Sharing Sensitive Information without Compromising Data

Peter Allor

Director of Intelligence,

Special Assistant to the CEO

Director of Operations, IT-ISAC

June 28, 2006

INTERNET | SECURITY | SYSTEMS®

- **Title: Sharing Sensitive Information without Compromising Data**
- **The Federal government is working to create a central repository of raw, but useful data collected from RFIs, RFPs, line of business research and the public sector. Unlike information, which is the final result of analysis of un-attributed data, raw data often lacks context, is specific, and often is identifiable to the sender and recipient. Should this collection of data be illegally accessed, used for unauthorized purposes, comprised or even destroyed, the affects would be far reaching. Pete Allor, director of security intelligence for Internet Security Systems, will discuss how to create "data centers of excellence" that employ best practices for cyber security and information assurance, enabling organizations to share the same data without the political and technical hurdles of ownership.**

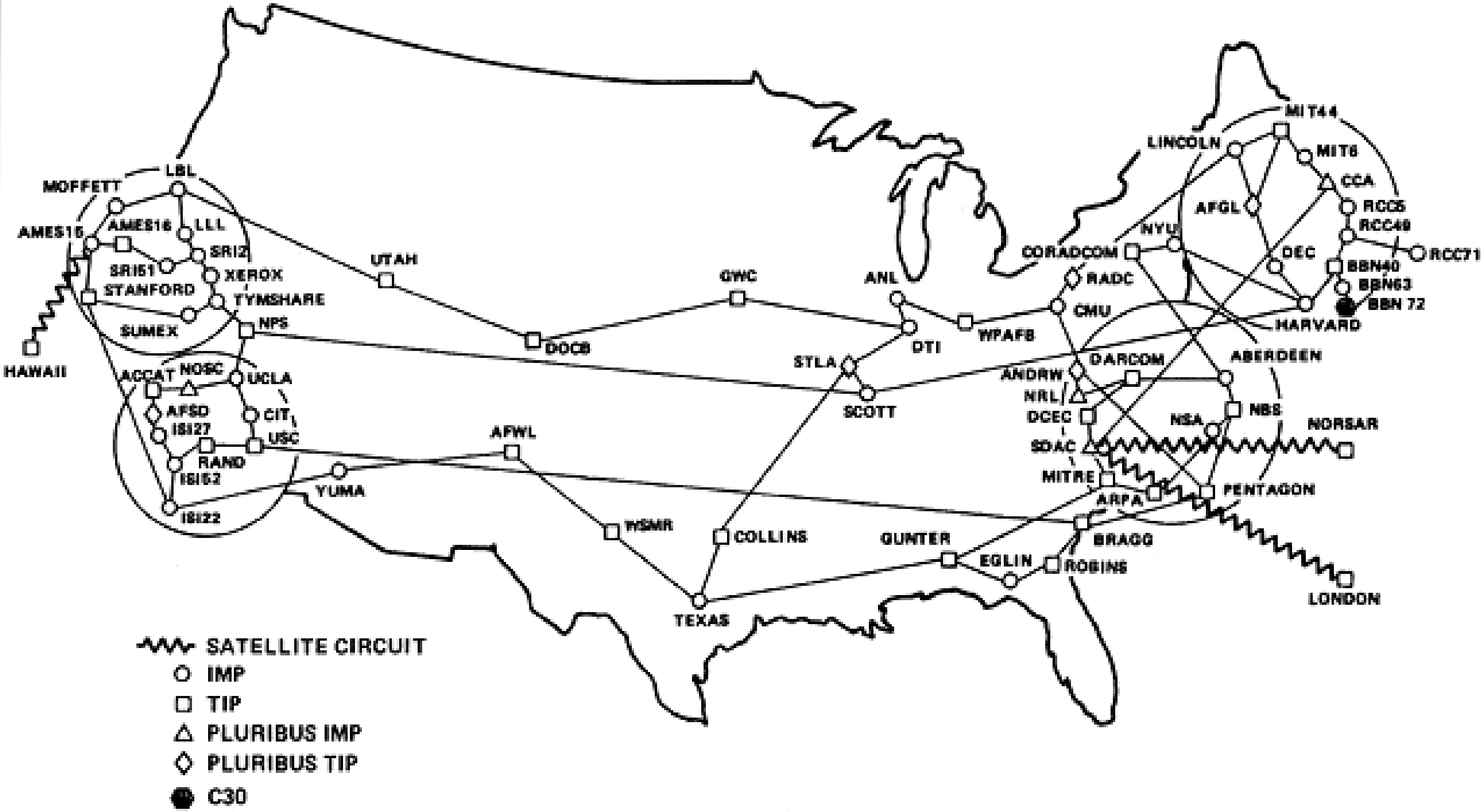
Agenda

- Who is working together
- Why it’s not working
- How it could
- Vision for next generation of sharing

INTERNET | SECURITY | SYSTEMS®

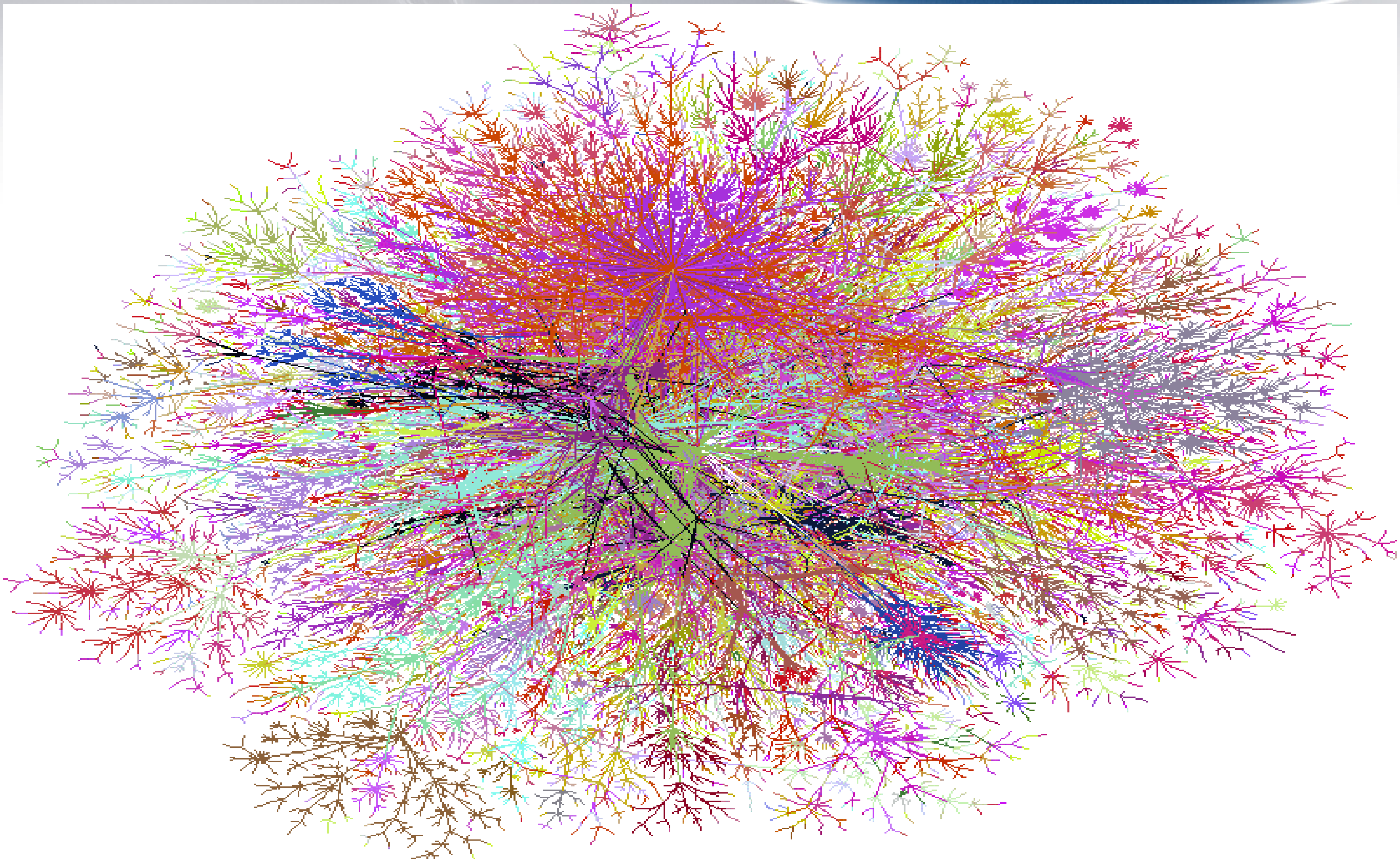
The “Good Ole’ Days”

