NASA
Ames Research Center

Strategy for
IT Security

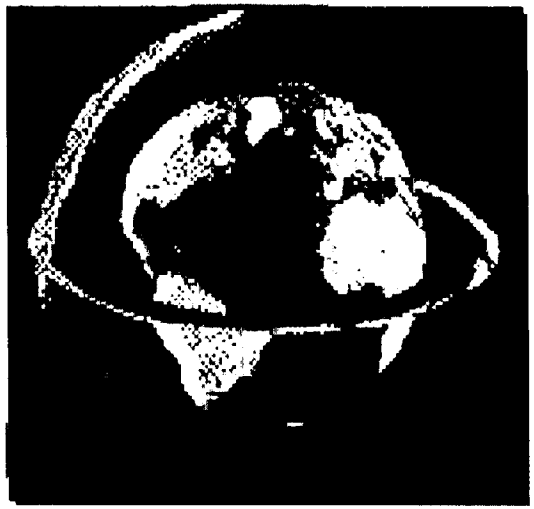
S. Scott Santiago
ARC CIO

Ames Research Center

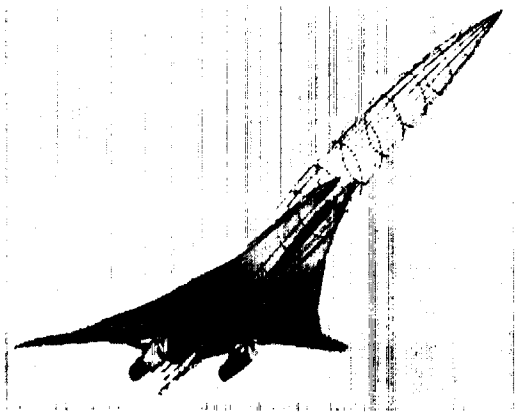
NASA Mission
and
IT Security

NASA Missions

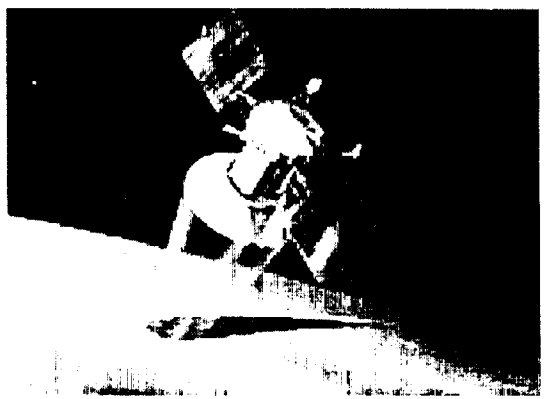
Human Exploration of Space



Earth Science



Aero-Space Technology



Space Science

Top management buy-in

- "NASA relies on computers, data and networks to perform our missions. Security and integrity of these information technology systems is essential if we are to accomplish our missions safely and reliably. Our policy and procedures provide a complete framework for information technology security.
- "Security of NASA's information technology is the responsibility of management. We have a cadre of experts who provide security assistance and oversight, but our managers must understand the risks and determine the safeguards.
- "Good security practices are everyone's responsibility. These include safeguarding passwords, special care of sensitive information, and the use of our public key infrastructure for sensitive communications."

Extract from Statement by NASA Administrator Dan Goldin to NASA senior management, June 19, 2000

What is the security problem we are trying to solve?

- Security with openness
  - Space Act of 1958 requires keeping public informed
  - Interactions with companies, universities, other agencies, foreign countries, public
- Decentralized management of Centers and programs
- Outsourcing of network operations, but not of Agency IT architecture or security responsibility
- Attractiveness of NASA as a hacker target
- Dynamic, multi-protocol/port, high-bandwidth (OC-3 and up) applications and data

How did NASA develop a business case?

- Deputy Administrator commissioned NASA-wide internal study of IT security after incidents and audits showed problems. Study developed business case and recommended actions.
- GAO audit of NASA IT security confirmed problems and supported conclusions of internal study.
- Senior management accepted recommendations, increased funding, identified staff, created IT Security Council at senior management level.

