System Security
Compliance Monitoring Program

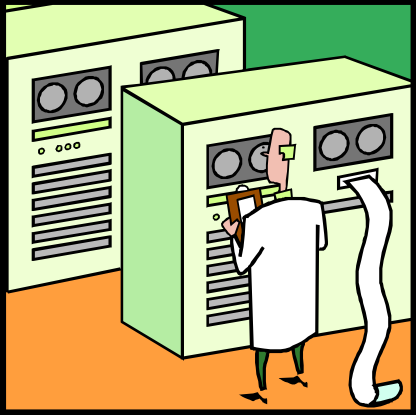
Monitoring compliance to corporate information security standards

Pat Hymes
First Union Corp.

Information Security Policies, Standards and Guidelines

Standards - support corporate policies and define what controls are needed

Guidelines - describes how to implement controls on a particular platform (e.g., AS/400, Unix, Novell, NT)



The Challenge

Are people following the standards?

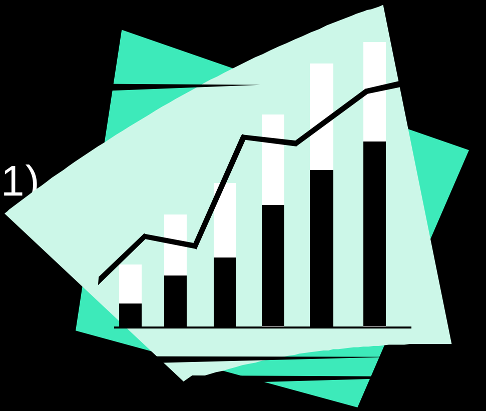
How compliant are our systems with the standards/guidelines?

Are weaknesses being identified and addressed?

How do we improve the security of our distributed environment?

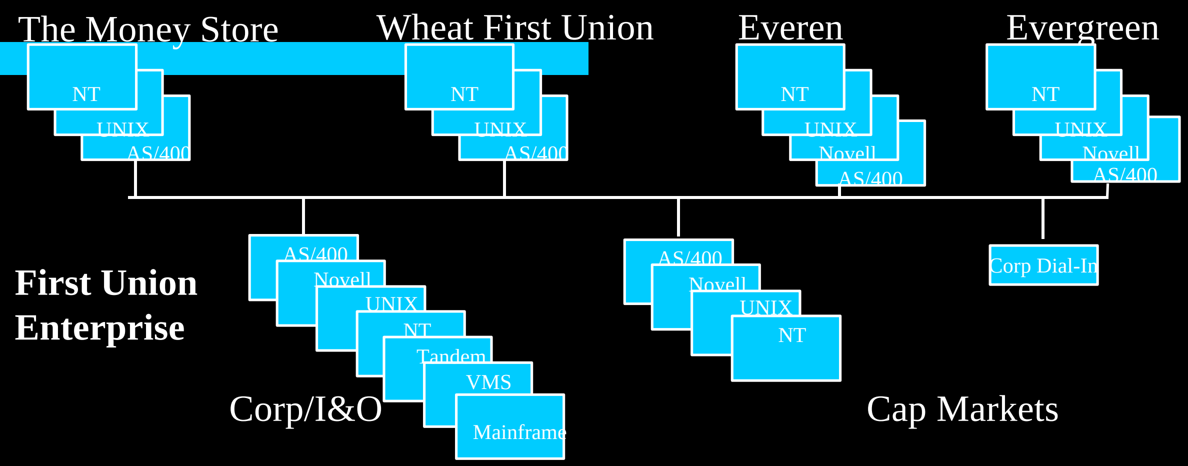
Why Monitor Compliance?

- We have better data to do our job
- Enterprises with weak information security controls suffer more than twice as many incidents than Best in Class organizations (1)
- Supports proactive identification of weak controls (for correction or sign-off)
- Helps satisfy OCC concerns regarding technology risk



(1) - European Security Forum, 1998/99 Information Security Status Survey

Considerations



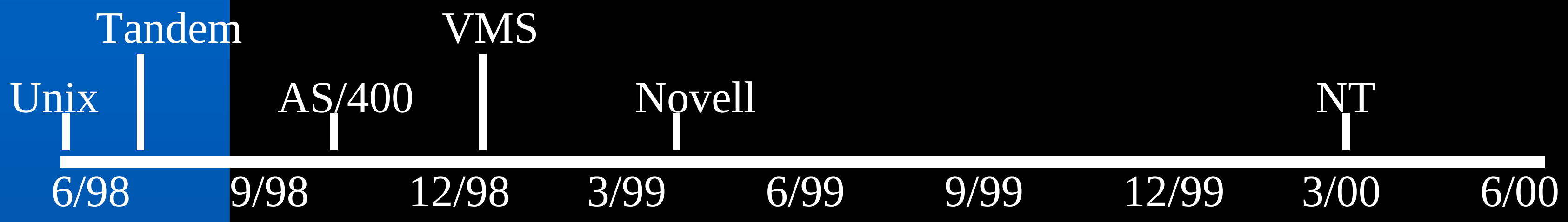
- Thousands of Systems
- Multiple IT Departments
- Low Security Awareness
- Technological Evolution, Complexity
- Time to Market Pressures
- Immature and Proprietary Controls

Approach

- Implement automated tools to assess compliance
- Use published security guidelines as criteria
- Assign weight to each test (scale: 1-10)
- Compute system compliance score
  - Based on points earned vs. total possible
- Pull results to central compliance database
- Provide multiple levels of reporting
- Re-assess on a regular basis
- Assist and support SAs wherever possible