ARPANET GEOGRAPHIC MAP, OCTOBER 1980



(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

The “New Net”



Information Sharing – same word, different meaning

- Congress
- Intelligence Community
- Department of Homeland Security
- State and Local Law Enforcement
- The Press
- Industry
- Your Enterprise / Agency

INTERNET | SECURITY | SYSTEMS®

Information Sharing

A collaborative exchange in which both parties demonstrate value or benefits that out weighs the risk of sharing and losing control of your information / data

Information Sharing is a participatory endeavor

INTERNET | SECURITY | SYSTEMS®

Levels of Information

- **Strategic – Intel and LE**
  - Focus on Terrorism – Physical in Nature
- **Operational – Critical Infrastructures**
  - Focus on providing Goods and Services – Cyber and Physical
- **Tactical – Law Enforcement**
  - Focus on Protection – Physical in Nature

INTERNET | SECURITY | SYSTEMS®

Tiers of Information Sharing Types

- **Incident**
- **Routine Data**
- **Collaboration on data**
- **Vulnerability specifics**
  - Bilateral
  - Multilateral
- **Protection (prior to an outbreak)**

Who is working together: On OUR side

INTERNET | SECURITY | SYSTEMS®

The Players

- FIRST
- Regional CERT/CIRT’s
- Academic CERT’s
- Corporate CIRT’s
- Law Enforcement
- Intelligence folks
- National CERT’s
- Smaller groups
  - NSIE
  - NSP-SEC