CIO Structure

NASA CIO

- CIO recognized that the information technology (IT) expertise existed across all the NASA enterprises and centers
- The CIO split the IT responsibility between the centers and established three Principle Centers to better focus efforts in
  - IT Security
  - Networking and communications
  - desktop computing

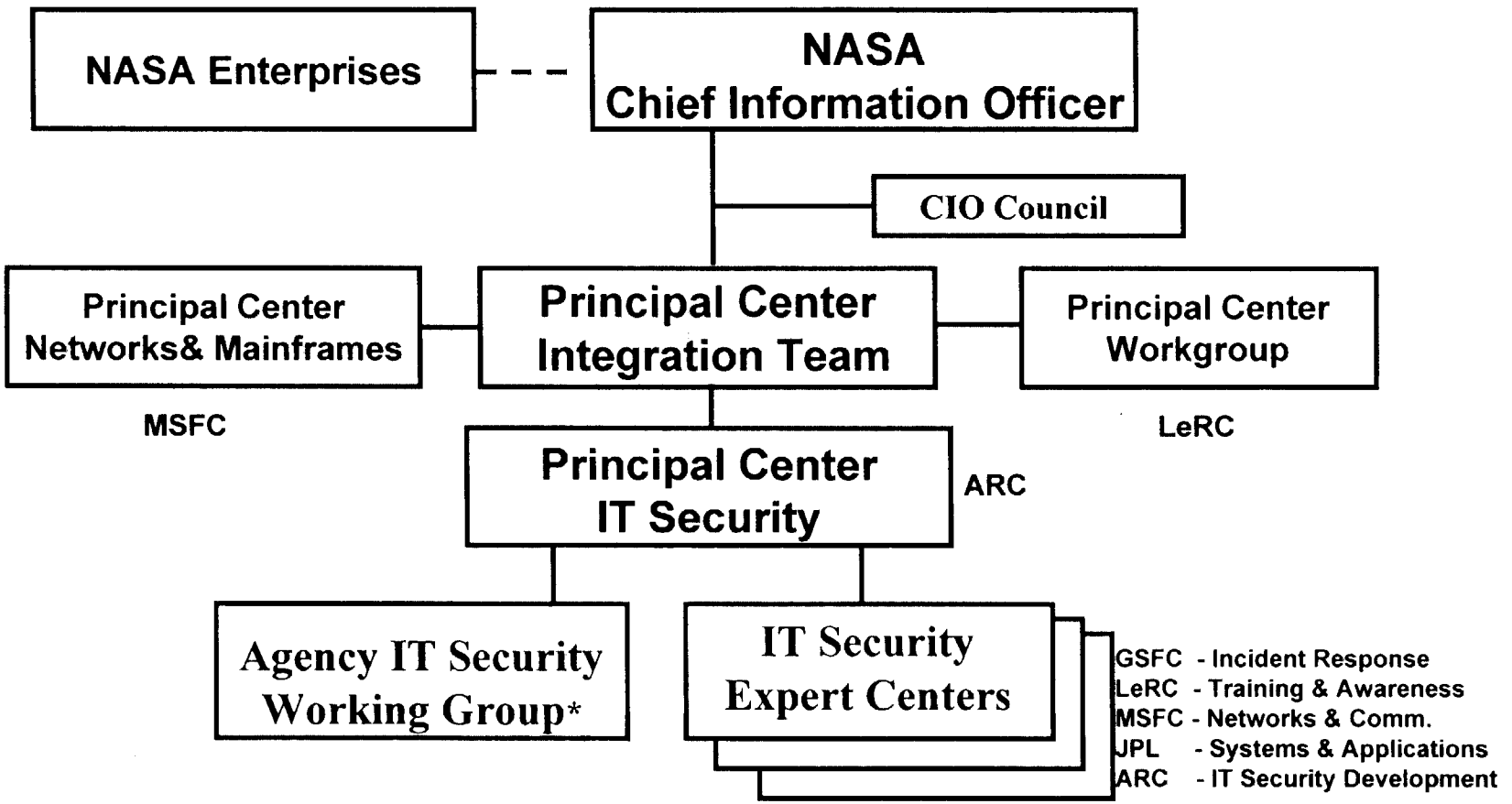
What is our business, and how does security affect it? (1)

