Who, What, Where,and How:
An Insider's View of the Internet Security Community

John Kristoff

DePaul University (ops role)
University of Illinois at Chicago (research role)

jtk@depaul.edu

The Players

- Network engineers
- Sysadmins
- Security incident response teams (IRTs)
- Software developers
- Software, Hardware, and Service vendors
- Government and law enforcement
- Journalists
- Researchers
- Miscreants

The FIRST.org community

- One of the earliest, longest running, best known
- IRT constituency focused, not individuals
- Broad international reach and participation
- Well organized, successful in-person events
- Professional organization, infrastructure
- Membership fee and sponsorship supported
- first-teams@ list explodes to first-team@ aliases
  - In hindsight, a very serious shortcoming
- Technical content is a mixed bag

The nsp-security community

- ISP/NSP network-backbone event coordination
- Vetted individuals, limited to two per ISP/NSP
  - Rules are made to be broken
- NANOG security track loosely arose from here
- Most work coordinated through a mailing list
- Early 2000's this was "the" place to be
  - Much early opsec history happened here
- Bit of a "boys club", some feuds and infighting
- Many modern day communities evolved from here

The ops-trust community

- Envisioned to be nsp-security++
  - Eliminate NSP and two-member restrictions
  - Maintain or enhance strong vetting model
- Evolved into a collection of “trust groups”
- Mostly still mailing lists
- Lots of trust groups, only a few useful
- Some good portal/list tech potential arose
- Success diluted by mismanagement

REN-ISAC community

- Higher education and R&E environments
- Cost-recovery based and run by IU.edu
- Lists, feeds, meetings, other services provided
- Except for grandfathered institutions, 5 eyes only
- Very successful comparatively speaking
- Rebelling to IU “stewardship” comes and goes

Recurring controversies

- Tussle: trust, group size, secrecy, newcomers
- Centralized list archives aka discovery boogey man
- Vetting graph maintenance
- Membership refutation
- Personality conflicts
- Kings, queens, and key holders