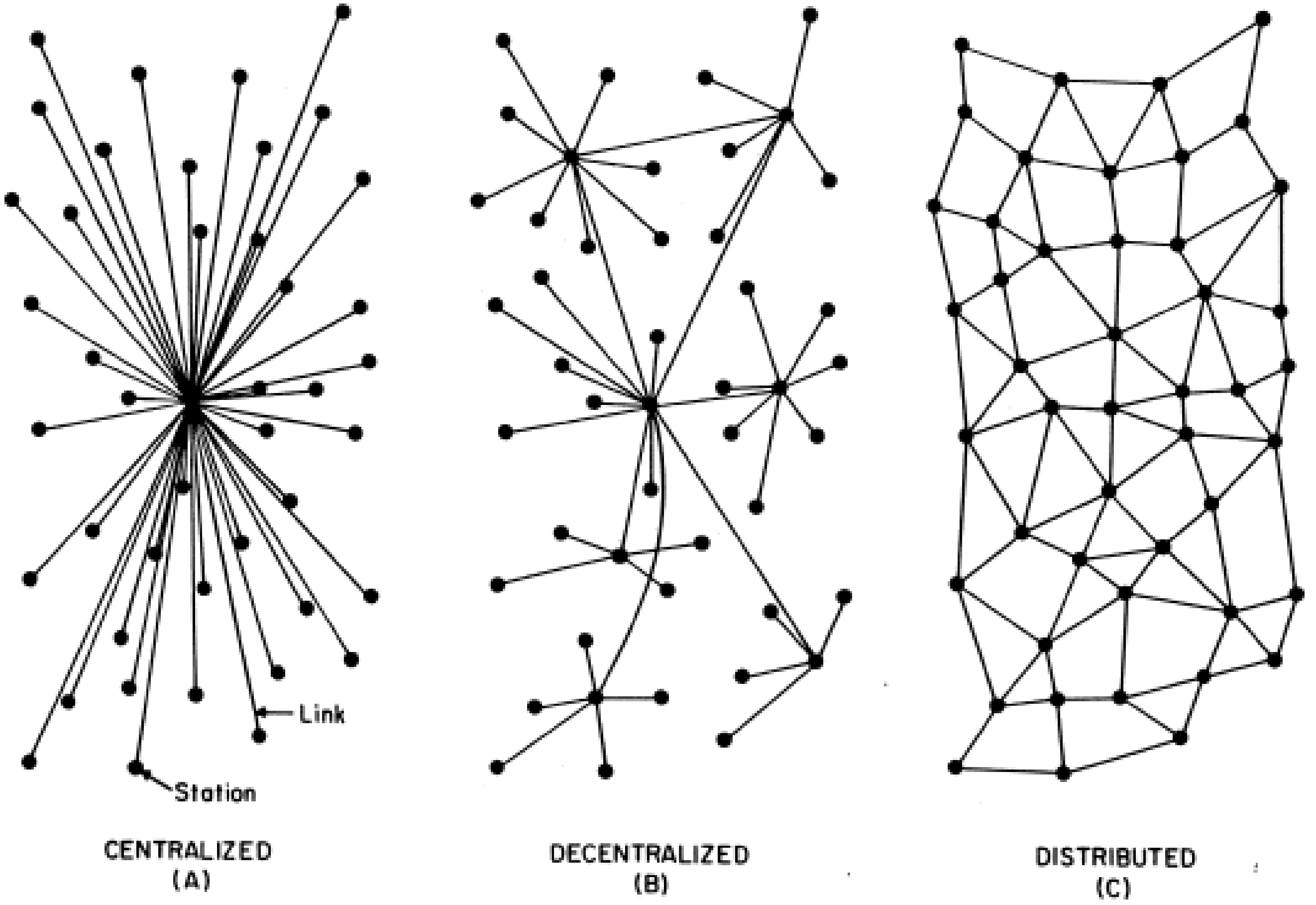
- Industry Groups
  - ISAC’s
- Regional / State Governments
- NGO / PVO’s
- Bilateral Arrangement
- Techie to Techie
- Sector Coordinating Councils (SCC)
- GFIRST

INTERNET SECURITY SYSTEMS®

Sharing network designs and communities of interest

INTERNET | SECURITY | SYSTEMS®

Baran's Network Designs



CENTRALIZED
(A)

DECENTRALIZED
(B)

DISTRIBUTED
(C)

FIG. I — Centralized, Decentralized and Distributed Networks

Who is working together - how it started: Infrastructure Protection to Information Sharing

The United States Model for operational sharing

INTERNET | SECURITY | SYSTEMS®

Information Sharing

- **Suggested by PDD-63 (superseded by HSPD-7)**
- **Private Sector formed ISACs starting in 2000**
- **Working together through ISAC Council**
- **Sector Coordinators – a moving target**
- **Three general types of information sharing (from NIAC Study)**
  - Intelligence Community
  - Law Enforcement
  - Critical Infrastructure

INTERNET | SECURITY | SYSTEMS®

Critical Infrastructures

- **85% owned and operated by the Private Sector**

- **Share information on three categories**
  - Physical terrorism
  - Natural disasters
  - Cyber events and vulnerabilities