- NASA conducts very visible research and communicates results to public. Public confidence is very important to NASA success.
  - *Safety, reliability, availability of systems, integrity of data*
- NASA works with other agencies, universities, companies, other countries and produces sensitive technology.
  - *Safeguarding controlled, proprietary and national security data*

What is our business, and how does security affect it? (2)

- NASA depends heavily on IT for mission operations, scientific data collection, analysis, and dissemination, managing operations, and administration.
  - *Direct costs to clean up security compromises*
  - *Cost to recover lost or corrupted data*
  - *Additional indirect and opportunity costs due to compromises*
  - *Threats to safety, disruption of operations, damage to facilities, harm to national security*

CIO Structure



* IT Security Working Group is made up of the Center IT Security Managers or other representatives

Ames Research Center

NASA CIO

- All policies, standards and architecture recommendations developed by the Principle Centers must be approved by the majority of all NASA Centers (Federated Approach).

NASA CIO

- Philosophy of NASA's Computer Security Program
  - IT Security needs to be factored into all decisions concerning IT resources. Computer security should never be an afterthought. It must be planned for throughout the life cycle of a system--from project initiation through its disposal
  - Automated information resources shall be provided at a level of security and integrity consistent with the potential harm from their loss, inaccuracy, alteration, unavailability, or misuse.

NASA CIO

- Strengthening the weakest link by educating employees on vital security practices and establishing reasonable policies and practices to ensure employee compliance
  - NASA has embarked on a training program that requires;
    - » all managers to be trained in their responsibilities
    - » all employees to be made aware of the security threat
    - » all system administrators to be trained

NASA FY2000 IT security metrics (1)

Top-level metrics

- Goal: NASA and contractor employees understand ITS responsibilities and demonstrate skills needed to carry them out
  - Metric: Percentage of target groups that have received training
- Goal: Reduce system/application vulnerability exposure to level where operations aren't jeopardized
  - Metric: Vulnerabilities per system less than target value
- Goal: NASA, collectively, is alert to intrusion attempts and takes effective action to thwart them
  - Metric: Identify, distribute, and maintain a list of top sites engaging in hostile activities toward NASA

NASA FY2000 IT security metrics (2)

Top-level metrics

- Goal: NASA uses an effective infrastructure for authentication, encryption, signature, etc.
  - Metric: 100% deployment of PKI infrastructure and plan for improved authentication
- Goal: NASA Centers comply with Agency IT Security policy as documented in NPD 2810, NPG 2810, IT Technical Standards, and other management directives
  - Metric: Specific NASA systems fully comply with security policy

NASA CIO

- NASA bases the use of encryption technology on the risk to the information/data residing on the system
- What encryption technology used depends on the risk associated with the system

