# Best Practices, Conclusion…

# **BEFORE** an Incident (1/2)

- Have a good security policy
- Learn thy system(s)
- Turn on logging & accounting
- Create a Baseline
- Regularly audit your systems

# **BEFORE**… (2/2)

- Learn how miscreants abuse systems
- At least know how to gather forensic data
- Backups
- Know your neighbors
- Know who to contact in emergency

# Security Policy

- The most important thing
- Well documented, consistent systems
- Keep up to date with security patches, tools, and education

# The Coroner's Toolkit

- Barebones
- UNIX
- Simple freezing routines
- MACtime, unrm/laz, icat/pcat, timeline tools, etc.
- Precursor to Time Machine?

*http://www.fish.com/security/forensics.html*

# Abuse

- With knowledge comes responsibility
- Spying & abuse are easier than ever
- Arms race