Steps

- Define the Attacks
- Model the Threats
- Develop an Incident Response Plan
- Develop Education Plans
- Enterprise Solutions
Process Definition

1. Define terms
2. Define and refine attack trees
   - Enough detail?
     - No: Go to step 1
     - Yes: Proceed to next step
3. Analyze attacks
4. Identify weaknesses
**ID Theft Lifecycle**

**Planning**
- Target a firm
- Target a victim
- Target credentials
- Decide method
- Fraud objective
- Criminal collaboration
- Research/probing networks

**Setup**
- Create materials
- Setup destinations
- Obtain contact info
- Setup attack machinery
- Install physical traps/loggers

**Attack**
- Vector website
- Vector eMail
- Vector IM
- Vector news, chatroom, blog
- Vector bulletin board
- Vector wireless technology
- Vector P2P or games
- Vector insider
- Vector malware
- Vector backup media
- Dumpster diving
- Physical theft
- Shoulder surfing

**Collection**
- Web response
- eMail response
- IM response
- Gather malware data
- Read discarded disk/tape data
- Gather vectored data

**Fraud**
- True name fraud
- Account compromise
- Criminal fraud
- Credential trafficking
- Credentials used in 2nd stage attack
- Money laundering
- False registrations
- Pump and dump schemes

**Post Attack**
- Shutdown attack machinery
- Destroy evidence
- Qualify compromised accounts
- Assess effectiveness
- Launder proceeds
- Share/sell techniques or information
Threat Model

- Threats:
  - Social Engineering
  - Spoofing/Phishing
  - Keystroke logging
  - Trusted Insiders
  - Family Members
  - Stolen Hardware/Backups
  - Shoulder Surfing
  - Lost or Stolen IDs
  - Dumpster Diving
  - Network Sniffing
  - Wireless Penetration
  - Hacking
  - Pharming
  - Bogus Job Postings

- Financial Exposure
- Likelihood of Success

Size of the bubble = Perceived Threat
Establish Communication Channels

- Executive steering committee
  - Awareness
  - Issue resolution
  - Change agent
- Governance team
  - Articulation of objectives
  - Strategy
  - Coordination and oversight
- Working groups (permanent)
  - Day-to-day operation
  - Escalation and resolution of issues
  - Monitoring and improvement
- Task forces (temporary)
  - Selecting new tools
  - Process reengineering and documentation
Incident Response Plan

- Incident Response Flow
- Response Roles and Responsibilities
- Incident Communication
- Incident Contact Tree
- Incident Contact List
  - Names
  - Numbers
- Plan for *post mortem* after each incident
- Plan Testing and Update Cycles
Education

- Raise awareness among
  - Customers
  - Employees
- Avoid causing undue sense of fear or alarm
- Create a program of partnership
- Employees that are well-educated on ID Theft:
  - can respond to customer inquiries
  - can protect themselves online
- The best educational tool is the Web
Enterprise Solutions

- Mutual authentication
- Multi-factor authentication
- Increased log and infrastructure monitoring
- Participation in industry consortia
- Participation in standards bodies
- Develop threat intelligence sources
  - Commercial companies
  - Law enforcement
  - Peer companies
- Explore Open Standard solutions