Ames Research Center
IT Security

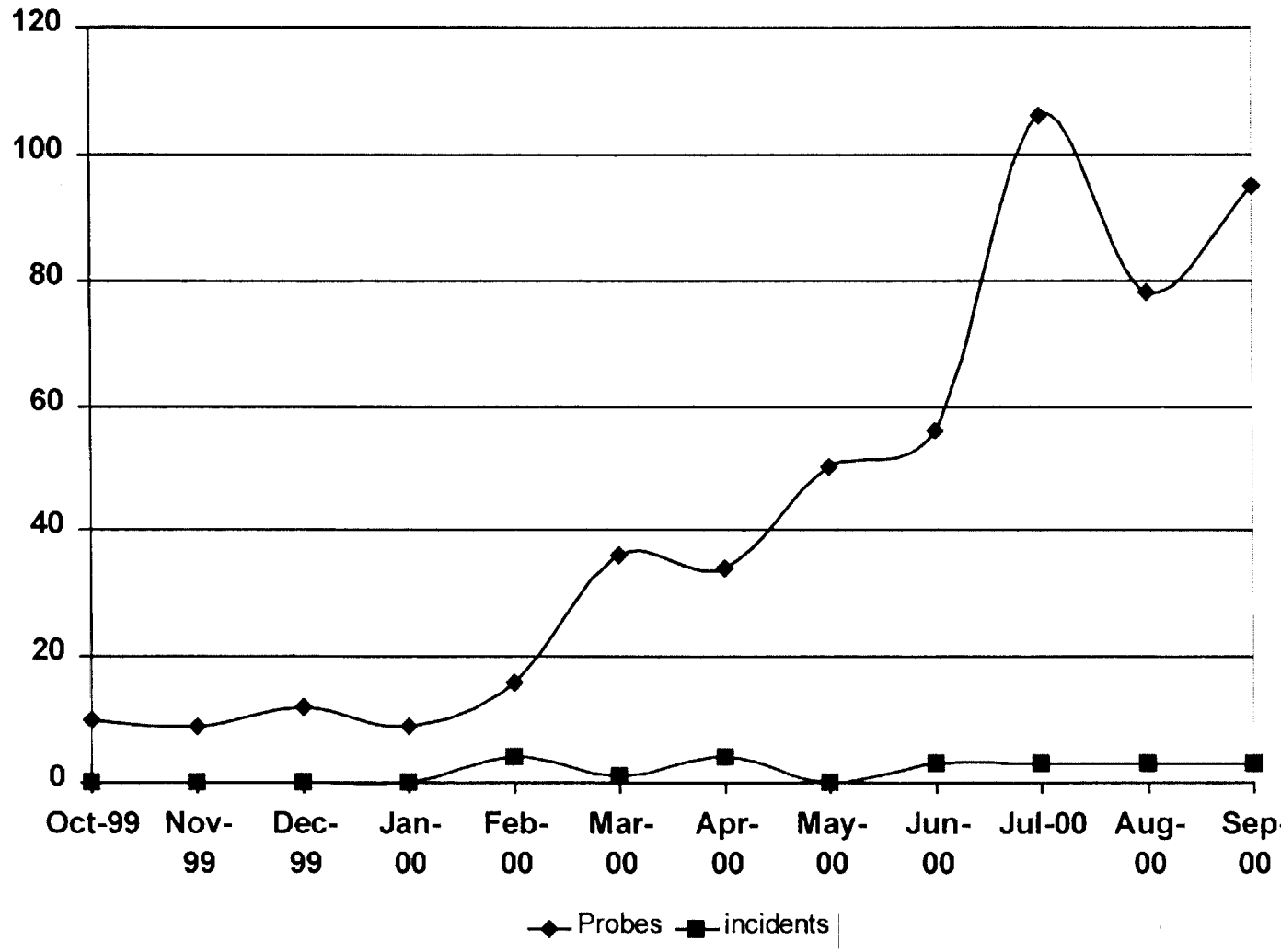
Ames Research Center

- Attitudes in a research environment can lean towards
  - Researchers viewing IT security as
    - » a drain on their resources
    - » will require them to act differently
  - Security is your problem
- Gaining acceptance of your security plan in a research environment
  - Constant communication with the researchers
  - Emphasizing benefits

Strategic Approach

- Mandatory ITS Planning and Risk mitigation
- Trained workforce in their ITS responsibilities
- Support for Center staff in their evaluation of their IT security risks and problems in order to determine appropriate steps and priorities
- Recommend "best-of-breed" products to infuse the center with state-of-the-art technology
- Tough Program to reduce system and network vulnerabilities
- Participate in Agency Working Groups (Firewall, VPN, PKI and IT Security Managers)
- Collaborate with Industry & University partners

