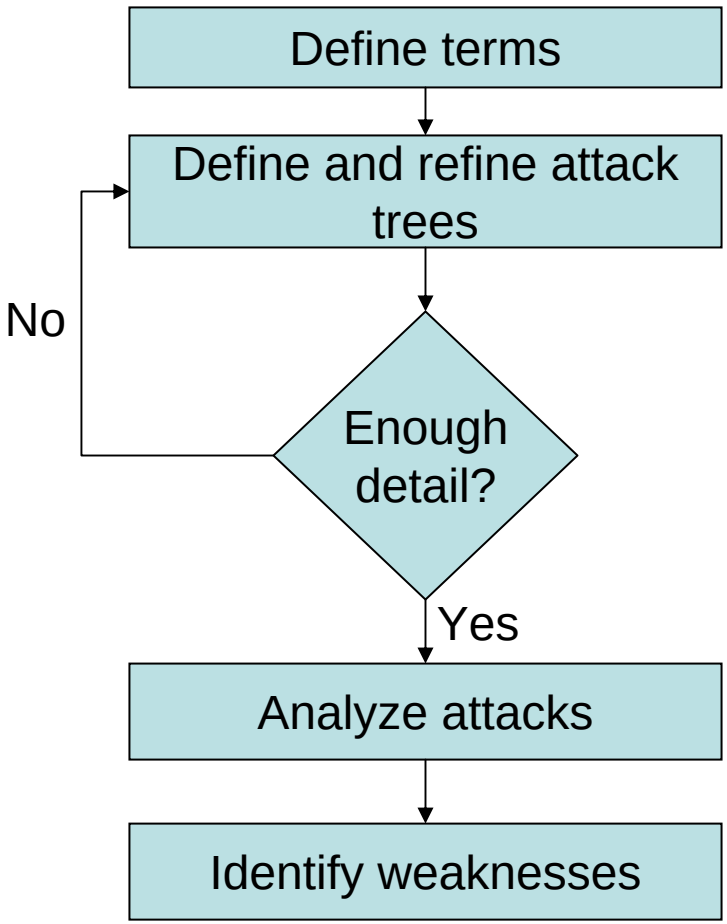
Paul Biciunas
Security Architect
Fidelity Investments
paul.biciunas@fmr.com