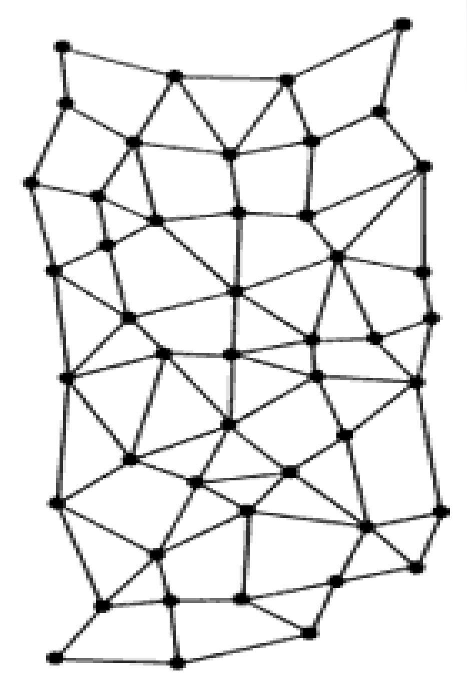
- **Each sector approaches the first two differently**

- **Cross –Sector discussion on cyber five days / week**

Milli – Second Sectors

- **Electric Services – Powers the Data**
- **Telecommunications – Transports the Data**
- **Information Technology – Manipulates and Stores the Data**

Distributed



INTERNET | SECURITY | SYSTEMS®

How sharing starts

- **Personal Relationships**
  - Trust
  - Point-to-point

- **Broader Concept**
  - Trusted Group – common goals and/or understanding
  - Protected Means
  - Needs buy-in from Senior Management
  - ***Execution*** by those who work the issues

INTERNET | SECURITY | SYSTEMS®

So what does this mean?

- **Personal exchange of information is like a barter system – benefits two parties at best**
- **The definition of Information Sharing should look like Currency**
  - Not just differing denominations
  - Use different currencies

Dollar	Information Technology
Euro	Communications
Yen	Electric
Pound	Financial

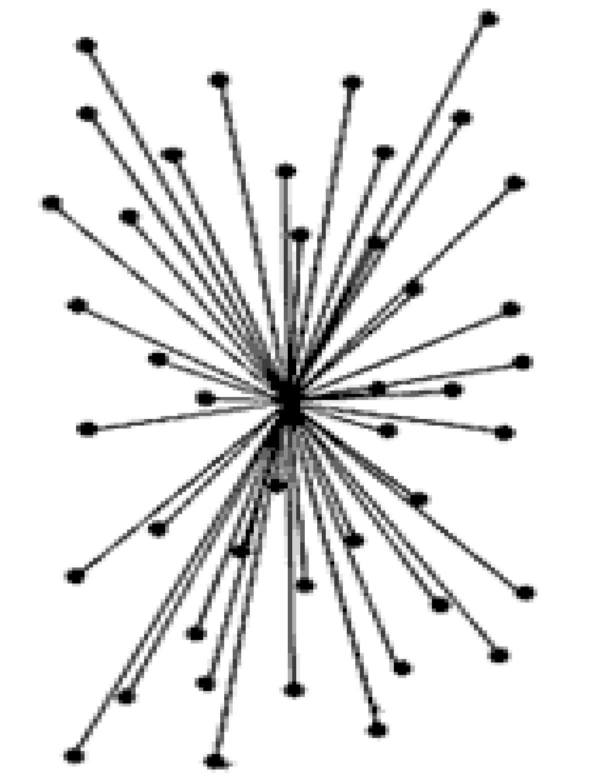
- Currency is of relevance to the recipient
  - Private Sector – Specific in view, global in action
  - Government – Global in view, specific in action

INTERNET | SECURITY | SYSTEMS®

Why it's not working

INTERNET | SECURITY | SYSTEMS®

Adapting Baran’s Centralized Design



AKA: the hub and spoke

Or what has become Information Sharing

INTERNET SECURITY SYSTEMS®

So why does that not work?