IT Security Probes vs Incidents



Center IT Security Policy & Practices

- Ames Policy
  - Covers network and computer security
  - applies to all computers and other devices connected to the Ames Research Center's Local Area Network
- Policy addresses the network structure and various security levels that are present; Open, Public and Private and the various Configuration Control Boards
  - ARCLAN CCB - reviews and recommends overall policies for network design and architecture changes
  - Firewall CCB - works in conjunction with the ARCLAN CCB and is responsible for review and approval of changes to the Firewalls rule sets

Center IT Security Policy & Practices

- Any system or service that poses an unacceptable risk to any other Ames system or service on the Ames network will be disconnected
- All devices that are connected or are to be connected to an Ames network must be registered with a proper IP address in the Ames DNS
- All systems that are being moved or added to the Ames network must meet an acceptance criteria prior to being connected
- Network scanning is restricted to the Ames IT Security Office or by an authorized official approved through official channels established by the Ames IT Security Manager

Center IT Security Policy & Practices

- The use of computer or network attack tools is prohibited
- All network devices including wireless, i.e., hubs, switches, routers, etc., will be placed in authorized locations
- Users must report any computer compromise immediately to the IT Security Office, 4-1234.

Workforce

- How to take advantage of the situation and provide an environment to keep the skills need is a challenge
- How does an Ames compete for these workers against a back drop of outsourcing our IT infrastructure
- How to improve (change) the work environment without creating a negative attitude
- change is the biggest cause of negativity
  - people always feel their competence is coming into question
  - losing control

Workforce

- Reports on dot-comm layoffs for last year (2000) put the number at around 50,000
- The lure of riches was undeniably a factor for many who went to work in new technology companies
- The experience shapes dot-comers
  - bent for collaboration
  - fast decision making
  - autonomy
  - working without managerial hierarchy
  - rules were unknown
- The desire for some stability of more traditional employment opportunities provides a great opportunity

Center IT Security Policy & Practices

- Existing Operating Procedures
  - Incident detection systems are used to monitor for known attack signatures published by the Vendor or provided by NASIRC
  - System Audit tools are used to scan a list of known vulnerabilities that is developed the IT security Managers from all Centers and approved by the NASA CIO Office
  - monitoring for un-approved modem utilization, system detects modem signal and originating phone number

IT Security

- As part of NASA's decision to outsource a large part of it's IT infrastructure Ames promoted
  - IT Security is a critical capability that should stay in-house
    - » even if we did outsource it if something went wrong NASA would still receive the full negative press
  - NASA IT Security team would serve as a skilled IT resource pool
    - » IT Security system audits and network monitoring give us good insight as to how well the outsource provider is performing
    - » retain skilled IT workforce that can be used the next time an outsourced contract is negotiated

Workforce

- Environment needs to be exciting and challenging to attract and keep the skilled employees needed to maintain and implement state-of-art applications and services
- Working conditions have to be attractive
  - salaries on par with other organizations
  - the latest equipment
  - good leaders
  - a learning environment

IT Security

- IT Security is fun and exciting work
  - ARC has been able to hire experienced team members even when Silicon Valley unemployment was near zero
  - NASA has strong name recognition
  - strong management support for the role within the Center and NASA top management
- The field is fast paced with constant change
- IT Security responsibilities expanded to provide engineering support for projects and operations