Steps

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

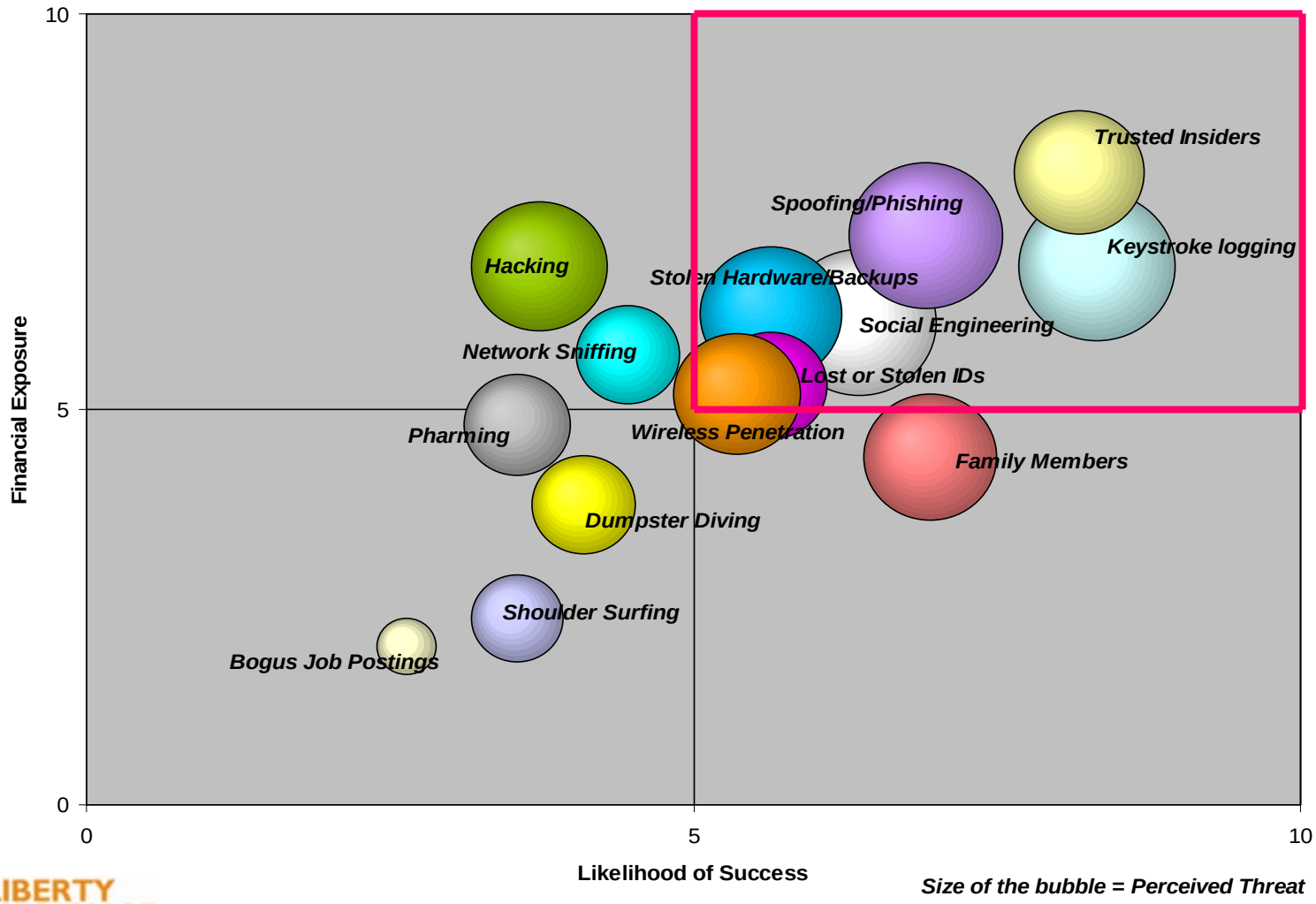
Process Definition



ID Theft Lifecycle

Planning	Setup	Attack	Collection	Fraud	Post Attack
▪ Target a firm ▪ Target a victim ▪ Target credentials ▪ Decide method ▪ Fraud objective ▪ Criminal collaboration ▪ Research/probing networks	▪ Create materials ▪ Setup destinations ▪ Obtain contact Info ▪ Setup attack machinery ▪ Install physical traps/loggers	▪ 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	▪ Web response ▪ eMail response ▪ IM response ▪ Gather malware data ▪ Read discarded disk/tape data ▪ Gather vectored data	▪ True name fraud ▪ Account compromise ▪ Criminal fraud ▪ Credential trafficking ▪ Credentials used in 2nd stage attack ▪ Money laundering ▪ False registrations ▪ Pump and dump schemes	▪ Shutdown attack machinery ▪ Destroy evidence ▪ Qualify compromised accounts ▪ Assess effectiveness ▪ Launder proceeds ▪ Share/sell techniques or information

Threat Model



LIBERTY ALLIANCE PROJECT

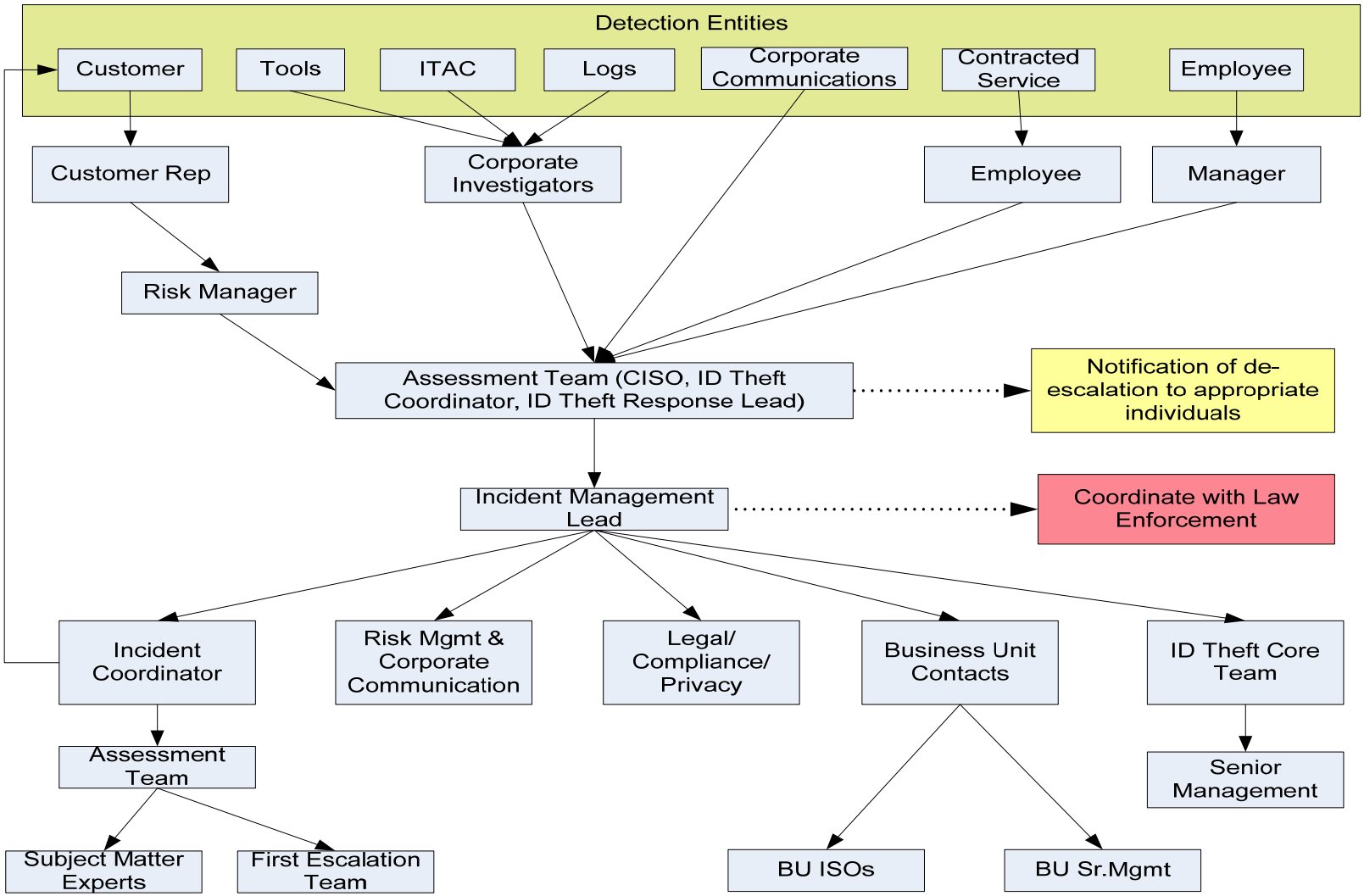
Establish Communication Channels

- 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

Incident Contact Tree



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