> ***"If you don't know where you're going,***
> ***you'll never know when you get there."***
> ***Yogi Berra***

Program Evolution



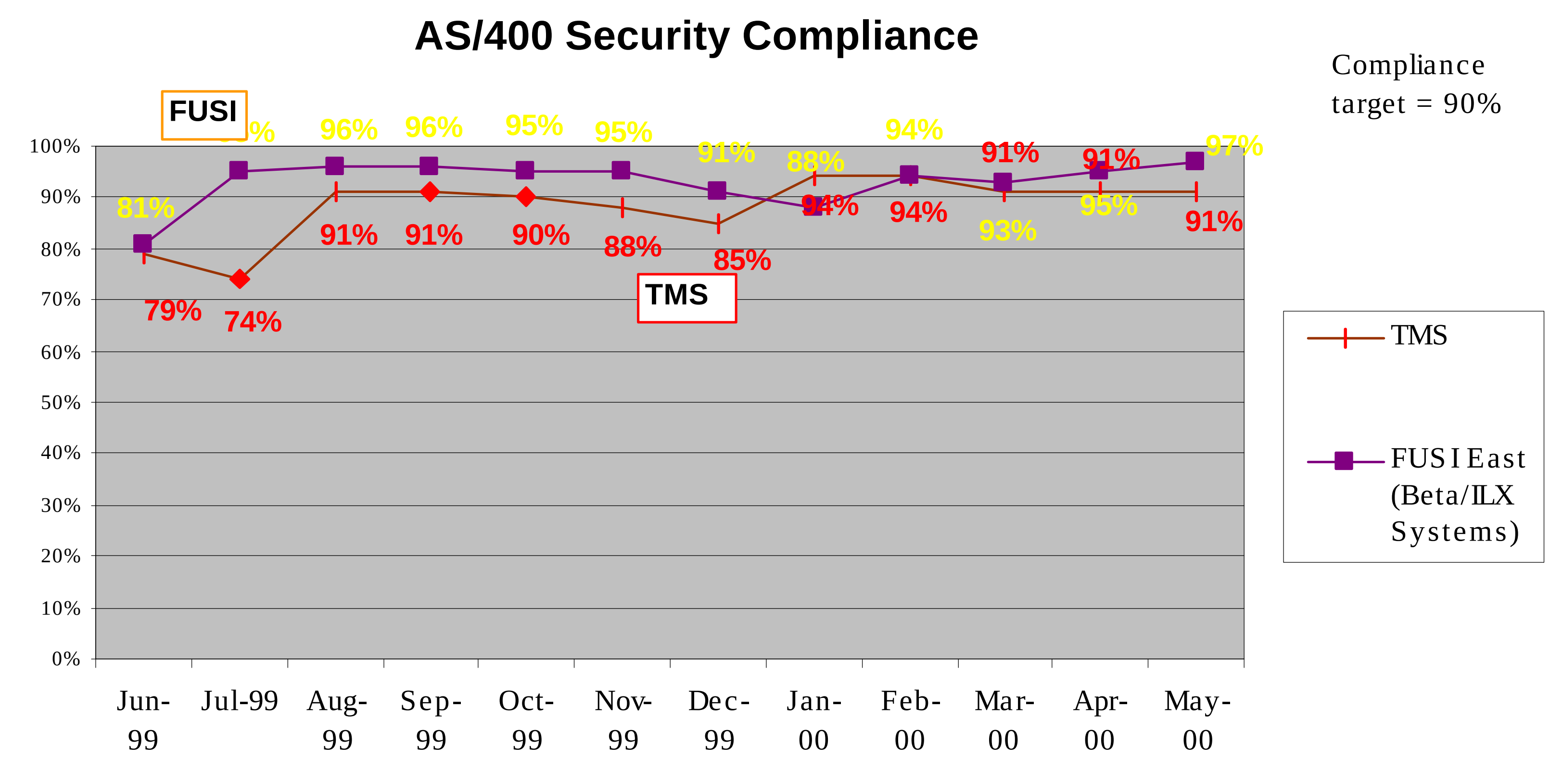
Current State

- Compliance tools deployed on over 1200 systems
- Monthly reporting to IT management
- High level compliance average include in “key management metrics” database
- NT rollout just beginning

Benefits to Date

- Average (overall) compliance score has increased from 62% to 86%
- Lockdown tools & processes have been established
- Security awareness and acceptance of accountability of SAs, IT management has increased significantly
- Security compliance part of performance reviews
- Good relationships established
- A foundation for future security initiatives has been established

Sample Chart From Monthly Compliance Report



- News….
- Key issues needing attention...

Pains, Gains & By-Products

- Compliance monitoring is more than a tool
  - Technology +
  - People
  - Process
- It's okay to start small and build, refine
- Set achievable goals
- Only use "the hammer" when needed
- Measurable results boosts ISD staff morale

Other Metrics Reported

- Virus Related
  - Percentage of file servers, mail servers and desktops with current pattern files
  - # virus related help desk calls
  - *Future: # viruses cleaned/blocked/eliminated*
- Laptop Theft
  - # of unsecured laptops observed by property mgmt guards
- *Future: Network device security compliance*
- *Future: Unsecured modem metrics*
- *Future: Technology Risk Scorecard for the Director of e-Commerce*

Improving System Security

Information Security Division

Platform Security Guidelines

Security Education

Consulting/Assistance

Compliance Monitoring/Enforcement

System Administrators

Change Behavior

Change Culture

Key Components