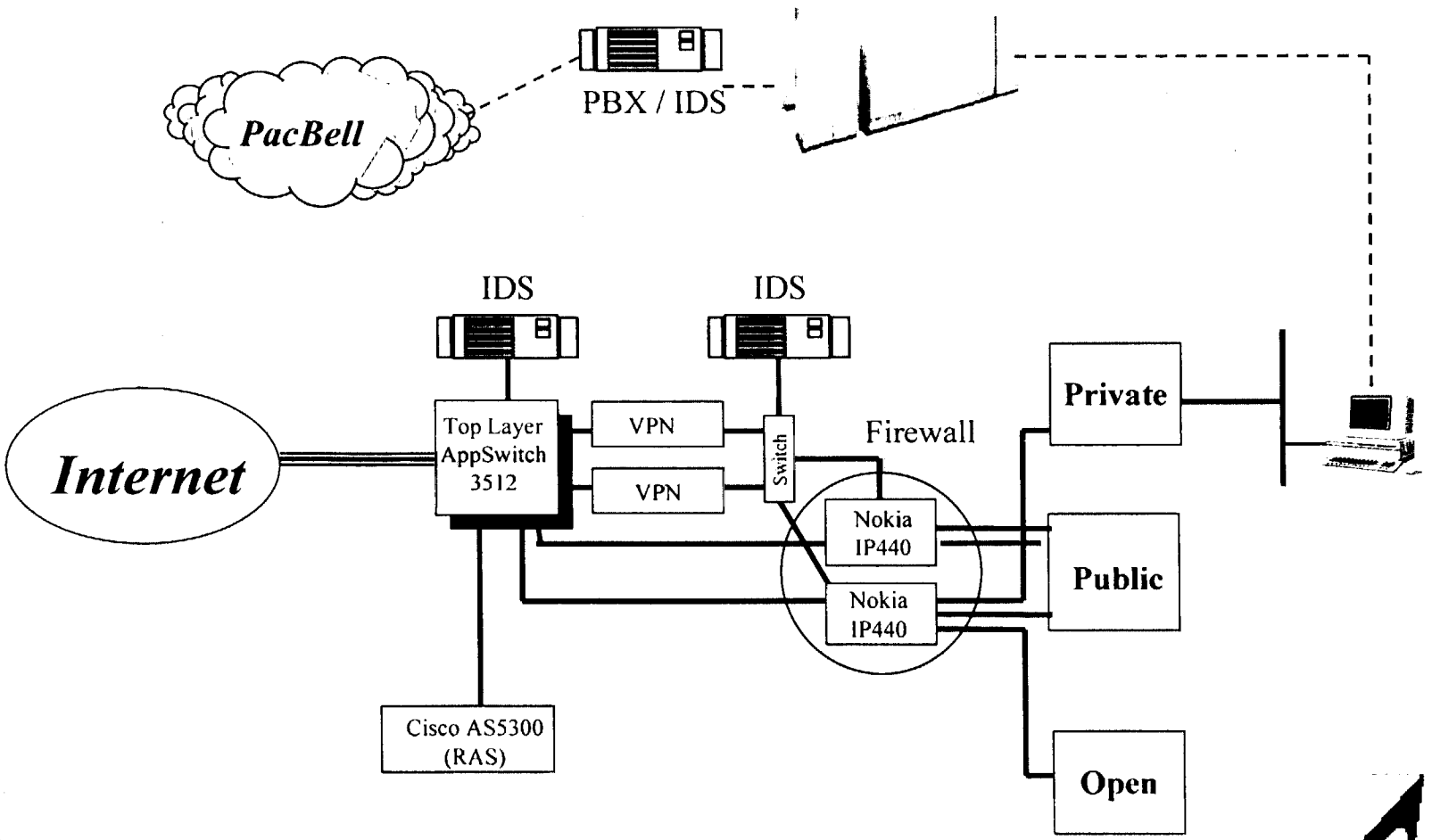
What did we do

Workforce

- Established Chief Architect that ensures that all technical solutions tie back to the architecture
- Identified strong leads in the areas of ITS engineering and IT security monitoring and intrusion detection
- Gave leads authority and resources to build their teams
- Set aggressive goals and objectives for the restructuring of the infrastructure

Changed the Infrastructure

- Built security into the ARC infrastructure
  - Upgraded the Local Area Network and
    - » created three levels of security that can be brought to the desktop
    - » Deployed a Virtual Private Network (VPN) solution as part of the upgrade
    - » expanded network monitoring to support Gigabit network
    - » Improved single logon authentication for central services
  - Created a secure enclave for housing services
    - » calendar and email
    - » document sharing
    - » web based applications
  - Public Key Infrastructure (PKI) used for strong authentication
  - Deployed PBX firewall