- Trust issues (no deposited currency – beginning balance)
- Single point – large scale events
- Focus is responsive to one group
- Not part of like minded concerns
- Unbalanced collection through analysis efforts
- Not Standardized reporting or analysis

INTERNET | SECURITY | SYSTEMS®

How it could

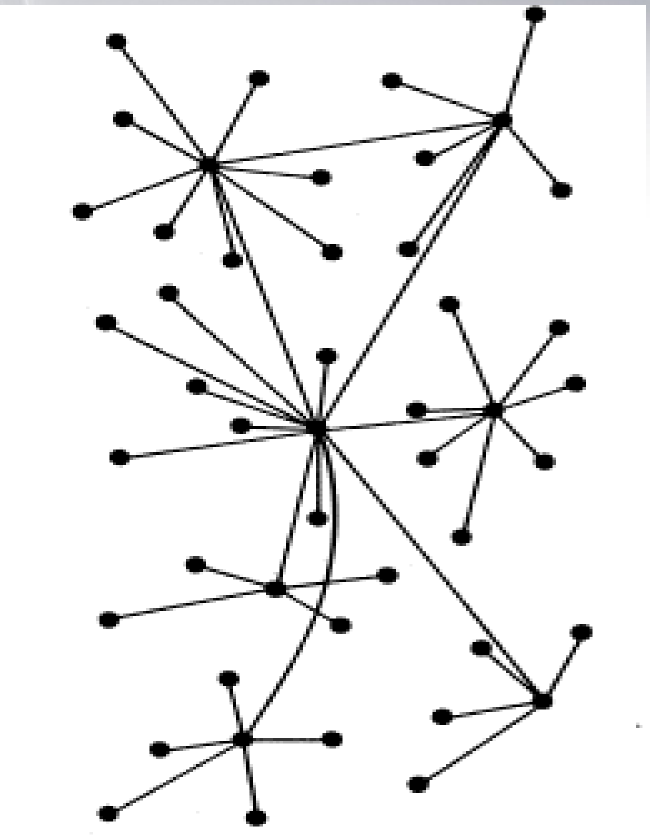
INTERNET | SECURITY | SYSTEMS®

What do we need for success?

- **Data Centers of Excellence**
- **Each with a specified constituency**
- **Collects data in an automated and routine fashion**
- **Collective analysis by those participants with direct knowledge of systems**
- **Able to be queried by other trusted centers (Private/Public)**

INTERNET | SECURITY | SYSTEMS®

Decentralized Information Sharing



DECENTRALIZED
(B)

INTERNET SECURITY SYSTEMS®

Why?

- Span of Control
- Flexibility to react and done quickly
- Concentration of knowledge to work remediation's
- Ability to bring resources into play
- Established multi-mode communications
- Not vendor / academic / government specific

INTERNET | SECURITY | SYSTEMS®

Sector ISACs working together

- Chemical*
- Electric Services*
- Energy*
- Financial Services*
- Highway
- Information Technology*
- Public Transit*
- Telecommunications*
- Multi-State*
- Surface Transportation*
- Water*
- Research & Education Network*
- Emergency Management & Response*

Types of Information Sharing

- **Routine Sharing of Information (vice automated Data)**
  - 24 / 7 / 365
  - Incident Coordination – Scanning of routine nature
  - Vulnerability remediation discussions – bulletins and patches
- **Emergency Sharing**
  - Imminent or ongoing attacks (DDoS etc)
  - New exploitation vectors and zero day vulns
- **Cross-sector responses and queries into data**

INTERNET SECURITY SYSTEMS®

What we are looking for as an outcome

- Situational Awareness
- Collaborative Analysis
- Coordinated Incident Response
- Preventative Protection

INTERNET | SECURITY | SYSTEMS®

Vision for next generation of security

INTERNET | SECURITY | SYSTEMS®

Models of How Data / Information is Shared (Individuals to Groups)

- **One-to-one – personal relationship, phone or IM, PGP e-mail**
- **Closed Group**
- **Small Communities of Interest**
- **Multi-Communities of Similar Interest**
- **Regional Communities of Interest**

