
 - o Not always compatible
- > **No logging**
- > No Timelines
- > No hashing
- > No Chain of Custody
- > No investigator attribution



Why do the Gaps Matter?

Are you the predator or the prey?

- Lack of reporting and prosecution:
 - > Emboldens criminals and intruders
 - > Sends a message that they may trespass with impunity
 - > Encourages them to continue or escalate their activity
 - > Does not help stop them from attacking other organizations



DON'T be the prey!

Developing Solutions

- Becoming the hunter:
 - > IT Staff need to be trained
 - > Tools need to be standardized
 - Automatic hashing
 - Automatic activity logs
 - Secure evidence storage
 - > Improve policy
 - > Get involved with information sharing
 - FBI's Infragard
 - US Secret Service Electronic Crime Task Forces (USSS ECTF)
 - Defense Industrial Base (DIB)
 - > Corporate buy-in for prosecution & reporting



Cyber Security Programs

Questions?



www.exelisinc.com