PacBell
PBX / IDS
IDS
IDS
Internet
Top Layer
AppSwitch
3512
VPN
VPN
Switch
Firewall
Nokia
IP440
Nokia
IP440
Private
Public
Open
Cisco AS5300
(RAS)

Broaden Roles and Responsibilities

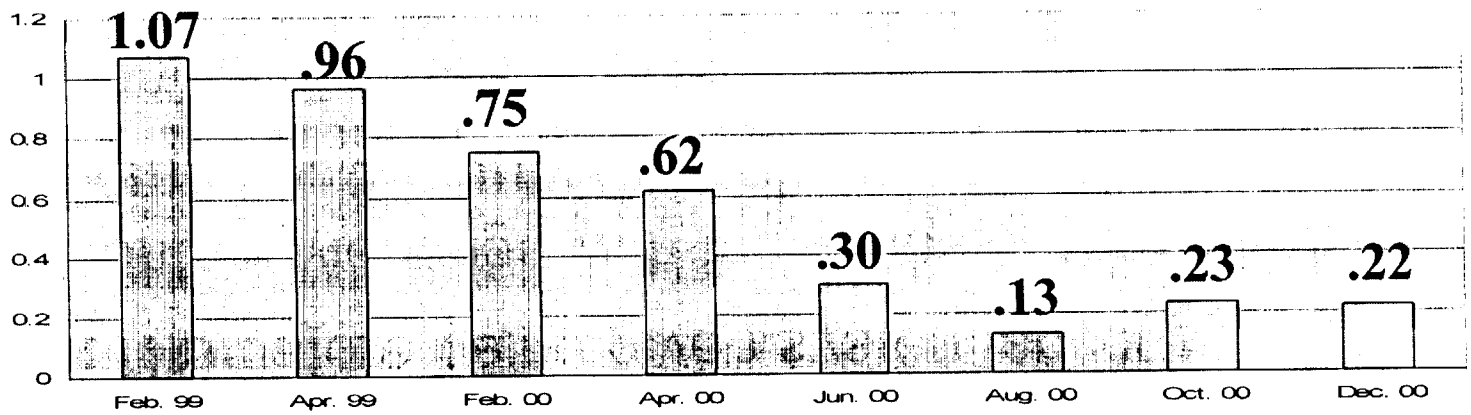
- Agency project management and technology evaluation activities
  - Agency PKI deployment and operation
  - Den/PKI evaluation
  - Token/smart card evaluation
    - » Agency effort to deploy common technology approach
    - » Working in conjunction with other federal efforts
    - » Recommendation due in July 2001

System and Intrusion Monitoring

- Developed team to conduct system and Intrusion monitoring as well as penetration testing
  - home grown team, if skills can't be bought we make
  - emphasis strong partnership with user/customer
    - » everyone learns
    - » team also acts as trainers
  - White-hat hackers (this is fun)
  - Incident response and forensics
  - Support from all levels of management
  - Goal driven

Vulnerability Reduction

- Reduce exposure against the NASA 50



- Manage an Aggressive Scanning Program:
  - Monthly Scan
  - User Requested Scans for Network & Hosts
  - Scan subnets involved in Computer Incidents
  - Ad Hoc Scans

Summary

- IT Security to be successful has to have management support
- Business case is aimed at management within all levels of your organization
- Must use management-level arguments
- Keep management motivators in mind, including fear
- Making ITS an integral part of your operation and culture
- "Security is good business"

Awareness & Training

- All managers and employees required to take ITS training
- All System Administrators are required to be trained in ITS before being given system access
- Monthly Meetings with the Ames organizational Computer Security Officials
- Monthly BoF's for Admins & Users
- Constant communications with Ames ITS personnel on various issues, i.e., updates on new vulnerabilities, patches, virus', etc
- In-house course development and training
- Expanded use of Web for on demand training