INTERNET | SECURITY | SYSTEMS®

Desired End States

- Working systems – with automation
- Serve Community of Interest needs
- Serve Internet at Large

INTERNET SECURITY SYSTEMS®

Strategery

- **Overarching International Group**
  - Sets Goals for protecting the Internet
  - Introduces sub-groups
  - Provides frameworks
- **Regional Operational Focus**
  - Localized by large region
  - IT or ICT focused
    - I.E. AP CERT, TERENA TF-CSIRT, IT-ISAC
  - Reduce Overlap and specialize

What does it need to become

- **Based on organizations and resilient over time**
- **Information sharing needs to be formalized**
  - Formal agreements
  - Concept where each member agrees to provide
  - Centralized operations
  - Collaborative analysis
  - Responsive to member needs and to public
  - Differing EXCHANGE rates, but exchange of ***value***
- **Based on the core competency of the sector**
  - We have sectors that are trying to be other sector competencies, instead on concentrate on strengths
- **Vendor neutral**

Information Sharing – Everyone is talking

INTERNET | SECURITY | SYSTEMS®

Who or How should we coordinate / React

- Sharing of data is with those who can impart an effect
- Cannot be a highly restrictive bar to admission
- Must be participatory (that is where the value is!!!!!)
- Do not discount newer technologies (add more tools to the tool box. All problems are not nails!)

Focus on the Goals

- **Better Planning**

- **Coordinated Action**
  - Detection
  - Deterrence
  - Protection
  - Response
  - Recovery

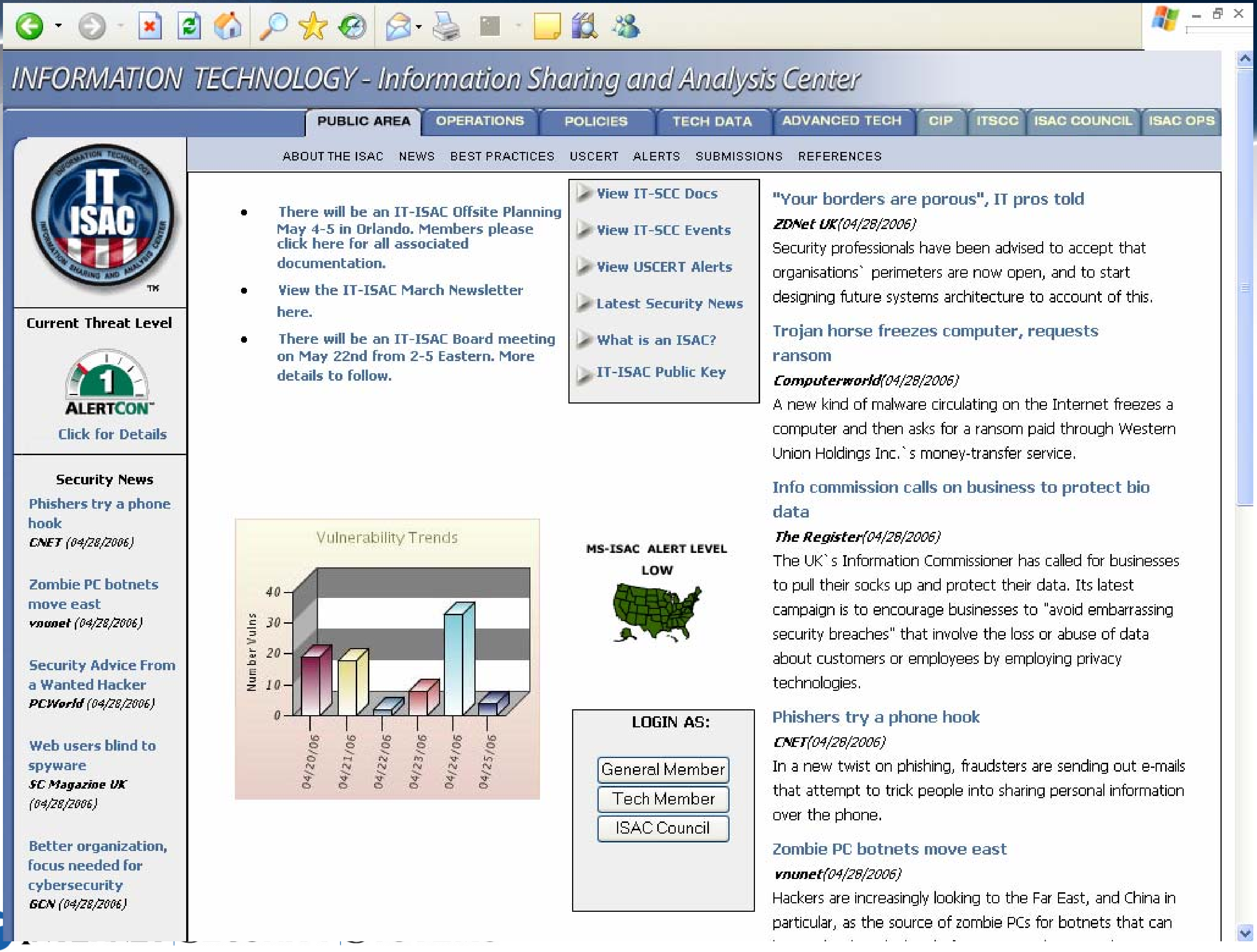
- **Rational Allocation of Resources**

- **Real results and cooperative support**

INTERNET | SECURITY | SYSTEMS®

Collection efforts

- Need to know what is priority for collection
- Need to have an agreed upon categorization of information
- Must have a formal agreement to conduct business
- Followed by a means of what is collected, and how analyzed, stored, and disseminated to include filters
- Must have data collection plan and automated means of submission to include anonymization of the submitter
- Categorize your submitters: by size, quantity and quality



- There will be an IT-ISAC Offsite Planning May 4-5 in Orlando. Members please click here for all associated documentation.
- View the IT-ISAC March Newsletter here.
- There will be an IT-ISAC Board meeting on May 22nd from 2-5 Eastern. More details to follow.

Security News

Phishers try a phone hook
CNET (04/28/2006)

Zombie PC botnets move east
vnunet (04/28/2006)

Security Advice From a Wanted Hacker
PCWorld (04/28/2006)

Web users blind to spyware
SC Magazine UK (04/28/2006)

Better organization, focus needed for cybersecurity
GCN (04/28/2006)

"Your borders are porous", IT pros told
ZDNet UK(04/28/2006)
Security professionals have been advised to accept that organisations` perimeters are now open, and to start designing future systems architecture to account of this.

Trojan horse freezes computer, requests ransom
Computerworld(04/28/2006)
A new kind of malware circulating on the Internet freezes a computer and then asks for a ransom paid through Western Union Holdings Inc.`s money-transfer service.

Info commission calls on business to protect bio data
The Register(04/28/2006)
The UK`s Information Commissioner has called for businesses to pull their socks up and protect their data. Its latest campaign is to encourage businesses to "avoid embarrassing security breaches" that involve the loss or abuse of data about customers or employees by employing privacy technologies.

Phishers try a phone hook
CNET(04/28/2006)
In a new twist on phishing, fraudsters are sending out e-mails that attempt to trick people into sharing personal information over the phone.

Zombie PC botnets move east
vnunet(04/28/2006)
Hackers are increasingly looking to the Far East, and China in particular, as the source of zombie PCs for botnets that can

Why Data Centers of Excellence

- They are within the Community of Interest
- They can establish regular communications to other COI
- They can hold sensitive data for the members of the COI
- They are operationally focused

INTERNET | SECURITY | SYSTEMS®

Thank You

INTERNET | SECURITY | SYSTEMS®

Internet Security Systems (ISS) strives to provide accurate and current information in all material. ISS does not assume any responsibility for the accuracy of the information or specifications provided.
Specifications and content are subject to change without notice.